nature physics

ARTICLES

PUBLISHED ONLINE: 29 SEPTEMBER 2013 | DOI: 10.1038/NPHYS2763

Experimental verification of quantum computation

Stefanie Barz[1]*, Joseph F. Fitzsimons[2,3], Elham Kashefi[4] and Philip Walther[1]*

Quantum computers are expected to offer substantial speed-ups over their classical counterparts and to solve problems intractable for classical computers. Beyond such practical significance, the concept of quantum computation opens up fundamental questions, among them the issue of whether quantum computations can be certified by entities that are inherently unable to compute the results themselves. Here we present the first experimental verification of quantum computation. We show, in theory and experiment, how a verifier with minimal quantum resources can test a significantly more powerful quantum computer. The new verification protocol introduced here uses the framework of blind quantum computing and is independent of the experimental quantum-computation platform used. In our scheme, the verifier is required only to generate single qubits and transmit them to the quantum computer. We experimentally demonstrate this protocol using four photonic qubits and show how the verifier can test the computer's ability to perform quantum computation.

The prevalent scientific paradigm of testing physical theories by comparing experimental results with predictions computed on a piece of paper or on a computer assumes that all such predictions are solvable in polynomial time on a classical computer. In present experiments involving quantum particles, such as fundamental tests of quantum mechanics or small-scale quantum computations and simulations[1–5], following this paradigm is still possible, as the results can be calculated on a classical computer and verified in experiments involving quantum systems. However, there is an entire class of problems—for example, the simulation of complex quantum systems[6]—that are solvable in polynomial time only on a quantum computer[7].

One of the central conceptual questions in present quantum computing is therefore whether any entity can test the results obtained by a quantum computer, even when that entity is unable to compute these results itself. Alternatively, from a different perspective, can an experimentalist with only classical resources or restricted quantum resources prove that a given device is a quantum computer[8]? Whereas the ultimate answer to such questions is still open, there are several proposals that offer a solution when the verifier is equipped with a range of quantum resources[9–14]—quantum memory, two entangled quantum computers, or a large number of qubits—which, however, are outside the reach of present technology.

Here, we demonstrate how to verify a quantum computation on four qubits. Our method is directly applicable to present technology and can be readily extended to more general cases. We show that only minimal quantum resources (specifically, single qubits) are required to certify a quantum-information processor. Our protocol is independent of the physical system on which it is implemented and it can therefore be applied to any quantum-computing platform.

We have implemented the new protocol on a photonic quantum system and demonstrate the necessary components for verifying a quantum device. We also show how our scheme can be used to verify the generation of the archetype of a quantum-computational resource, quantum entanglement, through a violation of Bell's inequality. In such a verification, the prover remains blind and cannot distinguish the verification procedure from standard quantum-computational tasks such as single- or multi-qubit gates or entire quantum algorithms. To the best of our knowledge, this is the first experiment towards certifying the correctness of a quantum computation.

Interactive proof systems and blind quantum computing

Our protocol combines interactive proof systems and blind quantum computing[9–11]. Interactive proof systems were originally invented in the field of computer science, to approach questions in classical complexity theory[15,16]. They have since been extended into the realm of quantum computation[7]. A quantum prover interactive proof system addresses the question of whether a prover who has access to quantum-computational resources can convince a classical verifier that he can solve a given problem. Interactive proof systems can therefore be used to address the fundamental questions posed above, provided the traditional scientific paradigm of 'predicting' is replaced by 'verifying'.

In our protocol, the framework of the interactive proof system is given by blind quantum computing (Fig. 1). In this framework, a verifier (or client) with limited quantum computational resources can delegate a quantum computation to a prover (or server) with the full power of quantum computing such that all data and the whole computation remain private[10,17]. More specifically, the verifier prepares single qubits in the state

$$|\theta_j\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta_j}|1\rangle\right)$$

with $\theta_j \in \{0, \pi/4, \ldots, 7\pi/4\}$ chosen uniformly at random and known only to the verifier. The qubits are then transmitted to the prover who entangles them to create a blind cluster state[18]. The actual computation is measurement-based[19,20]. The verifier calculates for each blind qubit measurement instructions according to

$$\delta_j = \theta_j + \phi_j + \pi r_j$$

where θ_j is the blind phase of the qubit, ϕ_j is the rotation that the verifier wants to perform (including any Pauli corrections) and $r_j \in \{0, 1\}$ is a randomly chosen value to hide

