Zhang et al. *Light: Science & Applications* (2021)10:169
https://doi.org/10.1038/s41377-021-00608-4

Official journal of the CIOMP 2047-7538
www.nature.com/lsa

ARTICLE Open Access

Quantum verification of NP problems with single photons and linear optics

Aonan Zhang[1,2], Hao Zhan[1,2], Junjie Liao[1,2], Kaimin Zheng[1,2], Tao Jiang[1,2], Minghao Mi[1,2], Penghui Yao[3]✉ and Lijian Zhang[1,2]✉

Abstract

Quantum computing is seeking to realize hardware-optimized algorithms for application-related computational tasks. NP (nondeterministic-polynomial-time) is a complexity class containing many important but intractable problems like the satisfiability of potentially conflict constraints (SAT). According to the well-founded exponential time hypothesis, verifying an SAT instance of size n requires generally the complete solution in an $O(n)$-bit proof. In contrast, quantum verification algorithms, which encode the solution into quantum bits rather than classical bit strings, can perform the verification task with quadratically reduced information about the solution in $\tilde{O}(\sqrt{n})$ qubits. Here we realize the quantum verification machine of SAT with single photons and linear optics. By using tunable optical setups, we efficiently verify satisfiable and unsatisfiable SAT instances and achieve a clear completeness-soundness gap even in the presence of experimental imperfections. The protocol requires only unentangled photons, linear operations on multiple modes and at most two-photon joint measurements. These features make the protocol suitable for photonic realization and scalable to large problem sizes with the advances in high-dimensional quantum information manipulation and large scale linear-optical systems. Our results open an essentially new route toward quantum advantages and extend the computational capability of optical quantum computing.

Introduction

Quantum computing has been found to unprecedentedly speed-up classically intractable computational tasks[1–7]. As building universal, error-corrected quantum computers is still challenging, the community now seeks practical uses of noisy intermediate-scale quantum (NISQ) technologies in computational problems of interest and importance[5]. Photonics has been a versatile tool in quantum information tasks[8–10] such as boson sampling[7,11–14], quantum walk[9,15,16], and variational quantum simulation[17,18]. By utilizing multi-degrees of freedom of photons[19,20] and well-developed linear optics[21–24], information can be encoded and processed in a high-dimensional Hilbert space. These features make photonics a suitable platform to realize quantum algorithms involving high-dimensional encoding, low degree of entanglement, and linear operations. Here we exploit the advantages of photonics to realize a new regime of quantum algorithm—the quantum verification machine (QVM) of nondeterministic polynomial-time (NP) problems.

The complexity class NP, which is the set of decision problems verifiable in polynomial time by a deterministic Turing machine, encompasses many natural decision and optimization problems. By definition, NP can be abstracted as a proof system which models computation as exchange of messages between the prover and the verifier. Verifying the correctness of a proof is a foundational computational model underpinning both the complexity theory and applications such as delegated

Correspondence: Penghui Yao (pyao@nju.edu.cn) or
Lijian Zhang (lijian.zhang@nju.edu.cn)
[1]National Laboratory of Solid State Microstructures, Key Laboratory of Intelligent Optical Sensing and Manipulation (Ministry of Education) and College of Engineering and Applied Sciences, Nanjing University, 210093 Nanjing, China
[2]Collaborative Innovation Center of Advanced Microstructures, Nanjing University, 210093 Nanjing, China
Full list of author information is available at the end of the article

computation. Specifically, we focus on the verification of the first discovered and most extensively studied NP-complete problem—the Boolean satisfiability problem (SAT)[25], that is, the problem of asking whether a given Boolean formula with n variables has a satisfying assignment. The NP-completeness signifies that any NP problem can be efficiently reduced to this problem. Corresponding to the problem of satisfying potentially conflict constraints, SAT has found numerous applications in circuit design, mode checking, automated proving and artificial intelligence[26]. Under the widely believed exponential time hypothesis (ETH)[27], which asserts that the best algorithm for solving 3-SAT (a representative form of SAT) runs in time $2^{\gamma n}$ for some constant $\gamma > 0$, verifying 3-SAT requires at least $O(n)$ bits. Otherwise the verifier can simply enumerate overall possible proofs, which yield a sub-exponential algorithm for solving 3-SAT. Surprisingly, this bound on proof length no longer applies if quantum bits are used in proofs and verified by quantum computers. This perception rapidly aroused substantial efforts on quantum verification of NP(-complete) problems[28–35]. In this line, Aaronson et al. proposed a protocol of proving 3-SAT with $O(\sqrt{n})$ unentangled quantum states each of $O(\log n)$ qubits[28] and variants of the protocol have also been developed[30,32]. However, to date a complete demonstration of quantum verification algorithm is still missing.

In this work, we report the first experimental quantum verification of SAT with single photons and linear optics, by implementing a modified version of recent proposals[34]. We present a scalable design of reconfigurable optical circuits in which quantum proofs are mapped to single photons distributed in optical modes. The experiment demonstrates faithful verification of NP problems in terms of a complete analysis on the satisfiable instance, unsatisfiable instance and cheating prover cases. Our work links the remarkable proof systems in computer science to the manipulation and detection of photons, which foreshadows further investigations of a variety of computational models in the photonic regime.

Results

Quantum verification algorithm of the satisfiability problem

An instance of SAT is formalized as the conjunction of a set of clauses $\phi = c_1 \wedge c_2 ... \wedge c_j$, each of which is the disjunction of a set of literals $l_1 \vee l_2 ... \vee l_m$. A literal could be a variable x_i or a negation of a variable $\neg x_i$. In 3-SAT instances, each clause has exactly three literals. The quantum verification of 3-SAT corresponds to the complexity class Quantum Merlin-Arthur [QMA(K)], as the quantum analogue of NP[36–38]. In this scheme, K non-communicating, omniscient provers (called Merlins) send K unentangled quantum proofs to a skeptical, computationally bounded verifier Arthur to convince Arthur the instance is satisfiable (see Fig. 1a). Arthur checks the proof in his computing machines and decide whether to accept or reject the proof. Two properties are required in a QMA protocol: (i) *Completeness*: if the instance is satisfiable, there exist a proof such that Arthur accepts with at least some high probability c; (ii) *Soundness*: if the instance is not satisfiable, for any proof Arthur accepts with at most some probability s.

The protocol firstly reduces the 3-SAT instance to a 2-out-of-4 SAT instance where each clause contains four variables x_i, x_j, x_k, x_l and is satisfied if two of them are true, i.e., $x_i + x_j + x_k\_x_l = 2$. In the verification, Merlins are supposed to send Arthur $K = O(\sqrt{n})$ identical, unentangled quantum states[28], each of the form

$$|\psi\rangle = \frac{1}{\sqrt{n}} \sum\nolimits_{i=1}^{n} (-1)^{x_i} |i\rangle \tag{1}$$

where $|i\rangle = \hat{a}_i^\dagger |0\rangle$ and $\hat{a}_i^\dagger$ is the creation operator on mode i. Here $x_1, x_2, ..., x_n \in \{0,1\}^n$ is an assignment of the n variables. A state of such form is called a proper state. The n-dimensional quantum state can be equivalently described by $\log n$ qubits revealing at most $\log n$ bits information by measurements on the state. To check whether the assignment x satisfies the clauses, Arthur can choose some clauses (i,j,k,l) at random and measure the K copies of $|\psi\rangle$ in a basis with a projection on $|c\rangle = (|i\rangle + |j\rangle + |k\rangle + |l\rangle)/2$ for each clause. For each copy Arthur will get a probability of observing the outcome $|c\rangle$

$$p_c = |\langle c|\psi\rangle|^2 = [(-1)^{x_i} + (-1)^{x_j} + (-1)^{x_k} + (-1)^{x_l}]^2/4n$$

