Quantum networks self-test all entangled states

Ivan Šupić1, Joseph Bowles2, Marc-Olivier Renou2, Antonio Acín2,3 & Matty J. Hoban4

Certifying quantum properties with minimal assumptions is a fundamental problem in quantum information science. Self-testing is a method to infer the underlying physics of a quantum experiment only from the measured statistics1,2. Although all bipartite pure entangled states can be self-tested3, little is known about how to self-test quantum states of an arbitrary number of systems. Here we introduce a framework of network-assisted self-testing and use it to self-test any pure entangled quantum state of an arbitrary number of systems. The scheme requires the preparation of a number of singlets that scales linearly with the number of systems, and the implementation of standard projective and Bell measurements, all feasible with current technology4. When all the network constraints are exploited, the obtained self-testing certification is stronger than what is achievable in any Bell-type scenario. Our work shows how properly designed networks offer new opportunities for the certification of quantum phenomena.

The difficulty in classically simulating quantum systems requires radically new avenues for information processing, and this difficulty even becomes an impossibility when causality constraints are imposed, such as in a Bell test5. These new possibilities bring challenges, as experimental demonstrations require a very precise control of the quantum devices involved. It is therefore crucial for the development of quantum information technologies to design tools to certify the correct functioning of complex quantum devices using our limited classical information processing capabilities6.

A ubiquitous form of certification is to determine that a system is in a particular quantum state. Standard state tomography7,8 achieves this by performing measurements on the system to certify and compare the obtained results with the predictions from the Born rule. This method is described as ‘device-dependent’, as it assumes that measurements are perfectly characterized (an unrealistic assumption in many set-ups). Measurements can also be certified device-dependently, through the preparation of, in turn, perfectly characterized quantum states, introducing a form of circularity in the procedure. The strongest form of device certification should then minimize the assumptions made: it should be based solely on experimental data and make very few assumptions about the devices involved, without requiring any detailed characterization of them. To attain this form of certification the ‘device-independent’ framework9–11, in which quantum devices are modelled as uncharacterized ‘black boxes’ with only classical interaction (inputs and outputs) with these boxes, offers a solution. Being a data-driven framework, to certify genuine quantum properties in the device-independent approach it is necessary to observe statistics without any classical analogue (for example, correlations violating a Bell inequality).

Self-testing pushes device-independent quantum certification to its strongest form; modulo some symmetries inherent to the device-independent framework, self-testing protocols certify the precise form of the quantum state and/or quantum measurements only from the statistics they generate1,2. The concept of self-testing was introduced in ref.1 (see also ref.12, and ref.13 for a precursor result) and relies on a standard Bell test in which local measurements are performed on an entangled state. The authors of ref.1 showed the existence of statistics (correlations) such that black boxes reproducing them must essentially prepare the maximally entangled state $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. These

1CNRS, LIP6, Sorbonne Université, Paris, France. 2ICFO – Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, Castelldefels, Barcelona, Spain. 3ICREA – Institució Catalana de Recerca i Estudis Avançats, Barcelona, Spain. 4Quantinuum, Oxford, UK. E-mail: matty.hoban@quantinuum.com
Bell correlations therefore self-test the state $|\phi^+\rangle$. These seminal works open a new research programme: what is the ultimate power of self-testing? In particular, can one design self-testing protocols for any quantum state? This question has remained open for more than 20 years. In a seminal result, Coladangelo and colleagues showed that all pure bipartite states can be self-tested\(^1\). In the general multipartite case, however, and despite partial progress for some restricted families of states\(^2\)–\(^9\), little is known. This should not come as a surprise, as entanglement is much richer and harder to characterize in the multipartite case.

In this Letter we answer this question by providing a self-testing protocol for any pure state of an arbitrary number of qubits. Our protocol easily generalizes to arbitrary local dimensions. To prove our results, we introduce the concept of ‘network-assisted self-testing’, in which a network made of non-trusted states and measurements is employed to self-test a target quantum device. We first show how to self-test a generic pure state of $N$ qubits using a network structure that utilizes $N$ additional maximally entangled states, standard Pauli single-particle measurements and two-particle Bell measurements, all of which are within experimental reach. This result is obtained under standard self-testing assumptions, that is, without assuming the causal constraints associated with the network geometry. Considering these additional constraints, we also show how our results imply a type of certification that is strictly stronger than any possible in standard self-testing.