[1]University of Vienna, Faculty of Physics, Boltzmanngasse 5, 1090 Vienna, Austria, [2]Singapore University of Technology and Design, 20 Dover Drive, Singapore 138682, Singapore, [3]Centre for Quantum Technologies, National University of Singapore, Block S15, 3 Science Drive 2, Singapore 117543, Singapore, [4]School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, UK. *e-mail: stefanie.barz@univie.ac.at; philip.walther@univie.ac.at

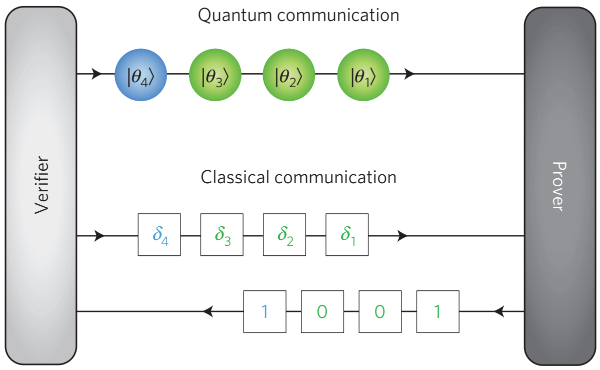

Figure 1 | Concept of a quantum prover interactive proof system based on blind quantum computing. The verifier wants to find out whether the prover can indeed perform quantum computations. Although the question of whether a classical verifier can test a quantum system is still open, it was shown that a verifier who has access to certain quantum resources can verify quantum computations. Here, in the framework of blind quantum computing, the verifier has to be able to generate single qubits and to transmit them to the prover. After the transmission of the qubits, the verifier and the prover exchange two-way classical communication.

the measurement outcome. The prover performs measurements in the basis

$$|\pm_{\delta_j}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\delta_j}|1\rangle)$$

and delivers the results to the verifier. Without the knowledge of the underlying rotation and the random phase, the prover cannot find out anything about the actual rotation ϕ_j—thus, the computation remains blind. The verifier, in contrast, knows the initial rotation and is able to interpret the results. Blind quantum computing therefore provides a powerful tool to delegate computations and to access the resources of powerful quantum computers without divulging the content of the computation. In the following, we show how this concept can be applied to verify quantum computations.

Verification of a quantum computation

In the framework of blind quantum computing, to test a quantum computation, the correctness of the measurements performed by the server has to be verified. Here we use a new verification procedure based on the creation of trap qubits[12,13]. Trap qubits are blindly prepared in a well-defined state, which is known only to the verifier, and are isolated from the actual computation. The measurement angle of these trap qubits is chosen such that the measurement result is predetermined by the verifier, and hence any cheating strategy used by the server that alters these measurement outcomes will be detected. By randomly choosing the locations of the trap qubits it is then possible to bound the probability that the server can cheat while remaining undetected. To reduce resource overhead, our protocol forgoes any encoding of logical qubits into an error detection code, and hence the probability of an error going undetected is polynomially rather than exponentially small, as can be achieved if greater resources are available[12,13].

In our setting, we implement the preparation of the trap qubits through a measurement-based computation on the non-trap qubits. The verifier chooses measurement settings on the cluster state such that any of the qubits could become a trap qubit, prepared in a random state $|\theta_j\rangle$. If the trap qubit is then measured in the basis $|\theta_j\rangle$, the outcome will always be known to the verifier (Fig. 2). Our measurement-based creation of the trap qubits means that we verify a correlation between a subset of measurements, rather than a single measurement outcome. We therefore have to be careful to ensure that the correctness of these correlations for all trap measurements does imply the correctness of a given computational run. In our demonstration using a four-qubit system, only one error remains undetected (see Supplementary Information). However, this particular error cannot alter the result of the measurement of Bell's quantity presented in this paper. In general, the use of measurement-based computation to prepare traps can be applied to systems of an arbitrary size. However, the existence of undetectable errors will depend on the particular entanglement graph and the desired computation. This is a distinct disadvantage of the present scheme when compared with scalable unconditionally secure schemes[12,13], but the result of making this sacrifice is a reduction in the technological burden.