Then Arthur rejects the proof if he gets the outcome $|c\rangle$ for at least one copy and accepts it otherwise. With this *Satisfiability Test*, Arthur will have $p_c = 0$ if $x_i + x_j + x_k + x_l = 2$, and some constant nonzero probability otherwise. An issue is that Merlins may cheat Arthur by sending him improper state, for example concentrating the amplitude in a subset of the basis $\{|i\rangle\}$ such that the *Satisfiability Test* passes even the instance is not satisfiable. To tackle this problem Arthur can perform *Uniformity Test*: he randomly chooses a matching M on the set $\{1,...,n\}$ such that the set is partitioned into $n/2$ groups of the form (i,j), then measures each copy of the state $|\psi\rangle$ in the basis with $\{|i\rangle + |j\rangle, |i\rangle - |j\rangle\}$ for each $(i,j) \in M$. Only if the state is proper (i.e., the amplitudes are equal), one of the two outcomes will never occur. With the statistics on the outcomes, Arthur rejects the proof if two outcomes $\{|i\rangle + |j\rangle, |i\rangle - |j\rangle\}$ both occur for a same $(i,j) \in M$. Here the K copies are used to obtain sufficient statistics on the outcomes to make a decision.

As the verification requires multiple copies of the state, another possible way for Merlins to cheat is to send

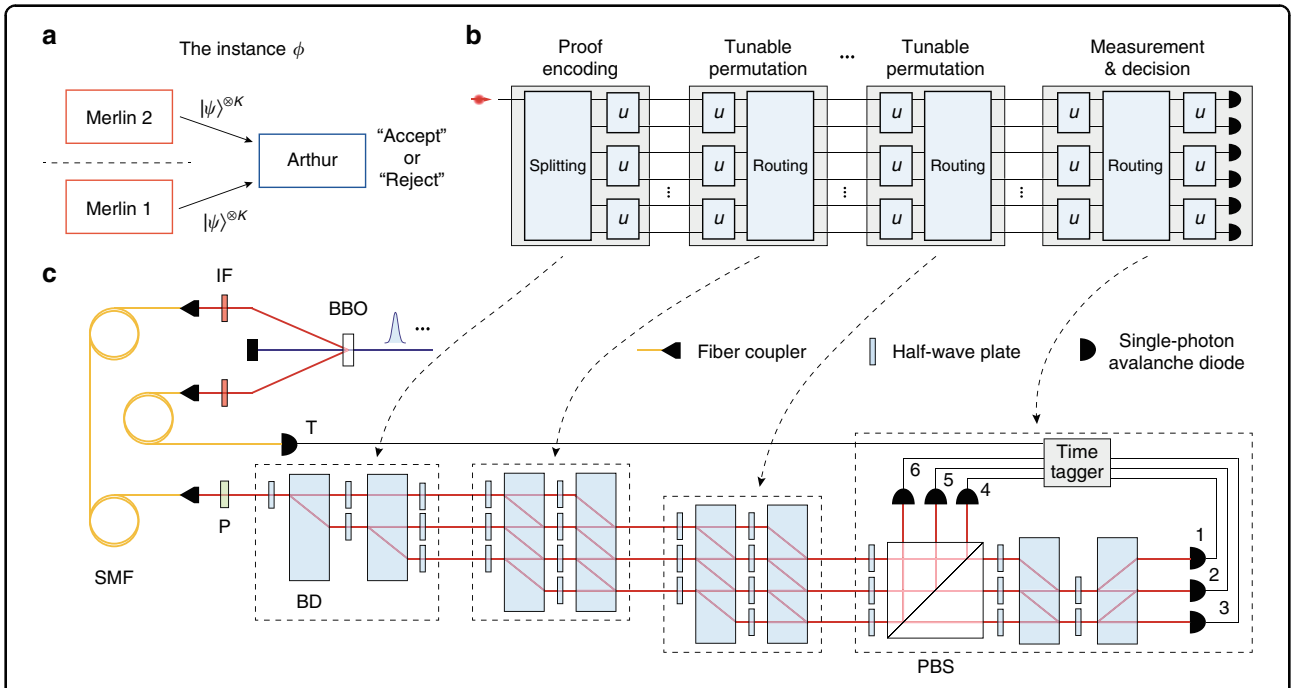

Fig. 1 Quantum verification machine. a The two-prover Quantum Merlin-Arthur protocol [QMA(2)]. On the basis of the given SAT instance, the two Merlins send unentangled, identical proof states to Arthur, who checks the proof on his quantum computer and makes an "accept" or "reject" decision. **b** The architecture of quantum circuit for the satisfiability and uniformity test. The design comprises proof encoding, tunable permutations and measurement on the modes. These operations are mainly based on tunable two-mode transformations *u* combined with mode splitting and routing. With the input of single photons, the circuit can verify the satisfiability of a set of clauses or the uniformity on random matchings. **c** Experimental setup for the satisfiability test and uniformity test. Merlins prepare single photons distributed in the polarization and path modes, encoding the assignment in the single-photon states as quantum witnesses. Arthur then applies permutations and interferences on these modes with linear optics. Note only states from one Merlin are required for the two tests. The output modes are detected by single-photon avalanche diodes (SPADs) and registered by a time tagger. BBO β-barium borate crystal, BD calcite beam displacer, P polarizer, IF interference filter, SMF single mode fibre, PBS polarizing beam-splitter.

different states rather than identical copies. For this reason, Arthur performs *Symmetry Test*: a swap test between two states, which accepts with certainty if the two states are identical and has a constant probability to reject when the two-state overlap is under a certain threshold. The QMA(K) protocol may be significantly reduced by simulating the K Merlins with a single Merlin who sends a product state of the K copies $|\psi\rangle^{\otimes K}$, yet in this case Arthur needs to guarantee the unentanglement among the K subsystems. To this end Arthur can ask for the proof state $|\psi\rangle^{\otimes K} \in \mathbb{C}_d^{\otimes K}$ from another Merlin and conduct a *Product Test*[32], which applies the swap test to each of the K pairs of corresponding subsystems of the two states. The proof will be accepted if all the swap tests pass and rejected otherwise. With the help of the product test, we can simulate the K-prover protocol with only two Merlins, which corresponds to the complexity result $\mathrm{QMA}(K) = \mathrm{QMA}(2)$ for $K \geq 2$ [32].

Overall, Arthur performs one of the four aforementioned tests with constant probability (e.g., 1/4 each). As a consequence, we have an efficient quantum algorithm to verify SAT with perfect completeness and constant soundness, using two unentangled proofs of length $O(\sqrt{n}\log n)$ qubits (see Materials and methods for a summary of the protocol).

Photonic implementation of the quantum verification machine

To realize the verification algorithm in photonic regime, we devise optical circuits for the four tests and experimentally implement the circuit in the case $n = 6$. The proofs from the two Merlins are unentangled photons generated by a parametric down-conversion process while the K copies of the state $|\psi\rangle$ correspond to photons generated sequentially at different time. In our experiment the K copies sent by a same Merlin are identical due to the fact that the apparatus to prepare the states is fixed within the duration of the experiment. For each copy we encode the n-dimensional quantum state in the polarization and path degrees of freedom of the photon. The optical modes $\{|1\rangle, |2\rangle, |3\rangle, |4\rangle, ..., |n\rangle\}$ are mapped to $\{|h_1\rangle, |v_1\rangle, |h_2\rangle, |v_2\rangle, ..., |v_{n/2}\rangle\}$, where $|h_j\rangle$ ($|v_j\rangle$) denotes the horizontal (vertical) polarization in path j. In the following we use $|x_1\, x_2\, x_3\, x_4\, x_5\, x_6\rangle$ to represent a proper state given in Eq. (1) encoding the assignment $x_1\, x_2\, x_3\, x_4\, x_5\, x_6$. When $x_i = 0$ the phase on mode i is 0, whereas $x_i = 1$ the phase is π.

