Verifiable blind quantum computing with trapped ions and single photons

Citation for published version:
Drmota, P, Nadlinger, DP, Main, D, Nichol, BC, Ainley, EM, Leichtle, D, Mantri, A, Kashefi, E, Srinivas, R, Araneda, G, Ballance, CJ & Lucas, DM 2024, 'Verifiable blind quantum computing with trapped ions and single photons', *Physical Review Letters*, vol. 132, no. 15, 150604, pp. 1-6.
https://doi.org/10.1103/PhysRevLett.132.150604

Digital Object Identifier (DOI):
10.1103/PhysRevLett.132.150604

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Publisher's PDF, also known as Version of record

Published In:
Physical Review Letters

Editors' Suggestion Featured in Physics

Verifiable Blind Quantum Computing with Trapped Ions and Single Photons

P. Drmota,[1] D. P. Nadlinger,[1] D. Main,[1] B. C. Nichol,[1] E. M. Ainley,[1] D. Leichtle,[2] A. Mantri,[3] E. Kashefi,[2,4] R. Srinivas,[1] G. Araneda,[1] C. J. Ballance,[1] and D. M. Lucas[1]

[1]*Department of Physics, University of Oxford, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, United Kingdom*
[2]*Laboratoire d'Informatique de Paris 6, CNRS, Sorbonne Université, Paris 75005, France*
[3]*Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, Maryland, USA*
[4]*School of Informatics, University of Edinburgh, Edinburgh EH8 9AB, United Kingdom*

(Received 10 May 2023; accepted 16 January 2024; published 10 April 2024)

We report the first hybrid matter-photon implementation of verifiable blind quantum computing. We use a trapped-ion quantum server and a client-side photonic detection system networked via a fiber-optic quantum link. The availability of memory qubits and deterministic entangling gates enables interactive protocols without postselection—key requirements for any scalable blind server, which previous realizations could not provide. We quantify the privacy at $\lesssim 0.03$ leaked classical bits per qubit. This experiment demonstrates a path to fully verified quantum computing in the cloud.

DOI: 10.1103/PhysRevLett.132.150604

Quantum computers are poised to outperform the world's most powerful supercomputers, with applications ranging from drug discovery to cybersecurity. These computers harness quantum phenomena such as entanglement and superposition to perform calculations that are believed to be intractable with classical computers. As quantum processors control delicate quantum states, they are necessarily complex and physical access to high-performance systems is limited. Cloud-based approaches, where users can remotely access quantum servers, are likely to be the working model in the near term and beyond; many users already perform computations on commercially available devices for state-of-the-art research [1–5].

However, delegating quantum computations to a server carries the same privacy and security concerns that bedevil classical cloud computing. Users are currently unable to hide their work from the server or to independently verify their results in the regime where classical simulations become intractable. Remarkably, the same phenomena that enable quantum computing can leave the server "blind" in a way that conceals the client's input, output, and algorithm [6–8]; because quantum information cannot be copied and measurements irreversibly change the quantum state, information stored in these systems can be protected with information-theoretic security, and incorrect operation of the server or attempted attacks can be detected—a surprising possibility which has no equivalent in classical computing. Blind quantum computing (BQC) requires not only a universal quantum computer as the server, but also a quantum link connecting it to the client [9,10]. Photons are a natural choice to provide that link, and indeed the first demonstrations of BQC were performed in purely photonic systems [11–14]. However, unavoidable photon loss, either due to limited photon detection efficiencies or absorption in the link, results in potential security risks [11,13] and places hard limits on the scalability of this approach due to the resource overhead incurred by postselection [15]. Ideally, quantum information at the server should be stored in a stable quantum memory that can be manipulated with high fidelity, yet readily interfaced to a photonic link. The ability to retain quantum information on the server then enables the client to perform adaptive midcircuit adjustments in order to execute the target computation deterministically and securely. Combining two completely different platforms at the single-quantum level is technically challenging [16,17]; so far, quantum network nodes with integrated memory qubits have been realized with solid-state systems [18,19] and trapped atoms [20,21].