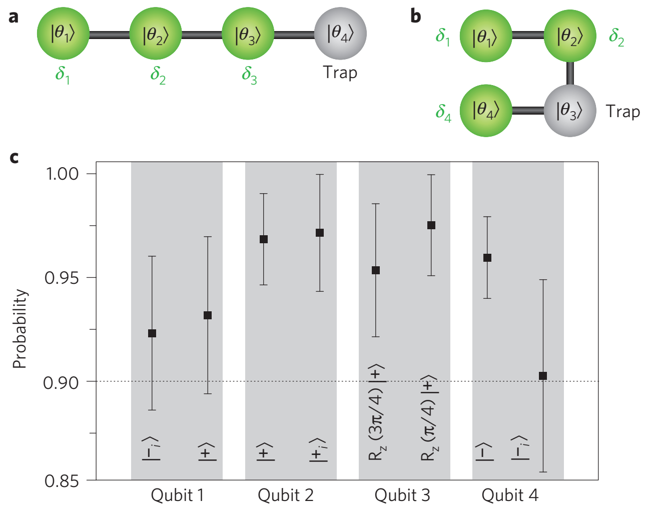

Figure 2 | Measurement verification. a,**b**, A blind linear cluster state (**a**) and a blind rotated horseshoe cluster state (**b**) that can be used for the preparation of trap qubits. **c**, Experimental results of the measurement verification. We prepare two different trap states, shown in the figure and in equations (1)–(5), on each qubit 1–4 (for details about the measurements see Supplementary Information) and show the probability of obtaining the correct outcome when measuring those qubits in a basis for which the expected state is an eigenstate.

This verification procedure can be used to verify that the quantum computation was performed correctly. Therefore, we consider multiple runs of the protocol, where the verifier randomly chooses to run an actual computation or a verification test (Fig. 3). This use of multiple runs of the blind-computation protocol lets us make optimal use of the qubits available in our system. Moreover, the server cannot distinguish between an actual computation run or a trap run. Hence, as discussed in detail in the Supplementary Information, this procedure can be used to verify not only the correctness of the measurement outcomes but also of the entire quantum computation. When trap computation and target computation are randomly interspersed, then the probability that the quantum computer produces the correct result for the verification runs but a wrong result for the computation runs is bounded by a value depending on three parameters: the number of computation runs, the number of trap runs, and the total number of qubits in the system (see Supplementary Information). Although error detection using the outcome of various computation runs can lead to an exponentially small probability of failing to detect a logical error, it should be noted that the verification procedure we use here cannot be directly extended to the case of quantum input and output with better than polynomial accuracy.

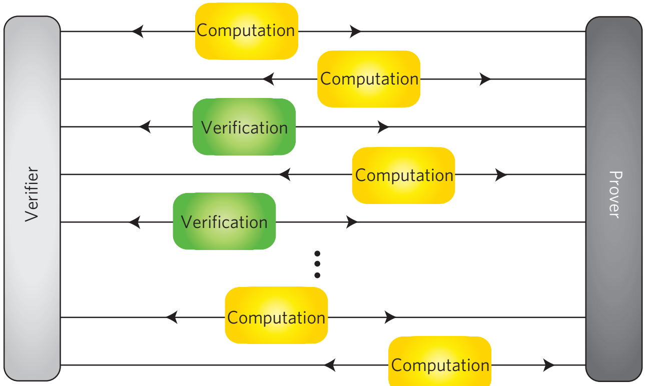

Figure 3 | Schematic of a quantum computation with verification sub-routines. We consider multiple runs of the protocol, where the verifier randomly chooses to run an actual computation or a verification test. The result of the verification test then allows us to conclude whether the computation was performed correctly.

