Device-independent verification of Einstein-Podolsky-Rosen steering

Yuan-Yuan Zhao,1,2,∗ Chao Zhang,1,3,∗ Shuming Cheng,4,5,6,† Xinhu Li,7,8,‡ Yu Guo,1,3 Bi-Heng Liu,1,3,§ Huan-Yu Ku,9,10 Shin-Liang Chen,11 Qiaoyan Wen,7 Yun-Feng Huang,1,3 Guo-Yong Xiang,1,3 ¶ Chuan-Feng Li,1,3,∗∗ and Guang-Can Guo1,3

1 College of the Science, China University of Petroleum, 266580 Qingdao, China
2 National Laboratory of Solid State Microstructures, School of Physics, and Collaborative Innovation Center of Advanced Microstructure, Nanjing University, Nanjing, 210093, China
3 Synergistic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, 230026, China
4 Department of Control Science and Engineering, Tongji University, Shanghai, 201804, China
5 Institute for Advanced Study, Tongji University, Shanghai, 200092, China
6 Institute for Quantum Computing, Baidu Research, Beijing, 100193, China
7 State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China
8 National Laboratory of Solid State Microstructures and School of Physics, Nanjing University, Nanjing 210093, China
9 Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria
10 Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria
11 Department of Physics, National Chung Hsing University, Taichung 40227, Taiwan

Entanglement lies at the heart of quantum mechanics, and has been identified as an essential resource for diverse applications in quantum information. If entanglement could be verified without any trust in the devices of observers, i.e., in a device-independent (DI) way, then the high security can be guaranteed for various quantum information processing tasks. In this work, we propose and experimentally demonstrate a DI protocol to certify the presence of entanglement based on Einstein-Podolsky-Rosen (EPR) steering. We first establish the DI verification framework by taking the advantages of measurement-device-independent technique and self-testing, which is able to verify all bipartite EPR-steerable states. In the scenario of three-measurement settings for per party, the protocol is robust in tolerance of inefficient measurements and imperfect self-testing. Moreover, a four-photon experiment is implemented for verification beyond Bell nonlocal states. Our work presents the new insight into quantum physics and paves the way for realistic implementations of secure quantum information processing tasks.

I. INTRODUCTION

Entanglement is of fundamental importance to understand quantum theory, and also has found wide applications in quantum communication and computation tasks [1]. If its presence could be certified without imposing any trust in the involved devices and their resources, then it is likely to guarantee information processing tasks with unconditional security. As a celebrated example, Bell inequalities [2, 3] violation offers such a device-independent (DI) protocol. However, the conclusive violation of Bell inequalities typically requires a high efficiency of measurement apparatuses to close the detection loophole. Besides, it also demands the low transmission loss since sufficiently lossy entangled states are unable to violate any Bell inequality [4]. Thus, the practical utility of this DI verification based on Bell inequalities is compromised in noisy quantum networks.

Notably, Bowles et al. has shown in [9, 10] that combining the measurement-device-independent (MDI) technique [7] with self-testing [7, 8, 10] yields an alternate way which is able to device-independently verify all entangled states and circumvent the potential detection loophole [11]. However, its complete implementation relies on the near-perfect self-testing of a set of prepared states with average fidelity above 99.998% [9], making it unrealistic to implement within current technology.

In this work, we propose an experimental-friendly DI protocol free of all above limitations (See Fig. 1), based on Einstein-Podolsky-Rosen (EPR) steering [2, 13, 14]. Quantum steering was introduced by Schrödinger to describe the ability that if certain pure entangled state is shared by two observers, one can remotely prepare the other’s states via choosing suitable measurements [1, 16–18]. It was operationally reformulated as EPR-steering via a task of verifying entanglement by Wiseman et al. [2]. Since it lies strictly intermediate between entanglement and Bell nonlocality [2, 19], this hierarchy implies that EPR-steering is experimentally less demanding than Bell nonlocality to verify entanglement, confirmed in various experimental setups [20–27]. Moreover, the possibility of MDI verification of steering have been shown [4–
6, 30, 32, 33], together with experimental validations reported in [5, 6, 32]. Hence, following from works [9, 10], using self-testing, we can establish a DI protocol to verify EPR-steering and hence entanglement.

We first show that all EPR-steerable states can be verified within this DI framework. Particularly, if three-measurement settings as per party are assumed, we obtain a steering inequality suitable for DI certification under imperfect self-testing with average fidelity 99.7%, which is a significant reduction in comparison to the DI verification based on entanglement. Finally, we implement a proof of principle experiment with four photons to validate the DI steering protocol, and find it can even verify Bell local states with an experimentally attainable self-testing fidelity of around 99.95%.

II. PRELIMINARIES

Suppose that two space-like separated observers, Alice and Bob say, make measurements on a preshared state. Denote Alice’s and Bob’s measurements $x$ and $y$ respectively, and the corresponding outcomes $a$ and $b$. EPR-steering from Alice to Bob is demonstrated if the measurement statistics $p(a, b|x, y)$ cannot be explained by any local hidden state model as $p(a, b|x, y) = \sum_\lambda p(\lambda)p(a|x, \lambda)\text{Tr}[E_{bij}^B \rho_{\lambda}^B]$, where the hidden variable $\lambda$ specifies some classical probability distribution $p(a|x, \lambda)$ for Alice and some quantum probability distribution $\text{Tr}[E_{bij}^B \rho_{\lambda}^B]$ for Bob which is generated via performing a positive-operator-valued measurement $\{E_{bij}^B\}_{b,j}$ on quantum states $\rho_{\lambda}^B$ [2]. Note that Alice’s side may not obey quantum rules, so EPR-steering is intrinsically an one-sided device-independent verification task. For any steerable state, the detection task can be accomplished via violating a linear steering witness of the form [3]

$$W_S = \sum_j \langle a_j | B_j \rangle \leq 0. \quad (1)$$

Here $a_j$ corresponds to the outcome of Alice’s measurement $j$, and $B_j$ represents Bob’s $j$-th observable.

Certifying the presence of EPR-steering can be adapted to the MDI scenario [4–6, 30] where the trust in Bob’s devices required in Eq. (1) is transferred to a third observer, Charlie say, who prepares a set of quantum states and sends them at random to Bob. As in Fig. 1, upon receiving these states described by density matrices $\{\tau_{b,j}^c\}$ with $T$ being the transpose operation, Bob is required to perform an arbitrary binary measurement $B$ with which the outcomes are modelled as either “Yes” or “No”. Denote by $P(a, \text{Yes} | x, B, \tau_{b,j}^c)$ the probability that Alice obtains $a$ for the measurement $x$ and Bob answers “Yes” when assigned to $\tau_{b,j}^c$. Then, arranging the corresponding outcome statistics as Eq. (1) leads to a MDI steering witness [5, 6]

$$W_{\text{MDI}} = \sum_{a,b,j} g_{b,j} a_j P(a, \text{Yes} | x = j, B, \tau_{b,j}^c) \leq 0, \quad (2)$$

with $g_{b,j}$ being some predetermined weights. Typically, these coefficients can be chosen as the weights of measurement elements for Bob’s observable $B_j = \sum_k g_{b,j} E_{bij}^k$. As the measurement outcome “Yes” is only recorded, Bob’s side allows for extremely low measurement efficiency [11].

The optimal measurement strategy for Bob is to perform a partial Bell state measurement (BSM) $B = \{B_1, I - B_1\}$ where $B_1 = |\Phi^+_d\rangle\langle\Phi^+_d| \equiv |\sum_j |jj\rangle/\sqrt{d}$ models the answer “Yes” and $d$ is the dimension of the Hilbert space of $\{\tau_{b,j}^c\}$ equal to that of Bob’s local system. Indeed, given an arbitrary steerable state, its MDI witness (2) can be constructed from the corresponding witness (1), implying all steerable states are detectable in the MDI manner [5, 6].