At a high level, our protocol can be understood as transforming a standard local tomography protocol, in which $N$ main parties characterize a pure state with trusted measurements, into a fully device-independent protocol, by adding $N$ maximally entangled states and $N$ auxiliary parties in a network structure. This is achieved in three steps: (1) transform the tomography protocol into a measurement-device-independent protocol, using trusted quantum inputs, inspired from refs.\(^{10\)–\(^12\}; (2) use remote state preparation\(^{13\)–\(^15\)} to prepare the trusted inputs, adding maximally entangled states and an additional auxiliary party for each main party sharing the state to be self-tested; (3) generate statistics between each of the $N$ auxiliary/main party pairs that self-test the measurements needed for the remote state preparation. This results in a fully device-independent protocol that self-tests the presence of the multipartite state.

**Standard self-testing**

Self-testing aims at characterizing the informational content of quantum devices. It is defined in a standard Bell test in which an $N$-party state is distributed among $N$ observers who can run $m$ possible measurements of $r$ possible results. We label the choice of measurement by each party by $x_i = 1, \ldots, m$, and the obtained result by $a_i = 1, \ldots, r$, with $i = 1, \ldots, N$. The resulting statistics is described by the conditioned probability distribution $P(a_1\ldots a_N|x_1\ldots x_N)$, which we simply dub as correlations. In a quantum realization, these observed correlations read

$$P(a_1\ldots a_N|x_1\ldots x_N) = Tr(\rho \cdot M_{a_1|x_1} \otimes \ldots \otimes M_{a_N|x_N})$$

where $\rho$ denotes the states shared by the $N$ observers and $M_{a_i|x_i}$ the positive operators defining their local measurements. This assumption about the probabilities in equation (1) is often made in the device-independent setting, and it can be enforced through separating and screening-off devices from one another to prevent communication or crosstalk. The goal of self-testing is to certify the state and/or measurements in equation (1) only from the observed correlations. This is done in the device-independent scenario, assuming the validity of equation (1) but without invoking any assumptions on the state and measurements appearing in it. In particular, the dimension is not fixed, and as a result the state in equation (1) is taken to be pure, $\rho = |\psi_N\rangle \langle \psi_N|$. It is also standard to assume that measurements are projective, as correlations from arbitrary measurements can be simulated by projective measurements. To arrive at the correlations in equation (1) there is also the assumption of independent, identically distributed (i.i.d.) rounds, that is, that in each run of the experiment the state and measurement operators are the same. This is a standard assumption, although some recent works have proven self-testing results in a non-i.i.d. framework\(^{17\)–\(^20\)}.

The device-independent formulation of self-testing has important consequences. First, self-testing is limited to pure states. Second, the state can only be specified modulo some unavoidable symmetries. For example, a local rotation (or unitary) of one part of the state, compensated by a rotation of the corresponding measurement device, results in the same statistics. Also, a source creating extra unmeasured degrees of freedom produces the same statistics. Moreover, one cannot discriminate between a given quantum realization and its complex conjugate: they also lead to the same statistics. The formal definition of state self-testing we use in this work takes into account all these facts as follows.

**Definition 1.** (State self-testing.) A state $|\psi_N\rangle$ can be self-tested if there exist correlations $P(a_1\ldots a_N|x_1\ldots x_N)$ such that for any quantum realization of them, there exists a set of $N$ local quantum maps $T_1, \ldots, T_N$ that, when applied to the unknown state of the system, extract the state

$$|\psi'\rangle = \sqrt{a}|\psi_N\rangle \otimes |\psi_N\rangle + \sqrt{1-a}|\psi_N\rangle \otimes |\psi_N\rangle$$