Entanglement verification

Once the measurement outcomes are verified, we can proceed to use the system to probe the prover's entangling capabilities and present a Bell test as an example of a small verifiable computation. Quantum correlations are typically confirmed by well-established tests of Bell's inequality[21] (Fig. 4). To do so, combinations of specific measurement settings α, α' and β, β' are performed on the first (a) and on the second qubit (b), respectively, after generating an entangled state $|\Psi\rangle_{\mathrm{a,b}}$. The settings are chosen such that a maximal violation of the Bell inequality of the Clauser–Horne–Shimony–Holt type[22] is obtained for an entangled state:

$$S = |E(\alpha,\beta) - E(\alpha,\beta')| + |E(\alpha',\beta) + E(\alpha',\beta')| \le 2$$

The correlation coefficients $E(\cdot,\cdot)$ are defined by the coincidence counts when measuring qubit a in the basis α and qubit b in the basis β (for details see Supplementary Information).

To make the Bell test blind, we hide the generation of the entangled state as well as the Bell measurement settings. For this, we base our implementation on a blind zigzag cluster state with four qubits $|\theta_j\rangle$, which is shown in Fig. 4b. Single-qubit measurements on the blind zigzag cluster state realize a quantum circuit that offers exactly the degrees of freedom that are necessary for our blind Bell test. First, using this type of cluster, the verifier has the possibility to blindly switch between entangled or separable input states by choosing δ_4 and θ_4 accordingly. Second, the standard measurement settings for a Bell test are hidden as they are determined by the phases of the blind qubits $|\theta_1\rangle$, $|\theta_2\rangle$ and $|\theta_3\rangle$ and their respective measurement settings of δ_1, δ_2 and δ_3 (see Supplementary Information for details).

As a result, the state generation and the Bell-state measurements are encoded in the phase of blind qubits as well as in the measurement instructions, which remain unknown to the prover at any time. The choice of the cluster-state configuration also remains hidden from the prover. This is a particular advantage of our probabilistic implementation of blind quantum computing, where all qubits are measured coincidentally to verify that a blind cluster state has been created.

Experiment

We use the particular advantages offered by photons to realize a quantum network that can communicate and process quantum information[23] within the same physical system[18]. In our experiment, the blind cluster states are generated from photon pairs entangled in polarization and mode, which originate from spontaneous parametric down-conversion[24]. Our set-up and the methods used are explained in detail in ref. 10; in the present experiment, we generate blind cluster states for various settings of θ_j and use them to implement exemplary runs of trap computations as well as the Bell-test runs—the necessary building blocks of a verified test of Bell's quantity. We note that the requirement of having single photons can be relaxed to coherent states[25] or to the verifier doing only measurements[26].

For the demonstration of the measurement verification, we use blind linear cluster states and blind rotated horseshoe cluster states to prepare traps as shown in Fig. 2a,b. By choosing the blind phases θ_j and measurement settings