Figure 1b depicts the circuit design for the satisfiability test and uniformity test. The circuit comprises a sequence of stages, each of which involves a set of two-mode configurable transformations u combined with mode splitting or routing (see Materials and methods for details). Starting from proof encoding, Merlin firstly splits the input single photon into an equal superposition over n modes and encodes the assignment x into the K copies of the state. Each state is then sent to successive tunable permutation modules, which select the modes corresponding to the chosen clause (i,j,k,l) or group the modes into a random matching M. Finally, the measurement and decision module performs either projection on the certain state $|c\rangle$ or two-mode interferences on the certain matching M. The two-mode transformations u are implemented by half-wave plates (see Fig. 1c), of which the optical axes can be set in different angles to perform different two-mode sub-operations such as Pauli-X, Pauli-Z and Hadamard gates

$$X=\frac{1}{\sqrt{n}}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, Z=\frac{1}{\sqrt{n}}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, H=\frac{1}{\sqrt{2n}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

With appropriate configurations of these gates, the circuit can perform different permutations and interferences on the optical modes. The ability of the permutation stage is to sort the modes into groups (2 or 4 modes each, without regard to order). Configurations of the optical circuit are designed to realize the $\binom{6}{4}=15$ projections and the $\binom{6}{2}\times\binom{4}{2}\div 3!=15$ matchings. The measurement outcome is read out by single-photon avalanche diodes and we register the measurement outcome for each copy of the proof state with a multi-channel time tagger. For a single trial of the test, a decision on the proof ("reject" or "accept") is made based on the detector pattern of K copies: for the satisfiability test, whether the detector corresponding to the projector $|c\rangle\langle c|$ clicks; for the uniformity test, whether the two detectors in a same group (i,j) both click.

Quantum verification of SAT instances with linear optics

Firstly we demonstrate the performance of the verifier in the satisfiability and uniformity tests. By changing the settings of the wave plates to prepare the 64 proper states and verify the 15 clauses, we measure the probabilities p_c for all the 64×15 cases (Fig. 2a), which are consistent with the theoretical satisfiability of the clauses (Fig. 2b). The satisfying proofs manifest nearly zero outcome probabilities (0.28% in average), whereas all the unsatisfying proofs manifest significant outcome probabilities exceeding the probabilities of the satisfying cases by two orders of magnitude (larger than 13.47%). Regarding the uniformity test, we show the rejection probabilities when testing the 64 proper states for the 15 matchings with $K=3$ in Fig. 2c. The results exhibit a high probability of 98.67% to accept in average. For the

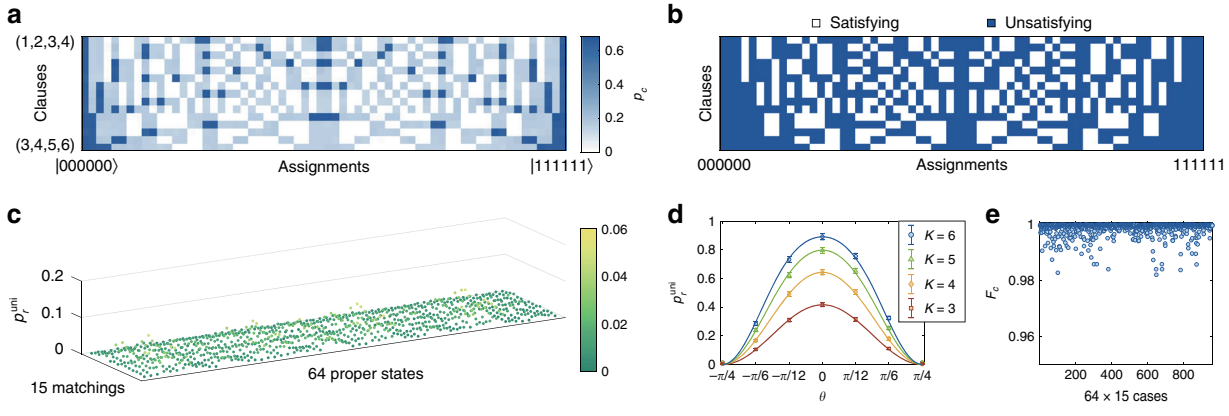

Fig. 2 Validation of the satisfiablity test and uniformity test. a The experimentally measured projection probabilities p_c when verifying the 15 clauses (rows) with the 64 proper states (columns). Here the proof states from left to right are $|000000\rangle$,$|100000\rangle$...,$|111111\rangle$, while the verified clauses from top to down are (1,2,3,4),(1,2,3,5)...,(3,4,5,6). (i,j,k,l) denotes the clause $x_i+x_j+x_k+x_l=2$. **b** The satisfiability of the 15 clauses for the 64 assignments. An assignment x may satisfies (white) or unsatisfies (blue) a certain clause. **c** The measured rejection probabilities p_r^{uni} of the uniformity test for the 64 proper states × 15 matchings when the number of copies $K=3$. **d** The rejection probability p_r^{uni} of the uniformity test for improper states of the form $|\psi_{\mathrm{im}}(\theta)\rangle=(\cos\theta,\sin\theta,\cos\theta,\sin\theta,\cos\theta,\sin\theta)/\sqrt{3}$. Here we take the results for the matching {(1,2),(3,4),(5,6)} under different numbers of copies as an example. For each θ we run the test 5000 times and collect the measurement outcomes of $5000\times K$ photons to acquire the rejection probability p_r^{uni}. The results given by numerical simulations are shown as solid lines. Error bars are uncertainties assuming Poisson count statistics. **e** The statistical fidelities $\mathcal{F}_c=\left(\sqrt{p_c^{\mathrm{the}}p_c^{\mathrm{exp}}}+\sqrt{(1-p_c^{\mathrm{the}})(1-p_c^{\mathrm{exp}})}\right)^2$ between the theoretical probabilities p_c^{the} and experimental probabilities p_c^{exp} for the 64×15 cases of the satisfiability test.