for some unknown $a \in [0,1]$. Operationally, this definition implies that from the measurement statistics one can conclude that the target state $|\psi_N\rangle$ can be extracted from the underlying state in the experiment. This extraction procedure is defined by a set of $N$ local quantum channels, that is, deterministic quantum operations that can be physically realized. Importantly, these channels describing the extraction do not need to be implemented. All that is required is a proof that such channels exist, implying the target state can be extracted. The extraction procedure takes care of the freedom inherent to self-testing in unmeasured additional degrees of freedom or local rotations. The symmetry with respect to complex conjugation is reflected by the unknown linear combination of the target state and its complex conjugate with auxiliary systems appearing in the definition of the extracted state $|\psi'\rangle$. In fact, the correlations derived when making local measurements $M_{a_i|x_i}$ on $|\psi_N\rangle$ can also be obtained by making local measurements $M_{a_i|x_i} \otimes (|0\rangle \langle 0| + |F\rangle \langle F|) \otimes |1\rangle \langle 1|$ on $|\psi'\rangle$ independently of $a$. Extracting state $|\psi'\rangle$ is in principle the most one can hope for when using only the observed correlations in the Bell test. Note that in the particular case of bipartite systems, the issue with complex conjugation does not appear because every pure state is real when rotated to its Schmidt decomposition; that is, one can always take $a = 1$ as in ref.\(^{20\).}

**Network-assisted self-testing**

Our work is based on the idea that networks provide new avenues for quantum certification. For that, we introduce the framework of network-assisted self-testing, as well as fully network-assisted self-testing. In the latter case additional network constraints are assumed. The general idea of the framework is to construct a network of $M \geq N$ parties and use it to generate statistics that guarantees the presence of the target state $|\psi_N\rangle$ in the network. The first variant of the network-assisted framework is very similar to the standard Bell scenario and assumes that the generated statistics has the same form as in equation (1), now for a system made of $M$ particles.

**Definition 2.** (Network-assisted self-testing.) A state $|\psi_N\rangle$ can be self-tested in a network of $M \geq N$ parties if there exist quantum correlations $P(a_1\ldots a_N|x_1\ldots x_N)$ such that, for any $M$-party quantum realization of them, there exists a set of $N$ local quantum maps $T_1, \ldots, T_N$ that, when
applied to a subset of \(N\) parties of the unknown state of the system, extract the state
\[
|\psi_N^a\rangle = \sqrt{\alpha} |\psi_N\rangle |0\rangle^\otimes N + \sqrt{1-\alpha} |\psi_N^a\rangle |1\rangle^\otimes N
\]
for some unknown \(\alpha \in [0,1]\).

This definition is illustrated in Fig. 1. Note that network-assisted self-testing includes standard self-testing by taking \(M = N\). Again, a self-testing statement in terms of \(|\psi_N\rangle\) is the most one can hope for if the only assumption is that the observed correlations have the form of equation (1). We can now present the first main result of our work.

**Theorem 1.** Any \(N\)-party pure state \(|\psi_N\rangle\) can be self-tested according to Definition 2 in a network involving \(M = 2N\) parties assisted by \(N\) maximally entangled states.

The network used to prove the theorem is shown in Fig. 2a. It consists of \(M = 2N\) parties, where each local, main party of \(|\psi_N\rangle\) shares a maximally entangled state of dimension \(2^k\) with an additional auxiliary party. Here, \(k\) is the smallest integer such that \(2^k\) is larger than the local Hilbert space dimension of \(|\psi_N\rangle\).

The proof of the theorem for arbitrary multipartite states is provided in the Supplementary Information. Here we provide the basic intuition behind the construction of the network-assisted self-testing protocol for multi-qubit states. The ingredients in the proof are presented in Fig. 3. The idea is to tune a standard device-dependent tomography process, where measurements are characterized and trusted, into a self-testing protocol in which the measurements are not characterized. To do so, we introduce \(N\) auxiliary parties that each share a maximally entangled state with one of the original \(N\) main parties; the main parties now have two systems. Each auxiliary and main party performs local measurements that maximally violate three different Clauser–Horne–Shimony–Holt (CHSH) \(^{27}\) Bell inequalities, which self-tests their shared maximally entangled state. The maximally entangled state can now be seen as a resource for essentially teleporting the initial local state of each main party to an auxiliary system. To perform this teleportation, a Bell measurement can be performed at each of the main parties. In addition to the measurements self-testing the maximally entangled state, the auxiliary parties perform tomographically complete measurements, and thus tomography is performed on these teleported states. Recall that tomography defines a one-to-one map between probabilities and states using trusted measurements. Thus, once we remove the trust on the measurements, we now have a one-to-one map between the observed correlations and the state \(|\psi_N\rangle\), always up to the relevant symmetries.

The proof for states of arbitrary local dimension is conceptually similar, where a maximally entangled state of larger dimension is used to teleport the state, and tensor products of Pauli operators are self-tested to perform the tomography (Supplementary Section F).