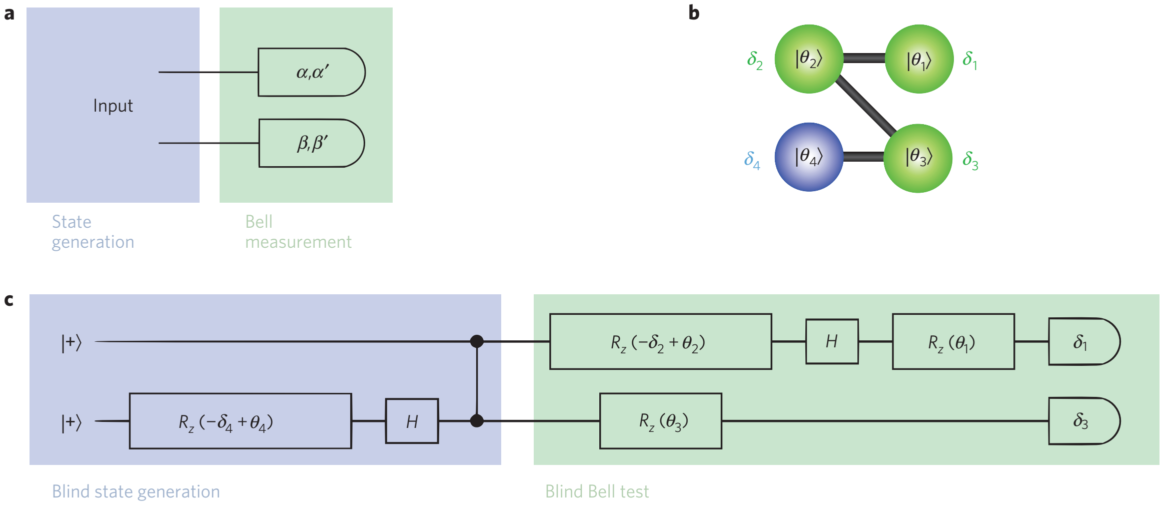

Figure 4 | A blind Bell test for the verification of quantum resources. a, Conventional scheme for a Bell test, where first an (entangled) state is created and then Bell measurements are performed. **b**,**c**, The blind zigzag cluster state (**b**) and its corresponding circuit (**c**). If the rotation R_z in the lower wire, $-\delta_4+\theta_4$, is chosen equal to zero (or π), the input state in the lower wire will be equal to $|0\rangle_{\mathrm{b}}$ ($|1\rangle_{\mathrm{b}}$); otherwise, if the rotation is chosen equal to $\pm\pi/2$, the input will be $|\pm_i\rangle_{\mathrm{b}}$. The edge between qubits 2 and 3 performs a CPhase gate on the two qubits, which results in an unentangled state in the former case, and in an entangled state in the latter. The values of δ_1, δ_2 and δ_3, as well as the phases θ_1, θ_2 and θ_3, determine the Bell measurement settings shown in equation (6).

δ_j as given in the Supplementary Information, we prepare the trap qubits:

$$|\mathrm{trap}_1\rangle = |-_i\rangle \text{ and } |+\rangle \tag{1}$$

$$|\mathrm{trap}_2\rangle = |+\rangle \text{ and } |+_i\rangle \tag{2}$$

$$|\mathrm{trap}_3\rangle = R_z(3\pi/4)|+\rangle \text{ and } R_z(\pi/4)|+\rangle \tag{3}$$

$$|\mathrm{trap}_4\rangle = |-\rangle \text{ and } |-_i\rangle \tag{4}$$

on qubits 1, 2, 3 and 4, respectively. Here, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ and $|\pm_i\rangle = (|0\rangle \pm i|1\rangle)/\sqrt{2}$. The probabilities to find the correct outcome are well above 90%, as shown in Fig. 2c.

For a verification of quantum entanglement, we choose combinations of θ_4 and δ_4 to create the entangled state:

$$|\Psi\rangle_{a,b} = \frac{1}{\sqrt{2}}(|+\rangle_{\mathrm{a}}|0\rangle_{\mathrm{b}} - i|-\rangle_{\mathrm{a}}|1\rangle_{\mathrm{b}}) \tag{5}$$

and to blindly implement the Bell measurements settings we choose:

$$\alpha = \pi/2, \qquad \alpha' = \sigma_z, \qquad \beta = -3\pi/4, \qquad \beta' = -\pi/4 \tag{6}$$

where the bases α, β and β' are defined as $\{(|0\rangle \pm \mathrm{e}^{i\alpha}|1\rangle)/\sqrt{2}\}$ and so on, and α' is a measurement in the computational basis $\{|0\rangle, |1\rangle\}$. To obtain the measurement settings given in equation (6), we choose combinations of $|\theta_j\rangle$ and δ_j as given in detail in the Supplementary Information. From the measured coincidence count rates, we calculate the correlation coefficients to be:

$$E(\alpha,\beta) = -0.540 \pm 0.084$$

$$E(\alpha,\beta') = 0.634 \pm 0.086$$

$$E(\alpha',\beta) = -0.646 \pm 0.067$$

$$E(\alpha',\beta') = -0.678 \pm 0.079$$

Those coefficients lead to an S parameter of

$$S = 2.498 \pm 0.158$$

which violates the classical bound ($|S| = 2$) by more than 3 standard deviations.