![DI verification framework of EPR-steering. The DI protocol is composed of two procedures. One is illustrated in the left side which corresponds to the MDI verification of the state $p_{12}$. In this step, Alice randomly takes measurements $x$ and obtains $a$, while Bob performs one binary measurement on his local system and a set of states $\{\tau_{b,j}^c\}$ assigned from Charlie, and collects the outcome “Yes”. The second is described in the right box, corresponding to the self-testing process. Noting $\tau_{b,j}^c$ can be prepared by Charlie performing local measurements $z_j = \{\tau_{b,j}^c\}$ on Bell state $|\Phi^+_d\rangle$ prepared by Bob and Charlie, this measurement strategy can be self-tested via the violation of Bell inequalities, such as the Bell-CHSH one used in the main text.](image)
forming a certain set of measurements on a specific state, up to some local isometry. Thus, using self-testing to determine the input states $\tau_{b,c}^j$ in Eq. (2), we can obtain a DI steering inequality as

$$W_{DI} = \sum_{a,c,j} g_{c,j} a_j P(a, \text{Yes}, c|x = j, B, z = j) \leq 0. \quad (3)$$

Here Charlie making measurements $z$ and obtaining outcomes $c$ is equivalent to he sending a state $\tau_{b,c}^j$ to Bob, and $g_{c,j}$ are close relate to the weights $g_{b,c,j}$ in Eq. (2). We remark that the self-testing process, involving $|\Phi_j^+\rangle$ and Charlie’s measurements, is not explicitly assessed in the above DI witness (3) and requires a detailed analysis case by case. For example, if dichotomic measurements are chosen, the Clauser-Horne-Shimony-Holt (CHSH) inequality [38] can be used. In the following section, we examine this issue in the case of three dichotomic measurements as per party.

As depicted in Fig. 1, we have established a DI framework to verify EPR-steering. As all pure bipartite entangled states and the associated measurements could be self-tested [39, 40], together with experimental confirmations [41, 42], it is naturally to witness all steerable states via this DI protocol.

IV. THREE MEASUREMENT SETTINGS

If Bob receives $\tau_{b,c}^j = (I + c \sigma_j)/2$ with $c = \pm 1$ and $j = 1, 2, 3$ sent from Charlie where $\sigma_j$ represent three Pauli observables as required in Eq. (2), then they can be self-tested if the following triple Bell-CHSH inequality [8, 36]

$$\mathfrak{B} = E_{1,1} + E_{2,1} + E_{1,2} - E_{2,2} + E_{3,1} + E_{4,1} - E_{3,3} + E_{4,3} + E_{5,2} + E_{6,2} - E_{5,3} + E_{6,3} \quad (4)$$

is maximally violated within quantum theory, where $E_{y,z} = \sum_{b,c=\pm 1} b c p(b, c|y, z)$ refers to the measurement expectations between Bob’s dichotomic measurements $y = 1, 2, \ldots, 6$ and Charlie’s $z = 1, 2, 3$. Specifically, its maximal quantum violation $\mathfrak{B}_{\text{max}} = 6\sqrt{2}$ is achieved at Bob’s six measurements $(\sigma_i \pm \sigma_j)/\sqrt{2}$ with $(i, j) = \{(3, 1), (3, 2), (1, 2)\}$ and Charlie’s $\sigma_1, \pm \sigma_2, \sigma_3$ on $|\Phi_j^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, up to a local unitary. Note that there is a sign problem in the second measurement $\sigma_2$ for Charlie, however, it does not affect its utility in the DI
steering protocol just as the DI entanglement certification [10].

Generally, it is impossible to achieve the perfect self-testing. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$. To evaluate imperfections of the violation bound $6\sqrt{2}$.
The theoretical results while blue dots are the experimental results. By contrast, we also perform the CHSH test to verify quantum steering. It is also interesting to device-independently certify genuine high-dimensional steering and also finds practical applications of self-testing.

There are many interesting open questions left for the future work. For example, the methods in [21, 49] may be used to tolerate more transmission loss and lower measurement efficiency. The resource efficient approach in [50] could also improve the success probability of the partial BSM, and self-testing could be more noise robust by adopting other techniques [7]. Moreover, an alternate DI framework [51] may be possibly used to verify quantum steering. It is also interesting to device-independently certify genuine high-dimensional steering [52] and steering networks [53].

VII. CONCLUSION AND DISCUSSION

We have studied the DI verification of EPR steering and implemented an optical experiment to validate our DI protocol. In principle, we prove that all steerable states, including Bell local states, can be verified device-independently. In practice, we analyse noise robustness towards imperfections of self-testing in the implementation process, and derive a steering inequality as per Eq. (5) for the three-measurement setting case. Finally, we perform a proof of principle experiment to successfully validate our DI steering protocol. We believe that our work paves the way for realistic implementations of secure quantum information processing tasks based on EPR-steering and also finds practical applications of self-testing.

ACKNOWLEDGMENTS

We acknowledge V. Scarani, M. J. W. Hall, Y. Han, and Y. Wang for constructive comments. This work was supported by the National Natural Science Foundation for the Youth of China (No.11704371), China Postdoctoral Science Foundation (No. 2017M612074, BH2030000088), the National Key Research and Development Program of China (No. 2017YFA0301400, 2016YFA0301300, 2016YFA0301700), NSFC (No. 11774335, 11734015, 11504253, 11821404, 11774334, 12134014), the Key Research Program of Frontier Sciences, CAS (No. QYZDY-SSWSLH003), Science Foundation of the CAS (ZDRWXH-2019-1), the Fundamental Research Funds for the Central Universities, USTC Tang Scholarship, and Anhui Initiative in Quantum Information Technologies (No. AHY020100, AHY060300, 2008085J02); Y. Zhao is supported by the Major Key Project of PCL. X. Li and Q. Wen are supported by NSFC (No. 61672110, 61671082, 61976024, 61972048) and the Fundamental Research Funds for the Central Universities (No. 2019XD-A01); S. L. Chen and H. Y. Ku are supported by National Science and Technology Council, Taiwan (Grants Nos. MOST 111-2917-I-564-005 and 111-2112-M-005-107-MY4).
C. Branciard, D. Rosset, Y.-C. Liang, and N. H.-Y. Ku, C.-Y. Hsieh, Shin-Liang Chen, Y.-N. Chen, H. M. Wiseman, S. J. Jones, and A. C. Doherty, Steering, S.-L. Chen, H.-Y. Ku, W. Zhou, J. Tura, and Y.-N. Chen, D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Fryde, Experimental EPR-steering using Bell-local states, Nat. Phys. 6, 845 (2010).

A. J. Bennet, D. A. Evans, D. J. Saunders, C. Branciard, E. G. Cavalcanti, H. M. Wiseman, and G. J. Pryde, Arbitrarily loss-tolerant Einstein-Podolsky-Rosen steering allowing a demonstration over 1 km of optical fiber with no detection loophole, Phys. Rev. X 2, 031003 (2012).

D. H. Smith, G. Gillett, M. de Almeida, C. Branciard, A. Fedrizzi, T. J. Weinhold, A. Lita, B. Calkins, T. Gerrits, H. M. Wiseman, S. W. Nam, and A. G. White, Conclusive quantum steering with superconducting transition-edge sensors, Nat. Commun. 3, 625 (2012).

V. Händchen, T. Eberle, S. Steinlechner, A. Sambowski, T. Franz, R. F. Werner, and R. Schnabel, Observation of one-way Einstein–Podolsky–Rosen steering, Nat. Photonics 6, 596 (2012).

J. Peise, I. Kruse, K. Lange, B. Lücke, L. Pezze, J. Arlt, W. Ertmer, K. Hammerer, L. Santos, A. Smerzi and C. Klempt, Satisfying the Einstein–Podolsky–Rosen criterion with massive particles, Nat. Commun. 6, 8984 (2015).

P. Kunkel, M. Prüfer, H. Strobel, D. Linnemann, A. Fröllian, T. Gasenzer, M. Gärttner and M. K. Oberthaler, Spatially distributed multipartite entanglement enables EPR steering of atomic clouds, Science 360, 413 (2018).