One can also see the protocol as consisting of two games. The first game (based on the CHSH Bell inequalities) tests that each main and auxiliary party share a maximally entangled state and perform the correct measurements for tomography. The second game occurs when the Bell measurement is performed at each party, and tests if the teleported state gives the correct statistics for tomography. Because the auxiliary parties are unaware whether the Bell measurement is performed or not, this forces them to play fairly, as an attempt to cheat at the second game would jeopardize the score of the first game. The first game for self-testing (multiple copies of) the maximally entangled state is one such game\(^{28}\) in the wider literature\(^{29,30,31}\), but it is particularly useful for us as it self-tests all Pauli observables for an arbitrary number of qubits.

**Fully network-assisted self-testing**

Remarkably, the use of networks allows for the introduction of another form of self-testing protocol. This second variant exploits the fact that, in a general network scenario, there may be causal constraints enforced by the network geometry that are not covered by equation (1). In particular, the network may consist of independent preparations of quantum states, which imply that not only the measurements but also the state in the network has a tensor-product form. Such source independence assumptions are common in the study of network non-locality (see refs. \(^{15,16,18}\), and ref. \(^{17}\) for a review). For example, if the network consists of two states prepared by two independent sources, as in a standard entanglement-swapping experiment, the network state is the tensor product of the two preparations. These constraints are also natural in the network of Fig. 2b, but were not used in the proof of Theorem 1, which simply assumes the validity of equation (1). In general, when also enforcing the independent-preparation constraints, the correlations in a network have the form
\[
P(a_1...a_M|x_1...x_M) = \text{Tr}_i \left( \rho_i \otimes \prod_j M_{a_j|x_j} \right)
\]
where we slightly abuse the notation and simply represent the independence constraints of the states and measurements in the network by the generic tensor products. The fact that the constraints on the observed correlations (equation (4)) are now stronger than those associated to the Bell tests used in standard self-testing (equation (1)) opens the possibility of stronger self-testing statements. In particular, using state-independence constraints it may be possible to exclude all the fully correlated states in \(|\psi_N^a\rangle\) and restrict the extraction process to the two extreme non-correlated cases \(\alpha = 0, 1\), that is, the target state or its complex conjugate. This idea was recently used to prove the necessity of complex numbers in quantum theory\(^{29}\). All these considerations lead to the following stronger definition of network-assisted self-testing, which is impossible when using standard Bell tests.

**Definition 3.** (Fully network-assisted self-testing.) A state \(|\psi_N\rangle\) can be self-tested in a network of \(M \geq N\) parties if there exist quantum correlations \(P(a_1...a_M|x_1...x_M)\) respecting the network independence constraints such that, for any \(M\)-partite quantum realization of them, there exists...
Fig. 2 | The network scenarios used to self-test any pure state $|\psi_N\rangle$. a, For network-assisted self-testing of $|\psi_N\rangle$, the network has $M = 2N$ parties, composed of $N$ main parties $A_1, \ldots, A_N$, each being assisted by an auxiliary party $B_1, \ldots, B_N$ (here $N = 6$). To establish the self-testing correlations, the main parties (holding the state $|\psi\rangle$ to be self-tested) each share an additionally maximally entangled state with their corresponding auxiliary party. By making joint measurements at the main parties, one can show that the resulting correlations imply the existence of local channels that extract the state $|\psi_6\rangle$ (for some $a$) from these devices. b, The network scenario we use to prove fully network-assisted self-testing (Theorem 2). Here, we have only a single auxiliary party that receives input $y = (y_1, \ldots, y_6)$ and outputs $b = (b_1, \ldots, b_6)$. The measurement strategy used to establish the self-testing correlations is the same as in a, where now all the auxiliary parties are grouped together. Assuming the independence of the sources defined by this network structure, we can prove that the extracted state must be $|\psi_N\rangle$ or its complex conjugate.