Although the main role of the Bell test is to serve as an archetypal quantum computation to be verified, the combination of the verification procedure and this violation of Bell's inequality also provides a measure for the quality of the entangling gates the prover performs. In our experiment, we implement a subset of all possible blind states. The states of qubits 1 and 4 are fixed to $|+\rangle$, whereas the states of qubits 2 and 3 are fully blind[18]. The whole verification procedure remains blind, however, if we assume that the prover has no a priori knowledge of our choice of states and measurements.

The violation of Bell's inequalities is impossible classically, not for the reason of high complexity, but rather on the basis of physical principles. In our implementation, we assume the correctness of quantum mechanics for the verification of the measurement outcomes. Without this assumption, a full demonstration would require the two entangled photons to be sent to two distant laboratories or servers, where only at the very last step of the computation the verifier gives the measurement instructions to the prover. In this way, no classical computer could mimic, even in principle, the output of the computation a priori, while ensuring that the verification procedure would still have a positive outcome.

Conclusion

Future large-scale quantum computers and quantum simulators[27–30] will require the verification of their experimental results[31]. Owing to the superior computational capacity of quantum systems the results cannot simply be calculated and checked on a classical device. The development of new methods for the verification of quantum computations is therefore a crucial task. Here, we have developed a new general method for verifying quantum computations that can be readily applied to present small-scale quantum computers.

Finally, how verification mechanisms provide insights into questions of computational complexity and into the foundations of quantum physics is a topic of active research. So far, the limit of high computational complexity is mostly unexplored and it is not impossible that quantum mechanics breaks down at some scale of complexity[32].

Verification methods, such as those reported herein, are not only important as a mechanism to certify quantum computers, but also provide an entirely new toolbox for addressing fundamental questions in quantum physics and computer science.

Received 12 June 2013; accepted 19 August 2013; published online 29 September 2013

References

1. Deutsch, D. Quantum theory, the Church–Turing principle and the universal quantum computer. *Proc. R. Soc. A* **400,** 97–117 (1985).
2. Deutsch, D. & Jozsa, R. Rapid solution of problems by quantum computation. *Proc. R. Soc. A* **439,** 553–558 (1992).
3. Grover, L. K. in *Proc. 28th Annual ACM Symp. on the Theory of Computing* (ed. Miller, G. L.) 212–219 (ACM, 1996).
4. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26,** 1484–1509 (1997).
5. Harrow, A. W., Hassidim, A. & Lloyd, S. Quantum algorithm for linear systems of equations. *Phys. Rev. Lett.* **103,** 150502 (2009).
6. Feynman, R. Simulating physics with computers. *Int. J. Theor. Phys.* **21,** 467–488 (1982).
7. Watrous, J. in *Computational Complexity* (ed. Meyers, R. A.) 2361–2387 (Springer, 2012).
8. Pappa, A., Chailloux, A., Wehner, S., Diamanti, E. & Kerenidis, I. Multipartite entanglement verification resistant against dishonest parties. *Phys. Rev. Lett.* **108,** 260502 (2012).
9. Aharonov, D., Ben-Or, M. & Eban, E. *Proc. Innovations in Computer Science* 453 (ICS, 2010).
10. Broadbent, A., Fitzsimons, J. & Kashefi, E. *Proc. 50th Ann. Symp. Found. Comp. Sci.* 517–526 (IEEE Computer Society, 2009).
11. Aharonov, D. & Vazirani, U. V. *Computability: Turing, Gödel, Church, and Beyond* 329 (MIT Press, 2013).
12. Fitzsimons, J. & Kashefi, E. Unconditionally verifiable blind computation. Preprint at http://arxiv.org/abs/1203.5217 (2012).
13. Morimae, T. No-signaling topological quantum computation in intelligent environment. Preprint at http://arxiv.org/abs/1208.1495 (2012).
14. Reichardt, B., Unger, F. & Vazirani, U. Classical command of quantum systems. *Nature* **496,** 456–460 (2013).
15. Babai, L. *Proc. 17th Ann. ACM Symp. Theory Comput.* 421–429 (ACM, 1985).
16. Goldwasser, S., Micali, S. & Rackoff, C. The knowledge complexity of interactive proof systems. *SIAM J. Comput.* **18,** 186–208 (1989).
17. Morimae, T. & Fujii, K. Blind topological measurement-based quantum computation. *Nature Commun.* **3,** 1036 (2012).
18. Barz, S. *et al.* Demonstration of blind quantum computing. *Science* **335,** 303–308 (2012).
19. Raussendorf, R. & Briegel, H. A one-way quantum computer. *Phys. Rev. Lett.* **86,** 5188–5191 (2001).
20. Raussendorf, R., Browne, D. E. & Briegel, H. J. Measurement-based quantum computation with cluster states. *Phys. Rev. A* **68,** 022312 (2003).
21. Bell, J. On the Einstein–Podolsky–Rosen paradox. *Physics* **1,** 195–200 (1964).
22. 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).
23. Knill, E., Laflamme, R. & Milburn, G. J. A scheme for efficient quantum computation with linear optics. *Nature* **409,** 46–52 (2001).
24. Kwiat, P. G. *et al.* New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.* **75,** 4337–4341 (1995).
25. Dunjko, V., Kashefi, E. & Leverrier, A. Blind quantum computing with weak coherent pulses. *Phys. Rev. Lett.* **108,** 200502 (2012).