J. Wang, S. Paesani, Y. Ding, R. Santagati, M. G. Thompson, Multidimensional quantum entanglement with large-scale integrated optics, Science, 360, 285 (2018).

M. Fadel, T. Zibold, B. Decamps and P. Treutlein, Spatial entanglement patterns and Einstein-Podolsky-Rosen steering in Bose-Einstein condensates, Science 360, 409 (2018).

E. G. Cavalcanti, M. J. W. Hall, and H. M. Wiseman, Entanglement verification and steering when Alice and Bob cannot be trusted, Phys. Rev. A 87, 032306 (2013).

S. Koësis, M. J. W. Hall, A. J. Bennet, D. J. Saunders, and G. J. Pryde, Experimental measurement-device-independent verification of quantum steering, Nat. Commun. 6 5886 (2015).

I. Jeon, and H. Jeong, Measurement-device-independent and arbitrarily loss-tolerant verification of quantum steering, Phys. Rev. A 99, 012318 (2019).

Y. Guo, S. Cheng, X. Hu, B.-H. Liu, E.-M. Huang, Y.-F. Huang, C.-F. Li, G.-C. Guo, and E. G. Cavalcanti, Experimental Measurement-Device-Independent Quantum Steering and Randomness Generation Beyond Qubits, Phys. Rev. Lett. 123, 170402 (2019).

Y.-Y. Zhao, H.-Y. Ku, S.-L. Chen, F. Nori, Y.-N. Chen, G.-Y. Xiang, C.-F. Li, and G.-C. Guo, Experimental measurement-device-independent measure of quantum steering, NPJ Quantum Inf. 6, 77 (2020).

P. L.-B. Bartosik, A. F. Duccara, T. Purves, and P. Skrzypczyk, Operational Significance of the Quantum Resource Theory of Buscemi Nonlocality, PRX Quantum 2, 020301 (2021).

E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, Experimental criteria for steering and the Einstein-Podolsky-Rosen paradox, Phys. Rev. A 80, 032112 (2009).

V. Scarani, The device-independent outlook on quantum physics, Acta Physica Slovaca 62, 347 (2012).
See Supplemental Material for the derivation of DI steering witness (C1), the self-testing process and the estimated fidelity $f_j$, the nontrivial derivation of the noisy DI steering inequality (5), and the experimental details, including the Ref. [14].

C. Zhang, Y.-F. Huang, Z. Wang, B.-H Liu, C.-F. Li, and G.-C. Guo, Experimental Greenberger-Horne-Zeilinger-type six-photon quantum nonlocality, Phys. Rev. Lett. 115, 260402 (2015).

J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, Phys. Rev. Lett. 24, 549 (1970).

T. H. Yang and M. Navascués, Robust self-testing of unknown quantum systems into any entangled two-qubit states, Phys. Rev. A 87, 050102(R) (2013).

A. Coladangelo, K. T. Goh, V. Scarani, All pure bipartite entangled states can be self-tested, Nat. Commun. 8, 15485 (2017).

W.-H. Zhang, G. Chen, X.-X. Peng, X.-J. Ye, P. Yin, X.-Y. Xu, J.-S. Xu, C.-F. Li, and G.-C. Guo, Experimental realization of robust self-testing of Bell state measurements, Phys. Rev. Lett. 122, 090402 (2019).

W.-H. Zhang, G. Chen, P. Yin, X.-X. Peng, X.-M. Hu, Z.-B. Hou, Z.-Y. Zhou, S. Yu, X.-J. Ye, Z.-Q. Zhou, X.-Y. Xu, J.-S. Tang, J.-S. Xu, Y.-J. Han, B.-H. Liu, C.-F. Li, and G.-C. Guo, Experimental demonstration of robust self-testing for bipartite entangled states, npj Quantum Inf. 5, 4 (2019).

A. Acín, S. Pironio, T. Vértesi, and P. Wittek, Optimal randomness certification from one entangled bit, Phys. Rev. A 93, 040102 (2016).

T. H. Yang, T. Vértesi, J.-D Bancal, V. Scarani, M. Navascués, Robust and versatile black-box certification of quantum devices, Phys. Rev. Lett. 113, 040401 (2014).

J.-D Bancal, M. Navascués, V. Scarani, T. Vértesi, and T. H. Yang, Physical characterization of quantum devices from nonlocal correlations, Phys. Rev. A 91, 022115 (2015).

M. Navascués, S. Pironio and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, New J. Phys., 10, 073013 (2008).

D. J. Saunders, A. J. Bennet, C. Branciard and G. J. Pryde, Experimental demonstration of nonbilocal quantum correlations, Sci. Adv. 3, 1602743 (2017).

T. Vértesi, More efficient Bell inequalities for Werner states, Phys. Rev. A 78, 032112 (2008).

A. Rutkowski, A. Buraczewski, P. Horodecki, and M. Stobińska, Quantum Steering Inequality with Tolerance for Measurement-Setting Errors: Experimentally Feasible Signature of Unbounded Violation, Phys. Rev. Lett. 118, 020402 (2017).

E. Verbanis, A. Martin, D. Rosset, C. C. W. Lim, R. T. Thew, and H. Zbinden, Resource-efficient measurement-device-independent entanglement witness, Phys. Rev. Lett. 116, 190501 (2016).

M. J. W. Hall and A. Rivas, Geometry of joint reality: device-independent steering and operational completeness, Phys. Rev. A 100, 062105 (2019).

S. Designolle, V. Srivastav, R. Uola, N. H. Valencia, W. McCutcheon, M. Malik, and N. Brunner, Genuine High-Dimensional Quantum Steering, Phys. Rev. Lett. 126, 200404 (2021).

B. D.M. Jones, I. Šupić, R. Uola, N. Brunner, and P. Skrzypczyk, Network Quantum Steering, Phys. Rev.
Supplemental material for:
Device-independent verification of Einstein-Podolsky-Rosen steering

In this supplementary material, we give a detailed analysis of fully device-independent (DI) verification of Einstein-Podolsky-Rosen (EPR) steering step by step. First, the standard EPR-steering is introduced and its detection is discussed. Then, we move to measurement-device independent (MDI) verification of EPR-steering, an important step to eliminate the trust in measurement devices with additional assumptions. Further, by using self-testing to remedy above extra assumptions, we arrive at a fully device-independent (DI) verification protocol. Moreover, the noise robustness of our DI steering protocol is analysed, especially robustness of self-testing, and a DI steering inequality is constructed to expose steerability of physical states, which naturally certifies the presence of entanglement within quantum theory. Finally, the optical experimental details to implement the complete DI verification of EPR-steering are presented.

Appendix A: What is EPR-steering?

Suppose that two observers, namely Alice and Bob, make some measurements on a preshared state (they may not have a quantum description). Steering was first introduced by Schrödinger to describe the ability that Alice’s local measurements could prepare Bob’s states remotely [1], and this phenomenon was generalised as EPR -steering by Wiseman et al. [2]. If all follows quantum rules, it has an operational interpretation as an entanglement verification task. Specifically, if Alice’s and Bob’s measurements are labeled as $x$ and $y$ respectively, and the corresponding outcomes $a$ and $b$, this task amounts to checking if the collected statistics $p(a, b|x, y)$ admit a local hidden state (LHS) model in a form of

$$p(a, b|x, y) = \sum_{\lambda} p(\lambda)p(a|x, \lambda)\text{Tr}[E^B_{b,y}\rho^B_\lambda],$$

where the hidden variable $\lambda$ specifies some classical probability distribution $p(a|x, \lambda)$ for Alice and some quantum probability distribution $\text{Tr}[E^B_{b,y}\rho^B_\lambda]$ for Bob which is generated via performing a positive-operator-valued measurement (POVM) $\{E^B_{b,y}\}_{b,y}$ on quantum states $\rho^B_\lambda$ [2]. If there is no such LHS model, then EPR-steering from Alice to Bob is demonstrated.