Here, we demonstrate BQC using a trapped-ion quantum processor (server) that integrates a robust memory qubit encoded in $^{43}\mathrm{Ca}^+$ with a single-photon interface based on $^{88}\mathrm{Sr}^+$ to establish a quantum link to the client (photon detection system). We implement an interactive protocol, where the client can remotely prepare single-qubit states on the server adaptively from shot to shot using real-time classical feedforward control. The complexity needed for universal quantum computation is contained entirely within the server, while the client is a simple photon polarization measurement device that is independent of the size and complexity of the algorithm and supports near-perfect blindness by construction. The client and the server are controlled by independent hardware and connected only by a classical signaling bus and an optical fiber. Our system achieves noise levels below a certain threshold for which arbitrary improvements to the protocol security and success rate (robustness) are theoretically possible [22].

Protocol.—Quantum algorithms can be described in the measurement-based quantum computing model, which prescribes a sequence of measurements on a highly entangled resource state [23,24]. Information-theoretic blindness can be achieved, even against maliciously operating servers, if either the state preparation or the measurements are performed by the client [6,25–27].

In the presence of noise, even a faithfully operating server produces erroneous results that are indistinguishable from nefarious modifications to the honest protocol [7,8,28,29]. Blindness allows the client to secretly test the quantum resources provided by the server. The protocol implemented here achieves this by interleaving "computation" and "test" rounds. A statistical argument provides bounds for the security and robustness of this protocol for the important class of bounded-error quantum polynomial time (BQP) decision problems [22]. The client accepts a result if the observed fraction of failed test rounds p_{fail} is below a chosen threshold ω. If ω is below the theoretical threshold ω_{max}, the overhead due to repetition is low: the probability of accepting an incorrect result decreases exponentially with the number of rounds. The minimum value for ω depends on the amount of noise in the devices. The client assumes a maximum expected test round failure rate p_{max} and chooses $\omega > p_{\mathrm{max}}$ such that the probability of rejecting any result also decreases exponentially with the number of rounds, making the protocol robust to a limited amount of noise.

For universal quantum computation, particular graph states, and a discrete set of single-qubit measurements, $\{\hat{B}_\alpha = \cos(\alpha)\mathsf{X} + \sin(\alpha)\mathsf{Y}\}_{\alpha\in\Theta}$, are sufficient [30], where $\Theta = \{0, \pi/4, \ldots, 7\pi/4\}$, and X, Y are Pauli operators. Graph states are specific multiqubit states in which vertices represent qubits initialized in $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and edges represent entanglement created by two-qubit CZ gates (Fig. 1), where $\mathrm{CZ} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \mathsf{Z}$. The qubits are measured in a fixed order, using the basis $\hat{B}_{\alpha_\ell}$ at node ℓ, where α_ℓ depends on the algorithm and on previous measurement outcomes.

To blindly run the above protocol with measurement angles α_ℓ, the client performs remote state preparation (RSP) into $|\theta_\ell\rangle = \exp[-\mathrm{i}(\theta_\ell/2)\mathsf{Z}]|+\rangle$, with secret phase shift $\theta_\ell \in \Theta$ for every qubit $\ell = 1, 2, \ldots, q$, and shifts the measurement angles accordingly. This way, θ_ℓ act as a classical encryption key such that α_ℓ remain private to the client. To ensure that the corresponding measurement outcomes $m_\ell \in \{0, 1\}$ are uninformative, the client hides bit flips in half of the measurement angles that are indicated by secret key bits, $r_\ell \in \{0, 1\}$ [Eq. (1)]. The client can recover the unencrypted measurement outcomes as $m_\ell \oplus r_\ell$.