Fig. 3 | The ingredients required for our self-testing protocols. a, d. We start with quantum state tomography (a), and by adapting the set-up we end up in the self-testing scenario (d), where we wish to perform the same task as tomography but through an uncharacterized set-up. Characterized, or trusted, devices (in green) are eventually replaced with uncharacterized, or untrusted devices (in black). a, Local tomography: by measuring the three (characterized) Pauli operators $\sigma_x, \sigma_y, \sigma_z$, we characterize a state $|\psi_N\rangle$ shared among $N$ parties (of which two are shown here). b, Measurement-device-independent (MDI) tomography: this modification of tomography removes the assumption that measurement devices are perfectly characterized, and introduces auxiliary systems in informationally complete single-qubit states, for example, the eigenstates of the three Pauli operators. If Bell-state measurements (BSM) are performed, this is equivalent to tomography, but a priori we do not need to assume this. c, MDI tomography assisted with remote state preparation (RSP): the auxiliary states used in MDI tomography can be obtained by measuring one half of a maximally entangled system. The reduced post-measurement state is thus informationally complete. d, Network self-testing: the characterized devices in MDI tomography with RSP are replaced with an initially uncharacterized measurement device and bipartite system shared between an original node and an auxiliary node. The maximally entangled two-qubit state and Pauli measurements on one qubit are then self-tested: for this we use maximal violations of three different CHSH inequalities, as shown in the Supplementary Information. A priori characterization is thus now unnecessary.

a set of $N$ local quantum maps $\tau_0, \ldots, \tau_y$ that when applied to a subset of $N$ parties of the unknown state of the system extract either the state $|\psi_N\rangle$ or $|\psi_N^*\rangle$.

Our second main result is to prove that all states can also be self-tested according to this stronger definition.

**Theorem 2.** Any $N$-party pure state $|\psi_N\rangle$ can be self-tested according to Definition 3 in a network involving $M = N + 1$ parties assisted with $N$ maximally entangled states.

The proof is given in the Supplementary Information but the idea behind is intuitive. The network is similar to the one used in the proof
of Theorem 1, but now the independence constraints are also enforced upon the states. Because this independence is assumed, in some sense, we do not need to separate out each system into an individual node. That is, there is no need to have $N$ auxiliary nodes as in Fig. 1, and they can now be grouped into a single node sharing the $N$ maximally entangled states with the $N$ systems in $|\psi\rangle$ (this weaker assumption is theoretically interesting, but might not be relevant in practical implementations). The resulting network is shown in Fig. 2b.

**Discussion**

Let us conclude this Letter with several remarks. Our protocol is the same for any state, and consists of a fixed structure into which any pure state can be plugged. The number of auxiliary systems required to self-test an $N$-partite state scales linearly in $N$, and the protocol is composed of the same repeated element for each subsystem. Importantly, in practice, the devices utilized in our modular scheme, namely maximallyentangled states and Bell measurements, are some of the most elementary building blocks of the quantum internet. Hence, our protocol is particularly appealing for practical purposes. The numbers of measurements at each party required to certify a multipartite state of local dimension $d$ are $3^d$ and $6^d + 3$ for the auxiliary and main parties, respectively, where $n$ is the smallest integer such that $d \geq 2$. Although our work applies to any state, for a given pure state one could replace tomography by any other, possibly more efficient, device-dependent certification procedure that establishes a one-to-one map between probabilities and the target pure state.

After presenting the first proof that all pure entangled states can be self-tested, the next important step is to explore how robust to noise our self-testing procedure is. Self-testing of tensor products of maximally entangled pairs is known to be robust to noise. The main task is to explore the robustness to noise of MDI self-testing, that is, how to perform self-testing if the quantum inputs are not fully characterized. Also, the proposition stated and proved in Supplementary Section D should be made robust to noise. In one particular direction, it would be useful to adapt the well-known numerical SWAP technique to our scenario [26], so that numerical bounds on robustness could be found. This could then lead to new, practical device-independent protocols for quantum key distribution and verifiable distributed quantum computation [14, 15], especially those requiring multipartite states [46].

**Online content**

Any methods, additional references, Nature Portfolio reporting summaries, source data, extended data, supplementary information, acknowledgements, peer review information; details of author contributions and competing interests; and statements of data and code availability are available at https://doi.org/10.1038/s41567-023-01945-4.