In principle, every steerable state can be witnessed in an experimental-friendly manner by violating a suitable linear steering inequality of the form [3]

$$W_S = \sum_j \langle a_j B_j \rangle \leq 0,$$  \hspace{1cm} (A2)

where $a_j$ represents the outcome of Alice’s measurement $j$ and Bob’s correlated measurement $j$ has a quantum-mechanical description $B_j$. For example, consider the measurement scenario where Alice and Bob are specified to three dichotomic measurements. If Bob’s measurements are further chosen as mutually unbiased observables, it immediately gives rise to a steering inequality [3]

$$W_S = \langle a_0 \sigma_0 + a_1 \sigma_1 + a_2 \sigma_2 + a_3 \sigma_3 \rangle$$

$$= \langle a_1 \sigma_1 + a_2 \sigma_2 + a_3 \sigma_3 \rangle - \sqrt{3} \leq 0,$$  \hspace{1cm} (A3)

where $\sigma_0 = \mathbb{I}$, $a_0 = -\sqrt{3}$, and operators $\sigma_j$ for $j = 1, 2, 3$ correspond to three Pauli operators $\sigma_x, \sigma_y, \sigma_z$. With respect to the family of Werner states in the main text,

$$\rho = v |\Psi^-_2 \rangle \langle \Psi^-_2 | + (1 - v) \frac{\mathbb{I}}{4}, \quad v \in [0, 1]$$  \hspace{1cm} (A4)

with $|\Psi^-_2 \rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$, it is easy to check that $W_S(\rho) = 3v - \sqrt{3}$. So, if the visibility is larger than the bound $\sqrt{3}/3 \approx 0.577$, i.e., violating this steering inequality, then the steerability of this class of states is exposed.
Given the measurement outcome statistics \( p(a, b|x, y) \) in Eq. (A1), if Alice’s side also admits a quantum description, then the above task reduces to the entanglement verification. In a seminal work \([7]\), Buscemi established a MDI framework to certify all entangled states, in which neither Alice nor Bob is trusted or assumed to follow quantum rules. Indeed, the trust in both sides is completely transferred to a third observer, Charlie say, who could prepare a set of quantum states and then randomly assigns them to either Alice or Bob.

The MDI framework was later extended to EPR-steering \([4]\). Since Alice is already device-independent, Bob’s trust is the only issue to be addressed. In the MDI scenario, Bob and his device are not trusted any more, and thus the quantum probability for Bob in Eq. (A1) and the steering inequality with \( B_j \) as per Eq. (A2) are not applicable neither. It works that Bob is instead specified to a set of quantum states and then randomly assigns them to either Alice or Bob.

For the class of Werner states given in Eq. (A4), when Bob is randomly input to \( W \equiv \{ B_1, \| - B_1 \} \) where \( B_1 = | \Phi^+_d \rangle \langle \Phi^+_d | \) with \( | \Phi^+_d \rangle = \sum_j | j \rangle / \sqrt{d} \) models the answer “Yes” and \( d \) is the dimension of the Hilbert space of \( \{ \tau_{b,j} \} \) equal to that of Bob’s local system. Note that Bob’s observables \( B_j \) in Eq. (A2) could be decomposed into a linear combination of their outcomes which are modelled by elements \( E_{b,j} \) of POVMs, i.e., there is

\[
B_j = \sum_b g_{b,j} E_{b,j}, \quad E_{b,j} \geq 0, \quad \sum_b E_{b,j} = \| I, \tag{B2}
\]

where \( b \) refers to the measurement outcome of \( B_j \). If Alice and Bob share a state \( \rho_{AB} \) to be tested, then the above QRS becomes

\[
W_{QRS} = \sum_{j,a,b} a_j g_{b,j} \text{Tr} \left[ E_{a|j} \otimes B \cdot \rho_{AB} \otimes \tau_{b,j}^T \right] = \frac{1}{d} \sum_{j,a,b} a_j g_{b,j} \text{Tr} \left[ E_{a|j} \otimes \tau_{b,j} \cdot \rho_{AB} \right]. \tag{B3}
\]

Here the measurement element \( E_{a|j} \) describes Alice’s measurement outcome \( a \) given a measurement \( j \). When these input states are chosen as \( \tau_{b,j} = E_{b|j} \) and the predetermined parameters satisfy \( g_{b,j} = g_{b,j} \), it leads to

\[
W_{QRS} = \frac{1}{d} \sum_{j,a} a_j \text{Tr} \left[ E_{a|j} \otimes B_j \rho_{AB} \right] = \frac{1}{d} \sum_j \langle A_j \otimes B_j \rangle = \frac{1}{d} W_S, \tag{B4}
\]

as in the main text, with \( A_j = \sum_a a_j E_{a|j} \). It was shown in \([5, 6]\) that each QRS witness can be constructed from a standard steering inequality as per Eq. (A2), implying that all steerable states can be witnessed in an MDI manner.

For the class of Werner states given in Eq. (A4), when Bob is randomly input to

\[
\tau_{b,j} = \frac{1}{2} (\| + b \sigma_j), \quad b = \pm 1 \tag{B5}
\]

with \( g_{b,j} = b = \pm 1 \) and performs a partial BSM, it is easy to derive that \( W_{QRS}(\rho) = (3\nu - \sqrt{3})/2 \).

**Appendix C: How can we verify EPR-steering device independently?**

It follows from above discussions that in the MDI framework both Alice’s and Bob’s side are already device-independent or trust-free, while the extra trust in the preparation of quantum states \( \{ \tau_{b,j} \} \) by Charlie is still required. Hence, eliminating this trust in Charlie immediately gives rise to a fully DI steering verification. One possible way to addressing this issue is self-testing \([7]\) which refers to a device-independent way to uniquely identify the state and the measurement for uncharacterised quantum devices. As the only information required is the number of measurements, the number of outputs of each measurement, and the outcome statistics, it is thus a completely device-independent process.
As discussed in the main text, in the fully DI verification of EPR-steering framework, we need to collect the measurement statistics to check whether it violates the DI steering inequality

\[ W_{\text{DI}} = \sum_{a,c,j} g_{a,c,j} P(a, \text{Yes}, c | x = j, B, z = j) \leq 0 \]  

(C1)

for the ideal case, given any quantum state \( \rho_{AB} \) to be tested. For example, suppose that Bob is input \( \tau_{b,j} = \frac{1}{2} (I + b \sigma_j) \) with \( b = \pm 1, j = 1, 2, 3 \) randomly from Charlie. Alternate, Bob’s input states could be generated by Charlie performing local measurements described by \( \{ E_{b,j} = \tau_{b,j} \} \) on the Bell state \( |\Phi^+_d \rangle \) shared by Bob and Charlie. Thus, the DI steering inequality (C1) could be expressed in a more explicit form of

\[
W_{\text{DI}} = \sum_{a,b,j} b_j a_j P(a, \text{Yes}, c | x = j, B, z = j) = 
\begin{align*}
&= \sum_{j,a,b} a_j b_j \text{Tr}[E_{a|j} \otimes |\Phi^+_2 \rangle \langle \Phi^+_2|_{BB_0} \otimes (I + b \sigma_j^B) / 2 \cdot \rho_{AB} \otimes |\Phi^+_2 \rangle \langle \Phi^+_2|_{B_0C}] \\
&= \frac{1}{4} \sum_{j,a,b} a_j b_j \text{Tr} [(I + b \sigma_j^B) / 2 \cdot \rho_{AB}] \\
&= \frac{1}{4} \sum_j \langle A_j B_j \rangle = \frac{1}{2} W_{\text{MDI}} = \frac{1}{4} W_S. 
\end{align*}
\]

(C2)

Here \( B_0 \) represents the Bob’s subsystem that \( \tau_{b,j} = \frac{1}{2} (I + b \sigma_j) \).

In particular, these trust input states \( \tau_{b,j} = \frac{1}{2} (I + b \sigma_j) \) for Bob in MDI steering scenario can be replaced by these untrusted observables via self-testing which refers to a device-independent way to uniquely identify the state and the measurement for uncharacterized quantum devices. The virtual protocol that one considers is described as following.