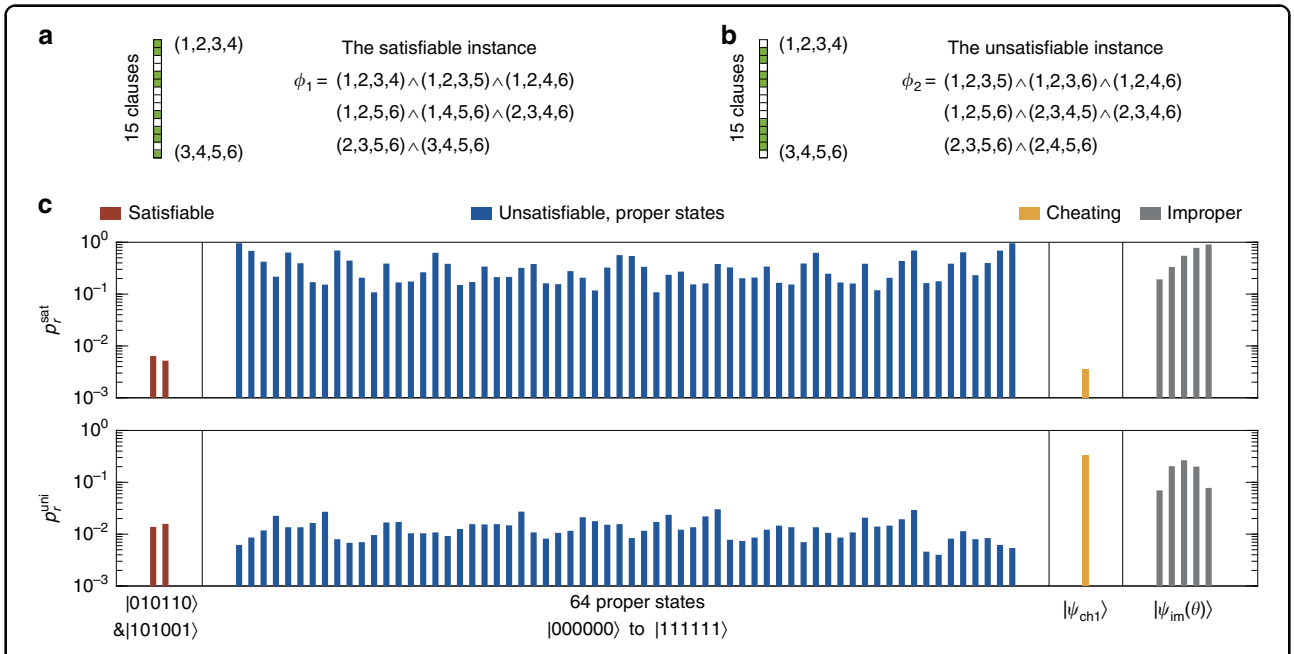

Fig. 3 Experimental verification of SAT instances. a The satisfiable instance ϕ_1. **b** The unsatisfiable instance ϕ_2. The shaded squares (green) illustrate which 8 of the 15 clauses are chosen in the instance. **c** The rejection probabilities of the satisfiability test (p_r^{sat}, top) and uniformity test (p_r^{uni}, down) for different proof states. For the satisfiable instance ϕ_1, Merlins will send proof states encoding the correct solution thus we show the results for the two satisfying proof states (red bars). For the unsatisfiable instance ϕ_2, we test different cases consisting of sending the 64 proper states (blue bars), a deliberate cheating state $|\psi_{ch1}\rangle$ in order to pass the satisfiability test (yellow bars), and improper states $|\psi_{im}(\theta)\rangle$ (gray bars). The number of copies $K = 3$ is adopted in the verification and the rejection probabilities are obtained by repeating each test 5000 times.

case that Merlins send improper states, we run the uniformity test for proof states of the form $|\psi_{im}(\theta)\rangle = (\cos\theta, \sin\theta, \cos\theta, \sin\theta, \cos\theta, \sin\theta)/\sqrt{3}$ with different numbers of copies $K = 3,4,5,6$ (Fig. 2d). Here $(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6)$ denotes a state with complex amplitudes α_i in mode $|i\rangle$, i.e., $\sum_{i=1}^{n} \alpha_i |i\rangle$. An increase in the rejection probability is observed with the transition from proper states to highly improper states, which fits the numerical simulations. On the other hand, higher rejection probabilities are obtained for improper states when increasing the number of copies K. In addition, we determine the average statistical fidelity $\mathcal{F}_c = \left(\sqrt{p_c^{the} p_c^{exp}} + \sqrt{(1-p_c^{the})(1-p_c^{exp})}\right)^2$ between the theoretical and experimental projection probabilities (p_c^{the} and p_c^{exp}) to be 0.9988 ± 0.0024 (see Fig. 2e), which justifies the excellent agreements between experimental results and theoretical calculations.

To demonstrate the verification of specific instances, we concentrate on the instances including eight clauses, in which there are $\binom{15}{8} = 6435$ instances. According to the satisfiability of the clauses (Fig. 2b), 90 instances are satisfiable (each with two solutions) and 6345 instances are unsatisfiable. Figure 3 visualizes the results of verifying a satisfiable instance ϕ_1 (illustrated in Fig. 3a) and an unsatisfiable instance ϕ_2 (illustrated in Fig. 3b). As Merlins aim to make Arthur accept the proof, for the satisfiable instance ϕ_1 Merlins will honestly send the proof encoding one of the two satisfying assignments. In this case the proof states successfully pass both tests with high probabilities ($p_r^{sat} = 0.64\%$ and $p_r^{uni} = 1.31\%$, averaging over the two states), as shown in Fig. 3c.

For the unsatisfiable instance ϕ_2, we consider situations where Merlins send different types of states (Fig. 3c). Firstly we perform the two tests with all the 64 proper states. The verifier attains rejection probabilities p_r^{sat} larger than 11.50% and up to 95.72% in the satisfiability test although these proofs could probably pass the uniformity test ($p_r^{uni} = 1.30\%$ averaging over the 64 proper states). Secondly we realize cheating Merlins by sending deliberately designed improper states in order to pass the satisfiability test. As an example, we construct the state $|\psi_{ch1}\rangle = (1, -3, 1, 1, 1, 1)/\sqrt{14}$ (as well as $|\psi_{ch2}\rangle = (-3, 1, 1, 1, 1, 1)/\sqrt{14}$ for instances given in the Supplementary Information), for which the projection probability p_c of verifying any of the eight clauses in ϕ_2 theoretically equals zero. Consequently, $|\psi_{ch1}\rangle$ reaches a rejection probability $p_r^{sat} = 0.44\%$ of the same order of magnitude as in the satisfiable case. Nevertheless, Arthur

can detect the cheating with the help of the uniformity test, in which a rejection probability of 31.90% is obtained. This result justifies the necessity of the uniformity test. Finally the verification is also executed by sending just improper states $|\psi_{\mathrm{im}}(\theta)\rangle$ with $\theta = \{-\pi/6, -\pi/12, 0, \pi/12, \pi/6\}$, which exhibit considerable rejection probabilities in both tests. We conclude from the results that for all the three cases, evident rejection probabilities are observed in at least one of the two tests. The typical realizations indicate close to perfect completeness and constant soundness and thereby experimentally achieve a clear completeness-soundness gap for the quantum verification (see Supplementary Information for more examples and results). Experimental imperfections, including the limited interference visibilities, phase fluctuations and errors in the operations, lead to deviations of the outcome probabilities from ideal ones for the satisfying proof states and thereby imperfect completeness for the protocol. In real-world applications of the QVM, of particular importance is the amplification of the completeness-soundness gap. For this reason we also demonstrate the amplification of the success probability for the instances ϕ_1 and ϕ_2, of which the protocol and results are given in the Supplementary Information.