**References**

1. Mayers, D. & Yao, A. Self testing quantum apparatus. Quantum Info. Comput. 4, 273–286 (2004).
2. Šupić, I. & Bowles, J. Self-testing of quantum systems: a review. Quantum 4, 337 (2020).
3. Coladangelo, A., Goh, K. T. & Scarani, V. All pure bipartite entangled states can be self-tested. Nat. Commun. 8, 15485 (2017).
4. Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: a vision for the road ahead. Science 362, eaam9288 (2018).
5. Bell, J. S. On the Einstein Podolsky Rosen paradox. Physics 1, 195–200 (1964).
6. Eisert, J. et al. Quantum certification and benchmarking. Nat. Rev. Phys. 2, 382–390 (2020).
7. Fano, U. Description of states in quantum mechanics by density matrix and operator techniques. Rev. Mod. Phys. 29, 74–93 (1957).
8. Vogel, K. & Risken, H. Determination of quasiprobability distributions in terms of probability distributions for the rotated quadrature phase. Phys. Rev. A 40, 2847–2849 (1989).
9. Acin, A. et al. Device-independent security of quantum cryptography against collective attacks. Phys. Rev. Lett. 98, 230501 (2007).
10. Pironio, S. et al. Device-independent quantum key distribution secure against collective attacks. New J. Phys. 11, 045021 (2009).
11. Colbeck, R. Quantum and Relativistic Protocols for Secure Multi-Party Computation. PhD thesis, Univ. Cambridge (2006); https://arxiv.org/abs/0911.3814
12. Mayers, D. & Yao, A. Quantum cryptography with imperfect apparatus. In Proc. 39th Annual Symposium on Foundations of Computer Science (cat. no. 98C38280) 503–509 (IEEE, 1998); https://doi.org/10.1109/sfcs.1998.743501
13. Summers, S. J. & Werner, R. Maximal violation of Bell’s inequalities is generic in quantum field theory. Commun. Math. Phys. 110, 247–259 (1987).
14. McGague, M. Self-testing graph states. In Revised Selected Papers of the 6th Conference on Theory of Quantum Computation, Communication, and Cryptography Vol. 6745 (eds Bacon, D. et al.) 104–120 (Springer, 2011); https://doi.org/10.1007/978-3-642-54429-3_7
15. Wu, X. et al. Robust self-testing of the three-qubit W state. Phys. Rev. A 90, 042339 (2014).
16. Pál, K. F., Vértesi, T. & Navascués, M. Device-independent tomography of multipartite quantum states. Phys. Rev. A 90, 042340 (2014).
17. Šupić, I., Coladangelo, A., Augusiak, R. & Acín, A. Self-testing multipartite entangled states through projections onto two systems. N. J. Phys. 20, 083041 (2018).
18. Baccari, F., Augusiak, R., Šupić, I., Tura, J. & Acín, A. Scalable Bell inequalities for qubit graph states and robust self-testing. Phys. Rev. Lett. 124, 020402 (2020).
19. Buscemi, F. All entangled quantum states are nonlocal. Phys. Rev. Lett. 108, 200401 (2012).
20. Branciard, C., Rosset, D., Liang, Y.-C. & Gisin, N. Measurement-device-independent entanglement witnesses for all entangled quantum states. Phys. Rev. Lett. 110, 060405 (2013).
21. Šupić, I., Hoban, M. J., Colomer, L. D. & Acín, A. Self-testing and certification using trusted quantum inputs. New J. Phys. 22, 073006 (2020).
22. Bennett, C. H. et al. Remote state preparation. Phys. Rev. Lett. 87, 077902 (2001).
23. Berry, D. W. & Sanders, B. C. Optimal remote state preparation. Phys. Rev. Lett. 90, 057901 (2003).
24. Bancal, J.-D., Redeker, K., Sekatski, P., Rosenfeld, W. & Sangouard, N. Self-testing with finite statistics enabling the certification of a quantum network link. Quantum 5, 401 (2021).
25. Gočanin, A., Šupić, I. & Dakić, B. Sample-efficient device-independent quantum state verification and certification. PRX Quantum 3, 010317 (2022).
26. 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).
27. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. Phys. Rev. Lett. 23, 880–884 (1969).
28. Bowles, J., Šupić, I., Cavalcanti, D. & Acín, A. Self-testing of Pauli observables for device-independent entanglement certification. Phys. Rev. A 98, 042336 (2018).
29. Wu, X., Bancal, J.-D., McGague, M. & Scarani, V. Device-independent parallel self-testing of two singlets. Phys. Rev. A 93, 062121 (2016).
30. Coudron, M. & Natarajan, A. The parallel-repeated magic square game is rigid. Preprint at https://arxiv.org/abs/1609.06306 (2016).
31. McKague, M. Self-testing in parallel with CHSH. Quantum 1, 1 (2017).
32. Natarajan, A. & Vidick, T. A quantum linearity test for robustly verifying entanglement. In Proc. 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017 1003–1015 (Association for Computing Machinery, 2017); https://doi.org/10.1145/3055399.3055468
33. Branciard, C., Gisin, N. & Pironio, S. Characterizing the nonlocal correlations created via entanglement swapping. Phys. Rev. Lett. 104, 170401 (2010).
34. Fritz, T. Beyond Bell’s Theorem II: scenarios with arbitrary causal structure. Commun. Math. Phys. 341, 391–434 (2015).
35. Renou, M.-O. et al. Genuine quantum nonlocality in the triangle network. Phys. Rev. Lett. 123, 140401 (2019).
36. Šupić, I., Bancal, J.-D. & Brunner, N. Quantum nonlocality in networks can be demonstrated with an arbitrarily small level of independence between the sources. Phys. Rev. Lett. 125, 240403 (2020).
37. Tavakoli, A., Pozas-Kerstjens, A., Luo, M.-X. & Renou, M.-O. Bell nonlocality in networks. Rep. Prog. Phys. 85, 056001 (2022).
38. Renou, M.-O. et al. Quantum theory based on real numbers can be experimentally falsified. Nature 600, 625–629 (2021).
39. Bădescu, C., O’Donnell, R. & Wright, J. Quantum state certification. In Proc. 51st Annual ACM SIGACT Symposium on Theory of Computing, STOC 2019, 503–514 (Association for Computing Machinery, 2019); https://doi.org/10.1145/3313276.3316344
40. Bancal, J.-D., Sangouard, N. & Sekatski, P. Noise-resistant device-independent certification of Bell state measurements. Phys. Rev. Lett. 121, 250506 (2018).
41. Renou, M.-O., Kaniewski, J. & Brunner, N. Self-testing entangled measurements in quantum networks. Phys. Rev. Lett. 121, 250507 (2018).
42. Morris, J., Saggio, V., Gočanin, A. & Dakić, B. Quantum verification and estimation with few copies. Adv. Quantum Technol. 5, 2100118 (2022).
43. 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).
44. Reichhardt, B. W., Unger, F. & Vazirani, U. Classical command of quantum systems. Nature 496, 456–460 (2013).
45. Coladangelo, A., Grilo, A. B., Jeffery, S. & Vidick, T. Verifier-on-a-leash: new schemes for verifiable delegated quantum computation, with quasilinear resources. In Advances in Cryptology – EUROCRYPT 2019 (eds Ishai, Y. & Rijmen, V.) 247–277 (Springer, 2019).
46. McKague, M. Interactive proofs for BQP via self-tested graph states. Theory Comput. 12, 1–42 (2016).