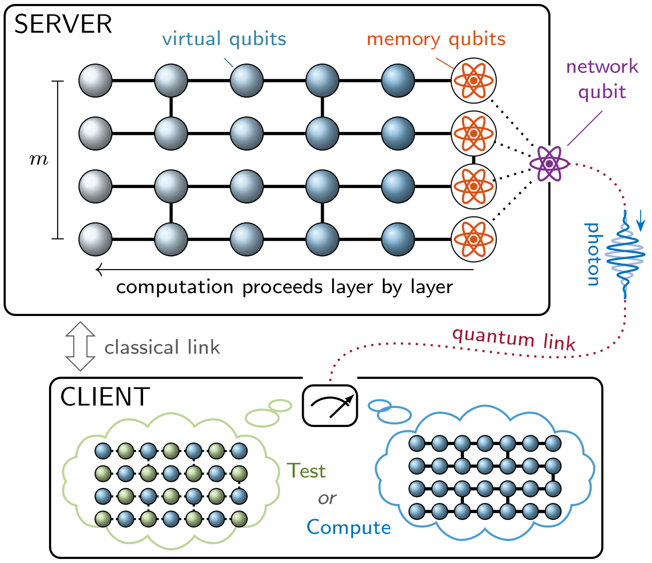

FIG. 1. Verifiable blind quantum computing in the measurement-based model. The computation is expressed as a sequence of measurements on a brickwork state (two-dimensional graph with vertices representing virtual qubits, and edges indicating CZ gates). The server holds m physical memory qubits (orange atoms) and one physical network qubit (violet atom). The server can entangle these qubits deterministically with each other. The network qubit can also be entangled with a photon; by measuring this photon, the client can steer the network qubit in the server remotely without the server learning about its state. This allows the client to hide the computation (inputs, outputs, and circuit) from the server. Moreover, the client can verify that the computation has not been tampered with by (randomly) interleaving test rounds, which produce classically simulatable outcomes and cannot be distinguished from the actual computation by the server.

Here we implement BQC on linear cluster states (Fig. 2). Two physical qubits are sufficient to implement linear clusters of arbitrary length, as qubits can be reinitialized after every midcircuit measurement. The first qubit—the network qubit—can be steered into an arbitrary state by the client using RSP [31], while the second qubit—the memory qubit—carries the information encoded in the leading node of the expanding linear cluster state. We break the cluster state into discrete interaction steps between the server and the client, starting with the initialization step (Fig. 2), which prepares the memory qubit in $|\theta_1\rangle$. At each interaction of a computation round, the client performs RSP to steer the network qubit into $|\theta_{\ell+1}\rangle$ and communicates

$$\delta_\ell = (-1)^{R_{\ell-1}}\alpha_\ell + \theta_\ell + \pi r_\ell \qquad (1)$$

to the server, where $R_\ell = \bigoplus_{1\le j<\ell/2} (m_{\ell-2j} \oplus r_{\ell-2j})$ is the adaptive feedforward correction from decrypted previous measurements. After applying the CZ gate and a SWAP gate, the server measures the network qubit in the $\hat{B}_{\delta_\ell}$ basis and returns the result m_ℓ to the client (interaction blocks in