26. Morimae, T. & Fujii, K. Blind quantum computation protocol in which Alice only makes measurements. *Phys. Rev. A* **87,** 050301 (2013).
27. Weitenberg, C. *et al.* Single-spin addressing in an atomic Mott insulator. *Nature* **471,** 319–324 (2011).
28. Islam, R. *et al.* Onset of a quantum phase transition with a trapped ion quantum simulator. *Nature Commun.* **2,** 377 (2011).
29. Monz, T. *et al.* 14-qubit entanglement: Creation and coherence. *Phys. Rev. Lett.* **106,** 130506 (2011).
30. Britton, J. *et al.* Engineered two-dimensional Ising interactions in a trapped-ion quantum simulator with hundreds of spins. *Nature* **484,** 489–492 (2012).
31. Leibfried, D. Could a boom in technologies trap Feynman's simulator? *Nature* **463,** 608–608 (2010).
32. Aaronson, S. *Proc. 36th Ann. ACM Symp. Theory Comput.* 118–127 (ACM, 2004).

Acknowledgements

The authors are grateful to S. Aaronson, D. Aharonov, C. Brukner, A. Zeilinger and F. Verstraete for discussions. S.B. and P.W. acknowledge support from the European Commission, Q-ESSENCE (No. 248095), QUILMI (No. 295293), EQUAM (No. 323714), PICQUE (No. 608062) and the ERA-Net CHISTERA project QUASAR, the John Templeton Foundation, the Vienna Center for Quantum Science and Technology (VCQ), the Austrian Nano-initiative NAP Platon, the Austrian Science Fund (FWF) through the SFB FoQuS (No. F4006-N16), START (No. Y585- N20) and the doctoral programme CoQuS, the Vienna Science and Technology Fund (WWTF) under grant ICT12-041, and the Air Force Office of Scientific Research, Air Force Material Command, United States Air Force, under grant number FA8655-11-1-3004. J.F.F. acknowledges support from the National Research Foundation and the Ministry of Education, Singapore. This material is based on research supported in part by the Singapore National Research Foundation under NRF Award No. NRF-NRFF2013-01. E.K. acknowledges support from UK Engineering and Physical Sciences Research Council (EP/E059600/1).

Author contributions

S.B. designed and performed the experiments, acquired the experimental data, carried out theoretical calculations and the data analysis, and wrote the manuscript. J.F.F. and E.K. carried out theoretical calculations, contributed the proofs, and wrote the manuscript. P.W. designed the experiment, edited the manuscript and supervised the project.

Additional information

Supplementary information is available in the online version of the paper. Reprints and permissions information is available online at www.nature.com/reprints. Correspondence and requests for materials should be addressed to S.B. or P.W.

Competing financial interests

The authors declare no competing financial interests.