Consider the scenario in which involves two non-communicating parties Bob and Charlie. Each has access to a black box with an underlying state |\( \psi \rangle\). It is accomplished with three Bell-CHSH tests and thus Bob needs to perform the six dichotomic measurements \( y = 1, 2, \ldots, 6 \) and Charlie performs \( z = 1, 2, 3 \). Bob’s inputs and outputs are denoted respectively by \( y \) and \( b \); Charlie’s by \( z \) and \( c \). After a large number of rounds of experiments, the joint probability distribution \( p(b, c | y, z) \) could be reconstructed. Then we are able to construct the triple Bell operator defined in ref. [8]

\[
\mathcal{B} = E_{1,1} + E_{2,1} + E_{1,2} - E_{2,2} + E_{3,1} + E_{4,1} - E_{3,3} + E_{4,3} + E_{5,2} + E_{6,2} - E_{5,3} + E_{6,3}. 
\]

(C3a)

(C3b)

(C3c)

Further, it was proven by Bowles et al. [9] that if the maximal quantum violation \( \mathcal{B} = 6\sqrt{2} \) is observed, then there exists a local auxiliary state \( |00\rangle \in [\mathcal{H}_B \otimes \mathcal{H}_B'] \otimes [\mathcal{H}_C \otimes \mathcal{H}_C'] \) (|00\rangle) is short for |0000\rangle_{B'B'C'C'} \) and a local isometry \( U \) (see Fig. 4) such that

\[
U[M^C_{i} |\psi \rangle \otimes |00\rangle] = |\xi \rangle \otimes \sigma^C_i |\Phi^+_2 \rangle_{B'C'}, \\
U[Y^C_{i} |\psi \rangle \otimes |00\rangle] = |\sigma^C_{0i} \rangle \otimes |\Phi^+_2 \rangle_{B'C'} C', 
\]

where \( M_i \in \{ I, X, Z \}; \sigma_i \in \{ I, \sigma_x, \sigma_z \} \) and \( \langle \xi | \rangle \) is the junk state left in systems \( [\mathcal{H}_B \otimes \mathcal{H}_B'] \otimes [\mathcal{H}_C \otimes \mathcal{H}_C'] \), in the form of

\[
|\xi \rangle = |\xi_0 \rangle_{BC} \otimes |00\rangle_B^{B''C''} + |\xi_1 \rangle_{BC} \otimes |11\rangle_B^{B''C''}. 
\]

(C4)

(C5)

with \( \langle \xi_0 |\xi_0 \rangle + \langle \xi_1 |\xi_1 \rangle = 1 \). It means that we can extract the exact information of the maximally entangled state of two-qubit \( |\Phi^+_2 \rangle \) and Charlie’s three measurements

\[
X^C = \sigma_x, \quad Y^C = \pm \sigma_y, \quad Z^C = \sigma_z, 
\]

(C6)

Although there exists the sign problem of \( \sigma_y \) to be distinguished, it does not pose any constraint to verify entanglement [10] and EPR steering to be discussed.

Note that the measurement set \{\( \sigma_x, \pm \sigma_y, \sigma_z \)\} could be transformed from the set \{\( \sigma_x, \sigma_y, \sigma_z \)\} on which is acted the transpose operation \( T \) because of \( \sigma_y^T = -\sigma_y \). It is easy to verify that the state \( \rho_{AB} \) has a local hidden state (LHS) model with respect to one measurement if and only if it holds for the other measurement set, since the partial
FIG. 4. The local isometry $U$ is explicitly constructed to self-test the singlet state and Pauli operators. The isometry is a virtual protocol, all that must be done in laboratory is to query the boxes and derive $p(b, c | y, z)$.

This again indicates that we can verify all steerable states with a DI protocol. Hence, we can obtain a DI protocol, combining MDI techniques with self-testing, to verify every steerable state.

Appendix D: Robust DI verification of EPR-steering

Ideally, our results derived work well. However, due to imperfections, such as transmission loss or measurement errors, we may collect the noisy data which is usually unable to violate the Bell inequality maximally. Thus the self-testing process is not perfect, and we need to estimate the distance between the observed statistics and the targeted one, a property known as robustness. In this section, we give a detailed analysis of robust self-testing for Pauli observables based on Navascués-Pironio-Acin (NPA) hierarchy and the semi-definite program (SDP). Then, we provide a DI steering inequality, allowing for imperfections of self-testing.

1. Robust self-testing of Pauli observables

In the ideal case, we have constructed a local isometry to certify the two-qubit Bell state $|\Phi^+\rangle$ from the unknown physical state $|\psi\rangle^{BC}$. Similarly, three Pauli observables $\sigma_j, j = 1, 2, 3$ are cast as the state self-testing of $\sigma_j^{BC} |\Phi^+\rangle$ from uncharacterised $M^C |\psi\rangle$, where $M^C \in \{X, Y, Z\}$ is the unknown local operator acting on Charlie. As shown in Fig. 4, this isometry circuit is a swap circuit [11] composed of a set of controlled gates and Hadamard gates. The idea of the swap method is to “swap” out the essential information onto auxiliary systems with the same dimensionality as the local systems of the target state.

We first consider the state $M^C |\psi\rangle^{BC}$ and local auxiliary state $|00\rangle \in \mathcal{H}_{B''} \otimes \mathcal{H}_{C''}$ through the swap gate part in the circuit shown in Fig. 4, which becomes

$$U_{swap} M^C |\psi\rangle^{BC} |00\rangle^{B''C''} = \frac{1}{4} \left( |\mathbb{I} + Z_B | \mathbb{I} + Z_C \rangle M^C |\psi\rangle |00\rangle + X_C (|\mathbb{I} + Z_B \rangle |\mathbb{I} - Z_C \rangle M^C |\psi\rangle |01\rangle + X_B (|\mathbb{I} - Z_B \rangle |\mathbb{I} + Z_C \rangle M^C |\psi\rangle |10\rangle + X_B (|\mathbb{I} - Z_B \rangle X_C (|\mathbb{I} - Z_C \rangle M^C |\psi\rangle |11\rangle \right). \quad (D1)$$

By denoting $|\phi\rangle = U_{swap} M^C |\psi\rangle^{BC} |00\rangle^{B''C''}$, then two Hadamard gates combing with the third pair of controlled
where |±⟩ = |0⟩ ± |1⟩. To extract the information of the trusted auxiliary systems \(B'\) and \(C'\), we take the partial trace of the whole system which be left

\[ \rho_{\text{data}} = \text{Tr}_{BB'CC''}(U \rho_{BC}^0 \langle 00 \rangle \langle 00 \rangle_{BB'CC''} U^\dagger) = \frac{1}{64} \sum_{m,n,k,l\in\{0,1\}} C_{mnkl}^j \langle n \rangle \otimes \langle k \rangle \langle l \rangle, \]

where \(\rho_{BC} = M_j^C \langle \psi \rangle \langle \psi \rangle M_j^{C\dagger}\) describes the density matrix of untrusted operator \(M_j^C\) acting on the uncharacterised state \(\langle \psi \rangle\) and \(C^j\) is the coefficient matrix of \(\rho_{\text{data}}\) with

\[ C_{mnkl}^j = \text{Tr}_{BB'CC''}( (-i Y_B X_B)^m (I + Z_B)^{1-m} (X_B - Z_B X_B)^m (i Y_B X_B)^n (I + Z_B)^{1-n} (X_B - X_B Z_B)^n \]
\[ \otimes (-i X_C Y_C)^k (I + Z_C)^{1-k} (X_C - Z_C X_C)^k (i Y_C X_C)^l (I + Z_C)^{1-l} (X_C - X_C Z_C)^l \rho_{BC}^j). \]

Looking into these single terms, it can be found that for each target Pauli observable, \(\rho_{\text{data}}\) is a 4 × 4 matrix whose entries are linear combinations of expectation values such as \(\langle X_A \rangle, \langle X_A Z_A \rangle, \langle X_A Z_B \rangle, \langle X_A Z_B X_C \rangle\), etc. Then the closeness of \(\rho_{\text{data}}\) to the target state \(\sigma_f^C(\Phi_f^+)^j\) can be then captured by the fidelity

\[ f_j = \langle \Phi_f^+ \rangle \| B' \otimes \sigma_f^C \rho_{\text{data}}^{BC} B' \otimes \sigma_f^C | \Phi_f^+ \rangle, \quad j = 1, 2, 3. \]

Here \(f_j\) is a linear function of two types of operator expectations: some observed behavior and some non-observable correlations which involve different measurements on the same party which are left as variables. We define an average fidelity

\[ \bar{f} = \frac{1}{3} \sum_{j=1,2,3} f_j \]

to evaluate the performance of self-testing. It is worth noting that \(\sigma_x\) and \(-\sigma_x\) have the same fidelity function and thus \(\bar{f}\) for two measurement settings \(\{\sigma_x, \sigma_y, \sigma_z\}\) and \(\{\sigma_x, -\sigma_y, \sigma_z\}\) are identical.