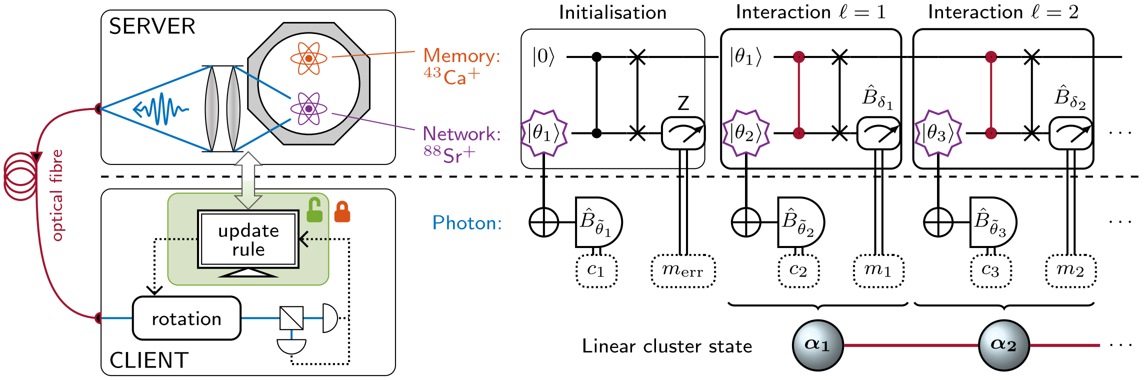

FIG. 2. Protocol used to generate a linear cluster state using a trapped-ion quantum server and a photonic client. The client can steer the network qubit into $|\theta_\ell\rangle = |\tilde{\theta}_\ell + c_\ell \pi\rangle$ by measuring the polarization of the photon in the basis $\hat{B}_{\tilde{\theta}_\ell}$ and obtaining $c_\ell \in \{0, 1\}$ as outcome. In the initialization step, the server transfers this state onto a memory qubit such that the network qubit can be steered again [21]. Every subsequent interaction step extends the size of the cluster state; the client steers the network qubit remotely into $|\theta_{\ell+1}\rangle$, the server entangles it (CZ gates), and performs a measurement in the basis $\hat{B}_{\delta_\ell}$, where δ_ℓ is provided by the client. See text for details.

Fig. 2). This process leaves the leading cluster state node on the memory qubit, encrypted by R_ℓ [32], while the network qubit is available for further RSP.

The client randomly assigns each round a secret label identifying them as a computation or a test. In test rounds, the client prepares every second qubit in a Z eigenstate $|r_\ell\rangle$, which are called "dummy qubits." This step leaves the remaining, so-called "trap qubits," in a separable state. The outcome $m_\ell \overset{!}{=} r_\ell$ of measuring these trap qubits with $\delta_\ell = \theta_\ell + \pi r_\ell$ can thus be predicted efficiently by the client.

Server.—The server controls an ion trap quantum processor containing one ^{88}Sr$^+$ and one ^{43}Ca$^+$ ion. Ion-photon entanglement needed for RSP is generated by fast excitation and spontaneous decay [37] on the 422 nm transition of ^{88}Sr$^+$. The single photons are collected by free-space optics and coupled into a single-mode optical fiber [38], which forms the quantum link with the client. The memory qubit is encoded in ^{43}Ca$^+$, which provides a long coherence time (∼10 s) and is unaffected by concurrent manipulation of ^{88}Sr$^+$ [21]. Thus, ^{88}Sr$^+$ can be used for midcircuit measurements and sympathetic cooling between interaction steps. The CZ gate required to build the cluster state is combined with the SWAP gate into an ISWAP gate. This enables reuse of ^{88}Sr$^+$ for RSP while the current state of the computation is retained on the memory qubit. Errors during the initialization step are detected in real time ($m_{\mathrm{err}} = 1$ in Fig. 2), in which case this step is repeated.

Client.—The client receives single photons from the server through an optical fiber. The quantum capability of the client is reduced to projective polarization measurements of these photons in a basis that can be dynamically reconfigured by changing the voltages on two electro-optic modulators (EOMs) [32] (Fig. 3). This measurement remotely steers the network qubit into a state that depends only on the polarization measurement basis and the measurement outcome obtained, information known exclusively to the client ($\tilde{\theta}_\ell$ and c_ℓ in Fig. 2). Birefringence in the optical fiber transforms the photonic state before reaching the client by an unknown unitary operation, which drifts on