The symmetry test and the product test require optical swap test[39], which can be implemented with a multi-mode Hong–Ou–Mandel (HOM) interference (Fig. 4a)[40]. Our experiment uses a non-polarizing beam-splitter (NPBS) to perform the two-photon interferences on the six optical modes distributed in both polarization and path degrees of freedom. In the optical swap test, the probability of rejection is $p_r^{\mathrm{swap}} = (1 - |\langle\psi_1|\psi_2\rangle|^2)/2$, where $|\psi_1\rangle$ and $|\psi_2\rangle$ are the photonic states in the two input ports of the NPBS. We register all the $\binom{6}{2} = 15$ coincidence channels, in which the six one-side channels (the two photons are detected in the same output port of the NPBS) correspond to the "accept" outcome and the nine two-side channels (the two photons are detected in different output ports of the NPBS) correspond to the "reject" outcome. We change the path difference between the two states with a delay line and observe the high-dimensional two-photon HOM interference. The HOM interference of identical proper states (Fig. 4b) manifests peaks for the "accept" outcomes and dips for the "reject" outcomes, resulting in a high acceptance probability of (97.48 ± 0.56)%. This result guarantees a high probability to accept

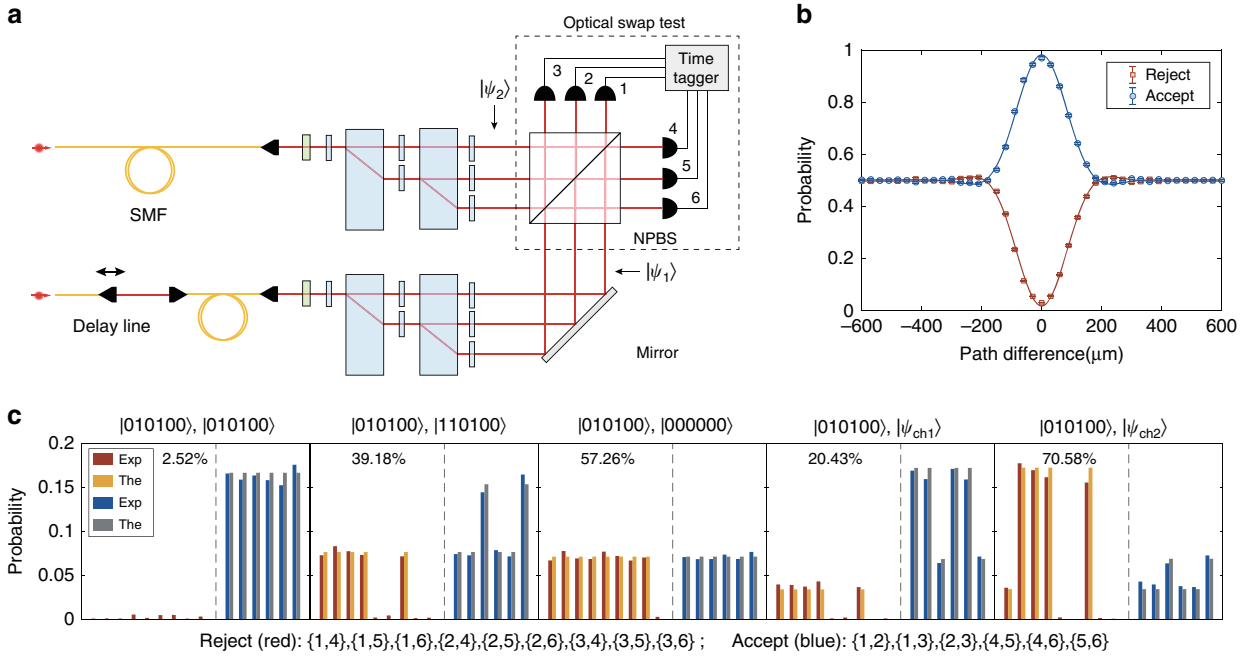

Fig. 4 The optical swap test. a Experimental scheme. Two single photons are injected into the setup and prepared as two quantum proofs $|\psi_1\rangle$ and $|\psi_2\rangle$. The two states $|\psi_1\rangle$ and $|\psi_2\rangle$ are interfered at a non-polarizing beam-splitter (NPBS), and the interference results are read out by detectors. A time tagger registers single-shot events from all the twofold coincidence channels. The path difference between the two photons can be changed by a delay line to observe the interference. **b** Multi-dimensional Hong–Ou–Mandel (HOM) interference. Solid lines are curve fittings of the data to a Gaussian multiplied by a sinc function. A HOM interference dip (peak) is observed for the rejection (corrected acceptance) probabilities. Error bars are uncertainties assuming Poisson count statistics. **c** The results of the swap test for typical cases: the two states are proper and the same (the first panel); the two states are proper but not the same (the second and third panels), one of the state is proper and the another is improper (the fourth and fifth panels). Each panel shows the experimental (red and blue bars) and theoretical (yellow and gray bars) outcome probabilities on the 15 coincidence channels. The percentage labelled in each panel denotes the rejection probability of the swap test p_r^{swap}

in product test, as an experimental demonstration of the reduction from QMA(K) to QMA(2). To demonstrate the performance of the symmetry test, we apply the optical swap test to different combinations of states, as shown in Fig. 4c. On the basis of the outcome probabilities over the detector patterns, it can be concluded that considerable probabilities are obtained in the "reject" outcomes if the two states are not the same. The theoretical predictions also agree with the experimental results.

Discussion

The results of the four tests, which constitute a complete quantum verification of SAT, highlight the capability of photonic machines to realize a new type of quantum advantage on the computational space[41]. Through the lens of computational complexity, the quantum provers reveal $O(\sqrt{n}\log n)$-bit information, whereas classical provers in the best algorithm need to reveal $O(n)$ bits, not better than simply writing down the complete solution. The QVMs driven by $\tilde{O}(\sqrt{n})$ qubits can efficiently carry out the classically impossible computation, breaking through the $O(n)$-bit limit for classical algorithms imposed by ETH. If we in turn focus on the task of NP verification with limited information, a classical computer with an $O(\sqrt{n}\log n)$-bit message runs in exponential time $2^{O(n-\sqrt{n}\log n)}$ just assuming ETH, whereas the quantum algorithm runs in a polynomial-time overhead[34]. Consequently, QVMs will show an exponential speed-up over classical computers with limited information. Developments on quantum computation pursue provable quantum-classical separation. As ETH is a well-founded complexity-theoretic conjecture in computer science, our result foreshadows a desirable route toward realizing quantum advantages in an useful problem under a "fine-grained" complexity assumption[4].

We have demonstrated the quantum verification algorithm of the satisfiability problem with two unentangled quantum witnesses, using single photons and tunable optical circuits. By combining algorithmic designs and experimental realizations, we optimize the whole architecture of the optical circuit and realize faithful verification of instances with high accuracies and scalability. Our demonstration extends the capability of optical quantum computing into the significant computational model of proof verification. Scaling up the scheme, which requires large scale programmable linear-optical systems and precise control of experimental imperfections, is an appealing route toward quantum advantage. With current advances in photonic technologies[8–10,42], we expect this scheme can be scaled to larger problem sizes in the near future. Among substantial prospects, we envision QVMs can stimulate experimental studies of various proof systems (QMA, QAM, QIP, MIP* etc[36–38,43,44]), inspire future developments of verifier-based quantum algorithms, and find applications in cloud-based quantum computing[45–48]. Our work opens a new avenue in the utility of photonic NISQ devices and adds a key ingredient to the investigation toward answering valuable questions on both computational complexity and quantum physics.

Materials and methods

Quantum verification algorithm

The class QMA(K) consists of the set of decision problems having K unentangled polynomial-size quantum proofs that can be verified on a quantum computer in polynomial time. As the quantum analogue of the complexity class nondeterministic-polynomial-time (NP), QMA(K) has received extensive interests and many natural problems are proven to be in the class, such as N-representability[49] in quantum chemistry. Formally, a language L is in QMA$(K)_{c,s}$ if there exists a polynomial-time quantum algorithm V such that, for all inputs $x \in \{0,1\}^n$:

(i) *Completeness*. If $x \in L$, there exists K witnesses with poly(n) qubits each, such that V outputs "accept" with probability at least c.

(ii) *Soundness*. If $x \notin L$, V outputs "accept" with probability at most s for all proof states.

Our quantum verification algorithm is a modified version of the recent proposals[28,32,34]. The protocol proceeds as follows.