Finally, the fidelity \(f_j, j = 1, 2, 3\) are calculated with the aid of the NPA hierarchy characterization of the quantum behaviors [11–13], and their lower bound can be computed via a SDP:

\[ \begin{align*}
\min & \quad \bar{f} \\
\text{s.t.} & \quad \Gamma \geq 0, \\
& \quad \text{the CHSH operators} \\
& \quad (C3a) = 2.8241, (C3b) = 2.8211, (C3c) = 2.8189, 
\end{align*} \]

where \(\Gamma\) is so-called NPA moment matrix whose rows and columns are numbered by products belonging to \(Q_l\), i.e., \(\Gamma_{ij} = \langle \psi | Q_{i1}^l Q_{j1}^l | \psi \rangle\), and \(Q_l\) is the set of product of \(B_l\) and \(C_l\) and defined as outer approximations of the quantum set (the level of the hierarchy \(l\) is the number of measurements in the product). In our problem, the moment matrix corresponding to \(Q_2\), that is to say the products set is with at most operators per party. To improve the precision of fidelity, we increased the size of the \(\Gamma\) matrix by adding terms such as \(\langle A_1 A_2 A_1 \rangle, \langle A_2 A_1 B_1 \rangle, \langle A_3 B_1 B_2 \rangle, \langle A_3 A_2 A_1 A_3 \rangle, \langle A_2 A_1 A_2 A_1 A_2 \rangle\), et.al. to contain all the average values \(\langle \cdot \rangle\) that appear in the expression of fidelity. It results in the \(\Gamma\) matrix having a size of 101 × 101 whose elements are divided into two kinds that observed behavior variables are real and non-observable variables are complex. The total number of constrains is \(K = 2167\) (28 variables are real and the left are complex). We used the MATLAB modeling language YALMIP and MOSEK as a solver to solve the SDP. According to our experimental results about the violation of the triple Bell-CHSH test, we obtain the average fidelity \(\bar{f} = 0.9995\) and \(f_1 = 0.9994, f_2 = 0.9999, f_3 = 0.9992\) for each Pauli observable.

2. Robust verification of EPR steering

It easily follows from Eq. (D3) that the distance between the pure state estimated from the experimental data via a SDP and the target state satisfies

\[ \| U[MC_j\langle \psi \rangle \langle 00 \rangle] - |\xi \rangle \otimes \sigma_f^C | \Phi_f^+ \rangle_{B'C'} \| = \sqrt{1 - \bar{f}_j}, \]

where the fidelity \(f_j\) is a linear function of two types of operator expectations: some observed behavior and some non-observable correlations which involve different measurements on the same party which are left as variables. We define an average fidelity

\[ \bar{f} = \frac{1}{3} \sum_{j=1,2,3} f_j \]

to evaluate the performance of self-testing. It is worth noting that \(\sigma_x\) and \(-\sigma_x\) have the same fidelity function and thus \(\bar{f}\) for two measurement settings \(\{\sigma_x, \sigma_y, \sigma_z\}\) and \(\{\sigma_x, -\sigma_y, \sigma_z\}\) are identical.

Finally, the fidelity \(f_j, j = 1, 2, 3\) are calculated with the aid of the NPA hierarchy characterization of the quantum behaviors [11–13], and their lower bound can be computed via a SDP:

\[ \begin{align*}
\min & \quad \bar{f} \\
\text{s.t.} & \quad \Gamma \geq 0, \\
& \quad \text{the CHSH operators} \\
& \quad (C3a) = 2.8241, (C3b) = 2.8211, (C3c) = 2.8189, 
\end{align*} \]

where \(\Gamma\) is so-called NPA moment matrix whose rows and columns are numbered by products belonging to \(Q_l\), i.e., \(\Gamma_{ij} = \langle \psi | Q_{i1}^l Q_{j1}^l | \psi \rangle\), and \(Q_l\) is the set of product of \(B_l\) and \(C_l\) and defined as outer approximations of the quantum set (the level of the hierarchy \(l\) is the number of measurements in the product). In our problem, the moment matrix corresponding to \(Q_2\), that is to say the products set is with at most operators per party. To improve the precision of fidelity, we increased the size of the \(\Gamma\) matrix by adding terms such as \(\langle A_1 A_2 A_1 \rangle, \langle A_2 A_1 B_1 \rangle, \langle A_3 B_1 B_2 \rangle, \langle A_3 A_2 A_1 A_3 \rangle, \langle A_2 A_1 A_2 A_1 A_2 \rangle\), et.al. to contain all the average values \(\langle \cdot \rangle\) that appear in the expression of fidelity. It results in the \(\Gamma\) matrix having a size of 101 × 101 whose elements are divided into two kinds that observed behavior variables are real and non-observable variables are complex. The total number of constrains is \(K = 2167\) (28 variables are real and the left are complex). We used the MATLAB modeling language YALMIP and MOSEK as a solver to solve the SDP. According to our experimental results about the violation of the triple Bell-CHSH test, we obtain the average fidelity \(\bar{f} = 0.9995\) and \(f_1 = 0.9994, f_2 = 0.9999, f_3 = 0.9992\) for each Pauli observable.
where \( |00\rangle \in \mathcal{H}_B \otimes \mathcal{H}_B' \otimes [\mathcal{H}_C \otimes \mathcal{H}_C'] \), \( |\xi\rangle \) is defined as in the form of
\[
|\xi\rangle = |\xi_0\rangle^{BC} \otimes |00\rangle^{BC'} + |\xi_1\rangle^{BC} \otimes |11\rangle^{BC'}
\] (D9)
with \( \langle \xi_0 | \xi_0 \rangle + \langle \xi_1 | \xi_1 \rangle = 1 \) and \( \| \cdot \| \) denotes the trace distance. Thus, these fidelity of Pauli observables \( f_j \) and the Bell state \( f_0 \) give us the error estimate when we use the experimental data to do the verification task.

Further, the self-tested pure states in Eq. (D8) could be decomposed as
\[
U[M^\xi_j |\psi\rangle \otimes |00\rangle] = |\xi\rangle \otimes \left( \alpha_j \sigma_j^{BC} |\Phi_2^j\rangle + \sqrt{1 - \alpha_j^2} |\phi_2^j\rangle \right).
\] (D10)
Here the state vector \( |\phi_2^j\rangle \) is orthogonal to \( \sigma_j^{BC} |\Phi_2^j\rangle \) and it is easy to check that \( \alpha_j = \sqrt{f_j} \). For each Pauli observable \( \sigma_j \), the deviation from the density matrices output from the swap circuit is
\[
\Delta_j = \text{Tr}_{BB'CC'} \left( U[M_j^\xi |\psi\rangle \otimes |00\rangle \otimes |U\rangle] - \text{Tr}_{BB'CC'} \left( |\xi\rangle \otimes \sigma_j^{BC} |\Phi_2^j\rangle \langle \Phi_2^j|_{BC'} \right) \left( \Phi_2^j \right) \langle \phi_2^j| \right)
\]
\[
= (\alpha_j^2 - 1) \sigma_j^{BC} |\Phi_2^j\rangle \langle \Phi_2^j| + \alpha_j \sqrt{1 - \alpha_j^2} \sigma_j^{BC} |\Phi_2^j\rangle \langle \phi_2^j| + \alpha_j \sqrt{1 - \alpha_j^2} |\phi_2^j\rangle \langle \phi_2^j|.
\] (D11)
This matrix has two eigenvalues \( \lambda_j = \pm \sqrt{1 - \alpha_j^2} = \pm \sqrt{1 - f_j} \) by solving the following matrix
\[
\Delta_j = \begin{bmatrix}
\alpha_j^2 - 1 & \alpha \sqrt{1 - \alpha_j^2} \\
\alpha \sqrt{1 - \alpha_j^2} & 1 - \alpha_j^2
\end{bmatrix}
\] (D12)
in the basis of \( \{ \sigma_j^{BC} |\Phi_2^j\rangle, |\phi_2^j\rangle \} \). Instead of Charlie’s local measurements \( \sigma_j \) for the ideal case, \( \sigma_j + \Delta_j \) represents the real measurements performed on the Bell state \( |\Phi_2^j\rangle \).