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

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

© The Author(s), under exclusive licence to Springer Nature Limited 2023
Data availability
This work does not have any associated data.

Acknowledgements
This work was funded by the ERC through grants QUSCO (I.Š.) and AdG CERQUTE, (A.A.), grant PCI2021-122022-2B financed by MCIN/AEI/10.13039/501100011033 (M.-O.R.), the European Union Next Generation EU/PRTR (M.-O.R.), a Swiss National Fund Early Mobility Grant P2GEP2_19144 (M.-O.R.), a FQXi large grant FQXi-RFP-18038 (M.J.H.), the Government of Spain through grants FIS2020-TRANQI (A.A.), Retos Quispin (A.A.), NexGen Funds (A.A.) and Severo Ochoa CEX2019-000910-S (A.A.), Fundacio Cellex (A.A.), Fundacio Mir-Puig, (A.A.), Generalitat de Catalunya through grants CERCA (A.A.), the QuantERA II Programme through grant Veriqtas (A.A.), and QuantumCAT (A.A.), and the AXA Chair in Quantum Information Science (A.A.).

Author contributions
All authors contributed equally to this work.

Competing interests
The authors declare no competing interests.

Additional information
Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41567-023-01945-4.

Correspondence and requests for materials should be addressed to Matty J. Hoban.

Peer review information Nature Physics thanks Anna Pappa, Arthur Mehta and Petros Wallden for their contribution to the peer review of this work.

Reprints and permissions information is available at www.nature.com/reprints.