Given a 2-out-of-4 SAT instance ϕ, each of the two Merlins sends to Arthur a quantum state in $\mathbb{C}_n^{\otimes K}$ (with K subsystems). The two quantum states are denoted as $|\varphi_1\rangle$ and $|\varphi_2\rangle$ respectively. Arthur performs one of the following four tests, each with probability 1/4.

(1) *Satisfiability Test*. Arthur randomly chooses a block containing a set of clauses such that no variable appears more than once. Then Arthur measures each of the K subsystems from Merlin 1 in a basis corresponding to the clauses in the block. For each clause (i,j,k,l), Arthur performs the projection on $|c\rangle = (|i\rangle + |j\rangle + |k\rangle + |l\rangle)/2$. If the outcome $|c\rangle$ is obtained for at least one subsystem, reject. Otherwise, accept.

(2) *Uniformity Test*. Arthur randomly chooses a matching M on the set $\{1,2,...,n\}$, and measures each of the K subsystems from Merlin 1 in a basis containing $\{(|i\rangle + |j\rangle)/\sqrt{2}, (|i\rangle - |j\rangle)/\sqrt{2}\}$ for every edge $(i,j) \in M$. If for some edge (i,j), the two outcomes $(|i\rangle + |j\rangle)/\sqrt{2}$ and $(|i\rangle - |j\rangle)/\sqrt{2}$ both occur, reject. Otherwise, accept.

(3) *Symmetry Test*. Arthur chooses the subsystem 1 and another randomly chosen subsystem from Merlin 1, and performs a swap test on the two states. If the swap test passes, accept. Otherwise, reject.

(4) *Product Test*. Arthur performs swap test on each of the K pairs of corresponding subsystems of $|\psi_1\rangle$ and $|\psi_2\rangle$, and accepts if all of the swap tests pass. Otherwise, reject.

Photon source

Frequency-doubled light pulses (~150 fs duration, 415 nm central wavelength) originating from a Ti:Sapphire laser (76 MHz repetition rate; Coherent Mira-HP) pump a beta barium borate (β-BBO) crystal phase-matched for type-II beamlike spontaneous parametric downconversion (SPDC) to produce degenerate photon pairs (830 nm central wavelength). The photon pairs are spectrally filtered by interference filters (IF) with 3 nm full-width at half-maximum and collected into single mode fibres (SMF). The pump power is set to ~150 mW to ensure a low probability of emitting two-photon pairs. By detecting one of the pair via a single-photon avalanche diode, we characterize the second order correlation function of heralded single photons to be $g^{(2)}(0) = 0.041 \pm 0.008$. A HOM interference visibility $V = 0.969 \pm 0.004$ is observed, indicating a great indistinguishability between the two photons. The high indistinguishability guarantees a good performance of the optical swap test. See Supplementary Information for details about the $g^{(2)}(0)$ measurements and the HOM interference.

Optical circuit

In the satisfiability test and uniformity test, Arthur merely needs to measure the quantum proof $|\psi\rangle^{\otimes K}$ from one Merlin (Merlin 1 in the experiments), therefore the optical circuit shown in Fig. 1b is designed to perform local operations with the input of a single photon in each measurement. The single photons generated in the SPDC source are firstly delivered to polarization controllers and polarizers to prepare horizontally polarized states and then directed toward the optical circuit. The circuit is divided into three stages: (i) proof encoding; (ii) a sequence of tunable permutations; (iii) measurement and decision.

In Stage (i), firstly the input single photon passes the splitting module and evolves to an equal superposition on $n/2$ optical modes

$$\hat{a}_1^\dagger|0\rangle \mapsto \sqrt{\frac{2}{n}}\left(\sum_{j=1}^{n/2-1}\hat{a}_{2j-1}^\dagger + \hat{a}_n^\dagger\right)|0\rangle \tag{2}$$

Here $|0\rangle$ denotes the vacuum state. This evolution is experimentally realized by a sequence of wave plates and calcite beam displacers. The following operation is a combination of $n/2$ two-mode transformations $\{u_j(\theta_j)\}$, which constitute an n-mode transformation

$$U = \bigoplus_{j=1}^{n/2} u_j(\theta_j) \tag{3}$$

Each two-mode transformation $u_j(\theta_j)$ can be written as

$$u_j(\theta_j) = \begin{pmatrix} \cos\theta_j & \sin\theta_j \\ \sin\theta_j & -\cos\theta_j \end{pmatrix} \tag{4}$$

where the angle of the optical axis of the corresponding half-wave plate is $\theta_j/2$. Each wave plate can be configured into one of the four different angles to prepare equal superposition encoding the assignment of the two variables (x_{2j-1}, x_{2j}) as 00,01,10 or 11. As a result, the overall transformation U can prepare arbitrary proper states. For the cheating Merlins, the wave plates are set into angles differing from the honest case to implement an unequal splitting and (or) a different transformation U. The details on proof encoding are given in the Supplementary Information.

Stage (ii) comprises a sequence of tunable permutations, each consisting of a transformation U and a mode routing. In this case the two-mode transformations $\{u_j(\theta_j)\}$ are set to two-mode X or Z operations to permutate the two modes or not. The operation of the mode routing is equivalent to a fixed permutation. For example, one of the permutation matrix for mode routing in our experiment can be described as

$$P_0 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

The combination of the aforementioned two operations enables programmable permutation $P \cdot U$ on the n optical modes. With a sequence of $O(n)$ tunable permutation modules, the circuit can be programmed to perform all the permutations required for the two tests (See Supplementary Information for details).

In Stage (iii), the first layer of two-mode transformations $\{u_j(\theta_j)\}$ are all configured as two-mode Hadamard operations $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ to interfere each of the $n/2$ pairs of the two optical modes $(2j-1, 2j)$. The following mode routing rearranges the optical modes to enable possible further interferences required by the satisfiability test. This routing is realized by a high extinction-ratio polarizing beam-splitter (PBS). Two different types of configurations are adopted for the second layer of $\{u_j(\theta_j)\}$ depending on which of the satisfiability test and uniformity test is applied. If the uniformity test is chosen, all the transformations in this layer are set to Z gates or

identity operators $I = \frac{1}{\sqrt{n}}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (without placing any operation on the two modes), which do not perform any interference. Therefore each mode corresponds to an outcome of the form $|i\rangle \pm |j\rangle$ for a certain matching M in terms of the permutation. Arthur will reject the proof when the outcomes $\{|i\rangle + |j\rangle, |i\rangle - |j\rangle\}$ both occur, that is, the two detectors (1,4),(2,5) or (3,6) labelled in Fig. 1c both click among the measurements on K copies. For the satisfiability test, part of transformations in the last layer of $\{u_j(\theta_j)\}$ are set into two-mode Hadamard operations to further interfere two adjacent modes after the aforementioned mode routing. Finally, one of the output modes (the "rejection mode") for a group (*i,j,k,l*) corresponds to the outcome $|i\rangle + |j\rangle + |k\rangle + |l\rangle$, thus Arthur can decide to reject or accept the proof based on whether the detector coupled to the rejection mode clicks (see Supplementary Information for details).

The whole experimental set-up can form various Jamin–Lebedeff interferometers for different permutations and transformations. The beam displacers are strictly aligned and calibrated in order to maintain high interference visibilities for the interferometers when altering the permutations and transformations. The interference visibility for this type of interferometers is measured to be 99.4%. Each of the six output modes of the circuit is coupled to a single-photon avalanche diode (Excelitas Technologies, SPCM-800-FC). Detection events are recorded by a time-correlated single-photon counting system (Swabian Instruments, Time Tagger Ultra) with a coincidence window of 4 ns. We register the measurement results of $5000 \times K$ photons for each test to provide the rejection probabilities shown in the figures.