To estimate the lower value of the witness when evaluated on a separable state \( \rho_{AB} = \sum p(\lambda) \langle a_j | \lambda \rho_{AB}^B \rangle \), accounting for the imperfections of self-testing, we are able to derive a steering inequality
\[
W_{\text{DI}}^{\text{noisy}} = \sum_{a,c,j} g_{c,j} a_j P(a, \text{Yes}, c | x = j, B, z = j)
\]
\[
= \sum_{\lambda, a,j} p(\lambda) \langle a_j | \lambda \text{Tr}[\sum c g_{c,j} E_{YES}^{BB} \rho_{AB}^B \otimes \tau_{c,j}]]
\]
\[
= \sum_{\lambda, a,j} p(\lambda) \langle a_j | \lambda \text{Tr}[\sum c E_{YES}^{BB} \rho_{AB}^B \otimes [I + c(\hat{\sigma}_j + \Delta_j)]]/2]
\]
\[
= \sum_{\lambda} p(\lambda) \sum_{a,j} \langle a_j | \lambda \text{Tr}[E_{YES}^{BB} \rho_{AB}^B \otimes (\hat{\sigma}_j + \Delta_j)]
\]
\[
= W_{\text{DI}} + \sum_{\lambda} p(\lambda) \sum_{a,j} \langle a_j | \lambda \text{Tr}[E_{YES}^{BB} \rho_{AB}^B \otimes \Delta_j].
\] (D13)
Here \( E_{YES}^{BB} \) models the answer “Yes” from Bob’s arbitrary joint measurement \( B \), and \( \hat{\sigma} \) denotes the second term in Eq. (S27). The third equality results from the relation \( g_{c,j} = c = \pm 1 \) and \( \tau_{c,j} = \frac{1}{2} (I + c(\hat{\sigma}_j + \Delta_j)) \). If self-testing is perfect, i.e., \( f_j = \alpha_j = 1 \) and thus \( \Delta_j = 0 \), then the above quantity recovers the ideal one \( W_{\text{DI}} \).

Next, we analyse the noise range induced by imperfection of self-testing. Note first that
\[
| \sum_{\lambda} p(\lambda) \sum_{a,j} \langle a_j | \lambda \text{Tr}[E_{YES}^{BB} \rho_{AB}^B \otimes \Delta_j]| \leq \sum_{\lambda} p(\lambda) \sum_{j} | \text{Tr}[E_{YES}^{BB} \rho_{AB}^B \otimes \Delta_j]| \leq \max_{\rho_{AB}} \sum_{j} | \text{Tr}[E_{YES}^{BB} \rho_{AB}^B \otimes \Delta_j]|.
\] (D14)
It follows further from the positivity of the measurement element \( E_{YES}^{BB} \) and states \( \rho_{AB}^B \) that the partial trace \( \rho_{AB}^{B_0} = \text{Tr}_B \left( E_{YES}^{BB} \rho_{AB}^B \otimes I \right) \) must be also a positive matrix. Thus, we are able to obtain
\[
| \text{Tr}[\Delta_j \rho_{AB}^B]| \leq | \lambda_j \cdot \lambda_{\text{max}}(\rho_{AB}^B) | = \sqrt{1 - f_j} \lambda_{\text{max}}(\rho_{AB}^B) \leq \sqrt{1 - f_j}.
\] (D15)
The first inequalities follows from the spectral decomposition of $\Delta_j$ with two eigenvalues $\lambda_j = \pm \sqrt{1 - f_j}$ and there is a
trivial bound 1 for the quantity $\max_{\rho_\lambda} \lambda_{\max}(\rho_\lambda^{B_0})$ or $\max_{\rho_\lambda} ||\text{Tr}_{B_j}...||$, as the eigenvalues of all positive matrices $E^{B_0}_{\text{yes}}$
and $\rho_\lambda$ are no larger than 1. In practice, if $E^{B_0}_{\text{yes}}$ models the “Yes” from Bob’s joint partial BSM $B = \{B_1, \mathbb{I} - B_1\}$, where
$B_1 = |\Phi_2^+\rangle \langle \Phi_2^+ |$ with $|\Phi_2^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, then there is $\max_{\rho_\lambda} \lambda_{\max}(\rho_\lambda^{B_0}) = 1$.

Considering the worst case, we obtain

$$W_{\text{DI}}^{\text{noisy}} \leq W_{\text{DI}} - \max_j \sum_{\rho_\lambda} \lambda_j \max ||\text{Tr}_{B_j}(E^{B_0}_{\text{yes}} \rho_\lambda \otimes \mathbb{I})||_1 = W_{\text{DI}} - \frac{1}{2} \sum_j (\sqrt{1 - f_j}) \leq 0. \quad \text{(D16)}$$

Thus, if $W_{\text{DI}}^{\text{noisy}} > 0$ witnesses steerability conclusively, under the imperfection of self-testing.

For the class of Werner states given as

$$\rho = v |\Psi^-\rangle \langle \Psi^- | + (1 - v) \mathbb{I}, \quad \text{(D17)}$$

the implementation of Bob’s partial BSM leads to

$$W_{\text{DI}}^{\text{noisy}}(\rho) = \frac{1}{4} \left[ 3v - \sqrt{3} \right] - \frac{1}{2} \sum_{j=1,2,3} (\sqrt{1 - f_j}) \leq 0. \quad \text{(D18)}$$

**Appendix E: Experimental details**

In this section, we will give the details about the generation of the photon source, the construction of the partial
BSM and the settings of the wave plates used in the self-testing stage.

**Photon source**- In our experiment, the maximally entangled state $|\Phi_2^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ is prepared through the
SPDC process, where the pump laser has a repetition rate of 80 MHz, a central wavelength of 390 nm, and a pulse
duration of 140 fs. A sandwich-like $\beta$-barium-borate crystal is configured in SPDC and a pair of the YVO4 crystal
and LiNO3 crystal is used for temporal and spatial compensations [14]. To be specific, the computer basis
0, 1 are encoded on the photon’s horizontally polarized direction (H) and vertically polarized direction (V) respectively.

The singlet state $|\Psi_2^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ is prepared by re-encoding one photon’s polarization $H(V)$ as 1(0) for
state $|\Phi_2^+\rangle$ and slightly tilting the temporal compensation crystals YVO4 to add a phase $\pi$. In the experiment, we
simulate the added white noise of the to-be-witnessed system $\rho_{AB}$ by flipping Alice’s measurement, and the noise
level $v$ is roughly estimated by the flipping probability $(1 - v)/2$ [15]. By performing the standard quantum state
tomography, we get the density matrix of the experimentally prepared state, which is approximated to the Werner
state $\rho_W$ with visibility $v$. The real part of density matrices $\rho_{AB}$ and the proximate Werner states are shown in Fig. 5,
and the corresponding fidelities are 0.9993(4), 0.9993(4), 0.9993(4), 0.9988(4), 0.9960(4) and 0.9959(1) respectively.