Optical swap test

Two single photons are injected into two proof encoding modules respectively to prepare the two quantum states $|\psi_1\rangle$ and $|\psi_2\rangle$, which yield the input field

$$\begin{aligned} |\psi_{\text{in}}\rangle = |\psi_1\rangle|\psi_2\rangle &= \left(\sum_{i=1}^{n} \alpha_{1,i}\hat{a}_{1,i}^{\dagger}|0\rangle_1\right)\left(\sum_{j=1}^{n} \alpha_{2,j}\hat{a}_{2,j}^{\dagger}|0\rangle_2\right) \\ &= \sum_{i,j}^{n} \alpha_{1,i}\alpha_{2,j}\hat{a}_{1,i}^{\dagger}\hat{a}_{2,j}^{\dagger}|0\rangle_1|0\rangle_2 \end{aligned} \tag{5}$$

Here $|0\rangle_1$ and $|0\rangle_2$ represent the vacuum state for the two input sides. Then the two single-photon states interfere at the 50:50 NPBS for a multi-mode HOM interference. To observe the HOM interference, the fibre coupler labelled in Fig. 4a is moved by an electronically controlled translation stage (Thorlabs PT1-Z8) to change the relative delay between the wave packets of the two photons. The relationships between the creation operators for the input fields and output fields of the NPBS can be written as

$$\begin{aligned} \hat{a}_{1,i}^{\dagger} &= \tfrac{1}{\sqrt{2}}\left(\hat{a}_{3,i}^{\dagger} + \hat{a}_{4,i}^{\dagger}\right) \\ \hat{a}_{2,i}^{\dagger} &= \tfrac{1}{\sqrt{2}}\left(\hat{a}_{3,i}^{\dagger} - \hat{a}_{4,i}^{\dagger}\right) \end{aligned} \tag{6}$$

By substituting Eq. (6) into Eq. (5), we obtain the output field

$$\begin{aligned} |\psi_{\text{out}}\rangle &= \sum_{i,j}^{n} \tfrac{\alpha_{1,i}\alpha_{2,j}}{2}\left(\hat{a}_{3,i}^{\dagger} + \hat{a}_{4,i}^{\dagger}\right)\left(\hat{a}_{3,j}^{\dagger} - \hat{a}_{4,j}^{\dagger}\right)|0\rangle_3|0\rangle_4 \\ &= \sum_{i} \tfrac{\alpha_{1,i}\alpha_{2,i}}{2}\left[\left(\hat{a}_{3,i}^{\dagger}\right)^2 - \left(\hat{a}_{4,i}^{\dagger}\right)^2\right]|0\rangle_3|0\rangle_4 \\ &\quad + \sum_{i,j}^{i\neq j} \tfrac{\alpha_{1,i}\alpha_{2,j}}{2}\left(\hat{a}_{3,i}^{\dagger}\hat{a}_{3,j}^{\dagger} - \hat{a}_{4,i}^{\dagger}\hat{a}_{4,j}^{\dagger}\right)|0\rangle_3|0\rangle_4 \\ &\quad + \sum_{i,j}^{i\neq j} \tfrac{\alpha_{1,i}\alpha_{2,j}}{2}\left(\hat{a}_{4,i}^{\dagger}\hat{a}_{3,j}^{\dagger} - \hat{a}_{3,i}^{\dagger}\hat{a}_{4,j}^{\dagger}\right)|0\rangle_3|0\rangle_4 \end{aligned} \tag{7}$$

For indistinguishable photons, the resulting output state can be represented as

$$\begin{aligned} |\psi_{\text{out}}\rangle &= \sum_{i} \tfrac{\alpha_{1,i}\alpha_{2,i}}{\sqrt{2}}\left(|2_i\rangle_3|0\rangle_4 - |0\rangle_3|2_i\rangle_4\right) \\ &\quad + \sum_{i,j}^{i<j} \tfrac{\alpha_{1,i}\alpha_{2,j}+\alpha_{1,j}\alpha_{2,i}}{2}\left(|1_i, 1_j\rangle_3|0\rangle_4 - |0\rangle_3|1_i, 1_j\rangle_4\right) \\ &\quad + \sum_{i,j} \tfrac{\alpha_{1,i}\alpha_{2,j}-\alpha_{1,j}\alpha_{2,i}}{2}|1_j\rangle_3|1_i\rangle_4 \end{aligned} \tag{8}$$

Here $|1_i,1_j\rangle_3$ denotes the state with one photon in mode i and another photon in mode j for the output port 3. The right side of Eq. (8) contains three terms, where the first two correspond to the one-side terms (two photons are in the same output port) and the last one corresponds to the two-side terms (one photon in the output port 3 and another photon in the output port 4). The probability of finding a "two-side" outcome is

$$\begin{aligned} p_r^{\text{swap}} &= \tfrac{1}{4}\sum_{i,j}\left|\alpha_{1,i}\alpha_{2,j} - \alpha_{1,j}\alpha_{2,i}\right|^2 \\ &= \tfrac{1}{2}\sum_{i,j}|\alpha_{1,i}|^2|\alpha_{2,j}|^2 - \tfrac{1}{2}\sum_{i,j}\alpha_{1,i}^{*}\alpha_{1,j}\alpha_{2,i}\alpha_{2,j}^{*} \\ &= \tfrac{1}{2}\left(1 - |\langle\psi_1|\psi_2\rangle|^2\right) \end{aligned} \tag{9}$$

considering the overlap between the two states is $\langle\psi_1|\psi_2\rangle = \sum_i \alpha_{1,i}^{*}\alpha_{2,i}$. The probability p_r^{swap} is consistent with the probability of finding a "reject" outcome in a swap test. In the experiment, each path mode of the output is attached to a SPAD, therefore the two polarization modes in the same path are detected by the same detector. This reduces the number of outcomes from $\binom{n}{2}$ to $\binom{n/2}{2}$. The coincidence channels {1,2}, {1,3},{2,3},{4,5},{4,6},{5,6} correspond to the "accept" outcome (here {*i,j*} denotes a coincidence channel between

detectors i and j as labelled in Fig. 4a). We also add photon number resolving detection by attaching a fiber beam-splitter (Thorlabs TN830R5F2) and an additional SPAD to two path modes. This scheme is capable of detecting more events on the "accept" outcome (see Supplementary Information for detailed results).

Acknowledgements
The authors thank N. Yu for helpful discussions. This work was supported by the National Key Research and Development Program of China (Grant Nos. 2019YFA0308700, 2017YFA0303703 and 2018YFB1003202), the National Natural Science Foundation of China (Grant Nos. 61972191, 11690032, 61975077 and 91836303) and the Fundamental Research Funds for the Central Universities (Grant No. 020214380068). P.Y. acknowledges financial support by Anhui Initiative in Quantum Information Technologies (Grant No. AHY150100).

Author details
[1]National Laboratory of Solid State Microstructures, Key Laboratory of Intelligent Optical Sensing and Manipulation (Ministry of Education) and College of Engineering and Applied Sciences, Nanjing University, 210093 Nanjing, China. [2]Collaborative Innovation Center of Advanced Microstructures, Nanjing University, 210093 Nanjing, China. [3]State Key Laboratory for Novel Software Technology, Nanjing University, 210093 Nanjing, China

Author contributions
L.Z. conceived the project. A.Z., P.Y. and L.Z. developed the theoretical analysis, numerical calculation and experimental design. A.Z., H.Z. and J.L. performed the experiments, with contributions from K.Z., T.J. and M.M.. A.Z., H.Z., P.Y. and L.Z. analyzed the data. A.Z., P.Y. and L.Z. wrote the paper with input from all authors.

Data availability
The data represented in Fig. 2a–c are available as Source Data. All other data that support the findings of this study are available from the corresponding authors upon reasonable request.

Competing interests
The authors declare no competing interests.

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41377-021-00608-4.

Received: 19 January 2021 Revised: 22 July 2021 Accepted: 30 July 2021
Published online: 18 August 2021

References

1. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**, 1484–1509 (1997).
2. Grover, L. K. A fast quantum mechanical algorithm for database search. Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. (Association for Computing Machinery, 1996).
3. Aaronson, S. & Arkhipov, A. The computational complexity of linear optics. Proceedings of the 43rd Annual ACM Symposium on Theory of Computing. (Association for Computing Machinery, 2011).
4. Harrow, A. W. & Montanaro, A. Quantum computational supremacy. *Nature* **549**, 203–209 (2017).
5. Preskill, J. Quantum computing in the NISQ era and beyond. *Quantum* **2**, 79 (2018).
6. Arute, F. et al. Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019).
7. Zhong, H. S. et al. Quantum computational advantage using photons. *Science* **370**, 1460–1463 (2020).
8. O'Brien, J. L., Furusawa, A. & Vučković, J. Photonic quantum technologies. *Nat. Photon.* **3**, 687–695 (2009).
9. Aspuru-Guzik, A. & Walther, P. Photonic quantum simulators. *Nat. Phys.* **8**, 285–291 (2012).
10. Flamini, F., Spagnolo, N. & Sciarrino, F. Photonic quantum information processing: a review. *Rep. Prog. Phys.* **82**, 016001 (2019).
11. Broome, M. A. et al. Photonic boson sampling in a tunable circuit. *Science* **339**, 794–798 (2013).
12. Spring, J. B. et al. Boson sampling on a photonic chip. *Science* **339**, 798–801 (2013).
13. Tillmann, M. et al. Experimental boson sampling. *Nat. Photon.* **7**, 540–544 (2013).
14. Crespi, A. et al. Integrated multimode interferometers with arbitrary designs for photonic boson sampling. *Nat. Photon.* **7**, 545–549 (2013).
15. Schreiber, A. et al. A 2D quantum walk simulation of two-particle dynamics. *Science* **336**, 55–58 (2012).
16. Tang, H. et al. Experimental quantum fast hitting on hexagonal graphs. *Nat. Photon.* **12**, 754–758 (2018).
17. Peruzzo, A. et al. A variational eigenvalue solver on a photonic quantum processor. *Nat. Commun.* **5**, 4213 (2014).
18. Santagati, R. et al. Witnessing eigenstates for quantum simulation of hamiltonian spectra. *Sci. Adv.* **4**, eaap9646 (2018).
19. Kagalwala, K. H. et al. Single-photon three-qubit quantum logic using spatial light modulators. *Nat. Commun.* **8**, 739 (2017).
20. Wang, X. L. et al. 18-qubit entanglement with six photons' three degrees of freedom. *Phys. Rev. Lett.* **120**, 260502 (2018).
21. Reck, M. et al. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.* **73**, 58–61 (1994).
22. Carolan, J. et al. Universal linear optics. *Science* **349**, 711–716 (2015).
23. Clements, W. R. et al. Optimal design for universal multiport interferometers. *Optica* **3**, 1460–1465 (2016).
24. Saygin, M. Y. et al. Robust architecture for programmable universal unitaries. *Phys. Rev. Lett.* **124**, 010501 (2020).
25. Cook, S. A. The complexity of theorem-proving procedures. Proceedings of the Third Annual ACM Symposium on Theory of Computing. (Association for Computing Machinery, 1971).
26. Malik, S. & Zhang, L. T. Boolean satisfiability from theoretical hardness to practical success. *Commun. ACM* **52**, 76–82 (2009).
27. Impagliazzo, R. & Paturi, R. On the complexity of *k*-SAT. *J. Comput. Syst. Sci.* **62**, 367–375 (2001).
28. Aaronson, S. et al. The power of unentanglement. *Theory Comput.* **5**, 1–42 (2009).
29. Blier, H. & Tapp, A. All languages in NP have very short quantum proofs. Proceedings of 2009 Third International Conference on Quantum, Nano and Micro Technologies. (IEEE, 2009).
30. Chen, J. & Drucker, A. Short multi-prover quantum proofs for SAT without entangled measurements. Preprint at https://arxiv.org/abs/1011.0716 (2010).
31. Chiesa, A. & Forbes, M. A. Improved soundness for QMA with multiple provers. *Chic. J. Theor. Computer Sci.* **19**, 1–23 (2013).
32. Harrow, A. W. & Montanaro, A. Testing product states, quantum Merlin-Arthur games and tensor optimization. *J. ACM* **60**, 3 (2013).
33. Brandão, F. G. S. L. & Harrow, A. W. Quantum de finetti theorems under local measurements with applications. *Commun. Math. Phys.* **353**, 469–506 (2017).
34. Arrazola, J. M., Diamanti, E. & Kerenidis, I. Quantum superiority for verifying NP-complete problems with linear optics. *npj Quantum Inf.* **4**, 56 (2018).
35. Centrone, F. et al. Experimental demonstration of quantum advantage for NP verification with limited information. *Nat. Commun.* **12**, 850 (2021).
36. Kitaev, A. Y., Shen, A. H. & Vyalyi, M. N. Classical and Quantum Computation. (American Mathematical Society, 2002).
37. Watrous, J. Succinct quantum proofs for properties of finite groups. Proceedings 41st Annual Symposium on Foundations of Computer Science. (IEEE, 2000).
38. Kobayashi, H., Matsumoto, K. & Yamakami, T. Quantum merlin-arthur proof systems: are multiple merlins more helpful to arthur? Proceedings of the 14th International Symposium on Algorithms and Computation. (Springer, 2003).
39. Garcia-Escartin, J. C. & Chamorro-Posada, P. Swap test and Hong-Ou-Mandel effect are equivalent. *Phys. Rev. A* **87**, 052330 (2013).
40. Hong, C. K., Ou, Z. Y. & Mandel, L. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 2044–2046 (1987).
41. Maslov, D. et al. Quantum advantage for computations with limited space. *Nat. Phys.* (2021). https://doi.org/10.1038/s41567-021-01271-7
42. Wang, J. W. et al. Integrated photonic quantum technologies. *Nat. Photon.* **14**, 273–284 (2020).

43. Jain, R. et al. QIP = PSPACE. *J. ACM* **58**, 30 (2011).
44. Ji, Z. F. et al. MIP*=RE. Preprint at https://arxiv.org/abs/2001.04383 (2020).
45. Barz, S. et al. Demonstration of blind quantum computing. *Science* **335**, 303–308 (2012).
46. Reichardt, B. W., Unger, F. & Vazirani, U. Classical command of quantum systems. *Nature* **496**, 456–460 (2013).
47. Barz, S. et al. Experimental verification of quantum computation. *Nat. Phys.* **9**, 727–731 (2013).
48. Fisher, K. A. G. et al. Quantum computing on encrypted data. *Nat. Commun.* **5**, 3074 (2014).
49. Liu, Y. K., Christandl, M. & Verstraete, F. Quantum computational complexity of the *N*-representability problem: QMA complete. *Phys. Rev. Lett.* **98**, 110503 (2007).