**Partial BSM**- The measurement bases of BSM are in the form of four Bell states $\{|\Phi_2^\pm\rangle, |\Psi_2^\pm\rangle\}$, where $|\Phi_2^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\Psi_2^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$.

In our experiment, we detect all two-photon coincidence of the eight APDs (D1 D8) in the BSM device, and category
the results into four classes. i) The coincidence happens between (1H, 2H) or (1V, 2V), the BSM resolves the
$|\Phi_2^\pm\rangle$ state. ii) The coincidence happens between (1H, 2V) or (1V, 2H), the BSM resolves the
$|\Psi_2^\pm\rangle$ state. iii) Both the two APDs in one output port fire, the BSM device detects the state $|\Psi_2^\pm\rangle$ or $|\Psi_2^\pm\rangle$, and we can’t tell two states apart.
iv) The coincidence happens between (1H, 1V) or (2H, 2V) are attributed to the high-order emission noise or the
imperfection of the HOM interference.

A standard quantum measurement tomography is performed to estimate the detailed form of the experimentally
implemented BSM. In the process, 36 states, the tensor products of the eigenstates of the Pauli operators $\sigma_x$, $\sigma_y$
and $\sigma_z$ are prepared and sent to our partial BSM module. Then the maximum likelihood method is used to estimate
the POVM elements. The fidelity between the experimentally constructed BSM and the ideal BSM is defined by the
fidelity of quantum state: $F(B^{\sigma_z}, B) = \left( \sum_{j=1}^2 w_j \sqrt{\text{Tr}_j} \right)^2$, where $w_j = \sqrt{\text{Tr}_j \text{Tr}_j} / d_j$, $F_j = F(\tilde{B}_j, \tilde{B}_j)$ is the fidelity
between the normalized BSM elements $\tilde{B}_j$ and $\tilde{B}_j = \frac{\tilde{E}_j}{\text{Tr}_j \text{Tr}_j}$, and $B_j$ is the experimentally implemented
BSM element. In our experiment, the purity of the partial BSM is $F = 0.9831 \pm 0.0040$ and the purity of
$B_1$ is given by $P_1 = \text{Tr}(\tilde{E}_1) = 0.9547$. The estimated forms of the normalized POVM elements $\tilde{B}_j$ are given
in Fig. 6. The main errors are caused by the imperfection of the HOM-type interference, where the photons coming
from different sources are not completely indistinguishable.
FIG. 5. State tomography for Werner states. The real parts of the Werner states are shown as the colorful bars, and the correspondingly theoretical values are as the transparent bars. Each state is constructed from about $9,800,000$ photon pairs.

FIG. 6. Measurement tomography for the partial BSM. The real part of the matrix $\tilde{B}_1^{x}$ (the left histogram) and $\tilde{B}_2^{x}$ (the right histogram) with the ideal theoretical values covered.

| Bob observable | QWP(°) | HWP(°) | Charlie observable | QWP(°) | HWP(°) |
|----------------|--------|--------|---------------------|--------|--------|
| $X+Z$          | 22.5   | 11.25  | $X$                 | 45     | 22.5   |
| $X-Z$          | -22.5  | -56.25 | $Z$                 | 0      | 0      |
| $X+Y$          | 45.00  | 33.75  | $X$                 | 45.00  | 22.50  |
| $X-Y$          | 45.00  | 11.25  | $Y$                 | 0      | 22.5   |
| $Y+Z$          | 0      | 11.45  | $Y$                 | 0      | 22.5   |
| $Y-Z$          | 0      | -56.25 | $Z$                 | 0      | 0      |

TABLE I. Detailed parameters of wave plates set for Charlie and Bob to do self-testing. The $X$, $Y$ and $Z$ denote the Pauli operators $\sigma_x$, $\sigma_y$ and $\sigma_z$, respectively.
Appendix F: In comparison to DI verification of entanglement

By contrast, it was discussed in [9] that to faithfully verify entanglement for Werner states device-independently. One can certify entanglement if

\[ I = \frac{1}{16} \left( (1 - 3v)\eta^2 + 2\eta(1 - \eta) + \frac{1}{4}(1 - \eta)^2 \right) \]

\[ \leq -12\left[ (\sqrt{2(1 - \hat{f})} + 1 - \hat{f})^2 + \sqrt{2(1 - \hat{f})} + (1 - \hat{f}) \right], \]

where \( \eta \) is the visibility of preparing the Bell state \(|\Phi^+\rangle\) being self-tested, and we use average fidelity \( \hat{f} = 1 - \theta^2 \) to replace the original one obtained in [9]. The fidelity required to verify entanglement for different values of \( \eta \) with \( v = 0.6 \) and \( 0.7 \) is plotted in Fig. 7. It is obvious that even for \( \eta = 1 \), it requires extremely high fidelity, i.e. \( \hat{f} > 0.99999 \) for \( v = 0.6 \) and \( \hat{f} > 0.99998 \) for \( v = 0.7 \) which are hard to realize in experiments, while our result derived in Eq. (D18) allows the fidelity of around 0.997, which is a significant reduction and attainable in current experiments.

![Fig. 7. The average fidelity of self-testing for DI verification of entanglement of Werner states with \( v = 0.6 \) and 0.7 derived in [9]. The fidelity of Pauli observables requires near-perfect self-testing to faithfully complete DI verification task, which is hard to reach within current technology.](image-url)

[1] E. Schrödinger, Discussion of probability relations between separated systems. Proc. Cambridge. Philos. Soc. 31, 555 (1935).
[2] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox, Phys. Rev. Lett. 98, 140402 (2007).
[3] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, Experimental criteria for steering and the Einstein-Podolsky-Rosen paradox, Phys. Rev. A 80, 032112 (2009).
[4] E. G. Cavalcanti, M. J. W. Hall, and H. M. Wiseman, Entanglement verification and steering when Alice and Bob cannot be trusted, Phys. Rev. A 87, 032306 (2013).
[5] S. Kocsis, M. J. W. Hall, A. J. Bennet, D. J. Saunders, and G. J. Pryde, Experimental measurement-device-independent verification of quantum steering, Nat. Commun. 6 5886 (2015).
[6] Y. Guo, S. Cheng, X. Hu, B.-H. Liu, E.-M. Huang, Y.-F. Huang, C.-F. Li, G.-C. Guo, and E. G. Cavalcanti, Experimental Measurement-Device-Independent Quantum Steering and Randomness Generation Beyond Qubits, Phys. Rev. Lett. 123, 170402 (2019).
[7] I. Šupić and J. Bowles, Self-testing of quantum systems: a review, Quantum 4, 339 (2020).
[8] A. Acín, S. Pironio, T. Vertesi, and P. Wittek, Optimal randomness certification from one entangled bit, Phys. Rev. A 93, 040102 (2016).
[9] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín, Self-testing of Pauli observables for device-independent entanglement certification, Phys. Rev. A 98, 042336 (2018).
[10] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín, Device-Independent entanglement certification of all entangled states, Phys. Rev. Lett. 121, 180503 (2018).
[11] T. H. Yang, T. Vértesi, J.-D Bancal, V. Scarani, M. Navascués, Robust and versatile black-box certification of quantum devices, Phys. Rev. Lett. 113, 040401 (2014).
[12] M. Navascués, S. Pironio and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, New J. Phys., 10, 073013 (2008).
[13] J.-D Bancal, M. Navascués, V. Scarani, T. Vértesi, and T. H. Yang, Physical characterization of quantum devices from nonlocal correlations, Phys. Rev. A 91, 022115 (2015).
[14] C. Zhang, Y.-F. Huang, Z. Wang, B.-H Liu, C.-F. Li, and G.-C. Guo, Experimental Greenberger-Horne-Zeilinger-type six-photon quantum nonlocality, Phys. Rev. Lett. 115, 260402 (2015).
[15] D. J. Saunders, A. J. Bennet, C. Branciard and G. J. Pryde, Experimental demonstration of nonbilocal quantum correlations, Sci. Adv. 3, 1602743 (2017).