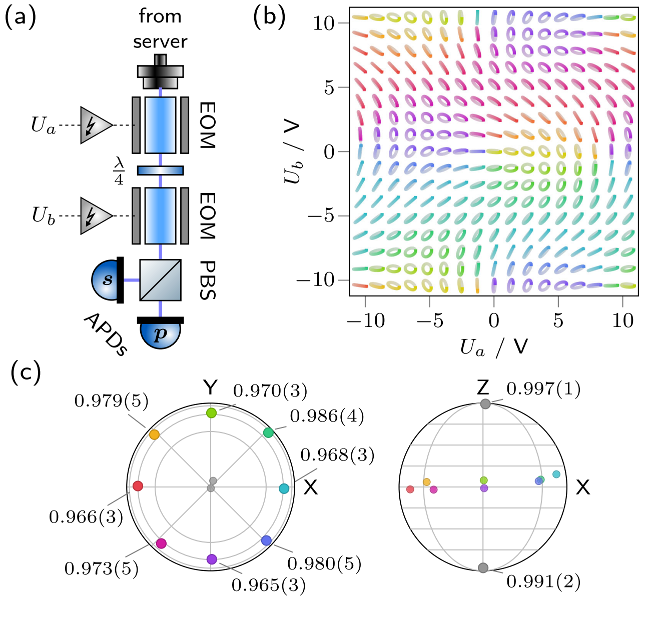

FIG. 3. The client performs remote state preparation (RSP) using a fast-switching polarization analyzer. (a) The control voltages (U_a, U_b) of two EOMs separated by a $\lambda/4$ wave plate enable the client to arbitrarily rotate the measurement basis given by the PBS. (b) Laser light is used to reconstruct this basis for different U_a, U_b. Polarization ellipses are shown for the basis states heralded by detector p, where the color represents their phase. (c) To find U_a, U_b which maximize the fidelity F to each target state needed during the protocol, we perform tomography on the network qubit after RSP. The averaged results from 36 calibrations over 2 weeks are shown in the Bloch sphere representation of the network qubit. Values indicate F, with standard deviations obtained from bootstrapping.

a timescale of ∼10 min due to thermal effects. To compensate for this drift, the client periodically recalibrates the EOM voltages [32] [Fig. 3(c)].

Blindness.—We consider information that could leak to an adversarial server, concerning the client's polarization measurement, via the network qubit, which is controlled by the server, and through classical signals, which are controlled by the client. We quantify the information that the server could gain from measuring the network qubit at 0.031(4) bits per interaction step using quantum state tomography and find good agreement with independent estimates [32]. In our demonstration, mismatched electronic delays between different polarization measurement outcomes are the dominant cause for information leakage. However, as the client controls the relevant classical signals, these delays could be matched. The remaining leakage of ∼0.001 bits per interaction step would be dominated by imperfections in the polarizing optics used by the client.

Results.—We realize different quantum computations with one and two interaction steps; see Figs. 4(a) and 4(b), respectively. We could use the output qubit in further interaction steps, or make a final measurement in the basis $\hat{B}_{\delta_{q+1}}$ to complete the $(q+1)$-node cluster computation. In this demonstration, however, the output qubit is always measured in the Z basis. Since this measurement commutes with the CZ gate preceding it, the computation is equivalent to a cluster state with one fewer node. The one- and two-step interactions therefore implement the computations $\mathsf{H}Z(\alpha_1)|+\rangle$ and $X(\alpha_2)Z(\alpha_1)|+\rangle$, respectively, where H is the Hadamard gate, $X(\alpha) = \exp[-\mathrm{i}(\alpha/2)\mathsf{X}]$ and $Z(\alpha) = \exp[-\mathrm{i}(\alpha/2)\mathsf{Z}]$ are single-qubit rotations, and α_1 and α_2 are encrypted using Eq. (1) during the protocol. From the server's perspective, the outcomes appear random [squares in Fig. 4(a)] as a result of the bit-flip encryption, $\delta_\ell \propto r_\ell \pi$, which is applied by the client in both the computation and test rounds. The client, on the other hand, can use the round type (computation or test) and encryption key (r_ℓ) to decode the outcomes. The decoded computation outcomes, indicated by the circles in Fig. 4(a) and the color map in Fig. 4(b), match the expected fringe pattern as a function of the blind measurement angles α_1 and α_2. Experimental imperfections lead to a reduction in contrast and to phase shifts. The client observes an error rate of $p_{\mathrm{fail}}^{(1)} = 0.201(3)$ on the first qubit and $p_{\mathrm{fail}}^{(2)} = 0.095(2)$ on the second qubit [bottom panel in Fig. 4(a)], which are consistent with known error sources [32]. By changing the final measurement basis from Z to $\hat{B}_{\delta_{q+1}}$ with an additional $\pi/2$ pulse, which would have no significant impact on the error budget, and randomly choosing one qubit as trap qubit in every test round, we find that a two-node cluster computation could be verified using our apparatus [32]; the expected average test round failure probability of ∼0.18 would be significantly below $\omega_{\max} = 0.25$ required for secure and robust verification of this state. The corresponding test round results for the three-node cluster computation are shown in the Supplemental Material [32]; the observed failure rates indicate that verification is not possible in this case, largely due to technical limitations (motional heating) on the ≈ 0.91 fidelity of the ISWAP gate [21].

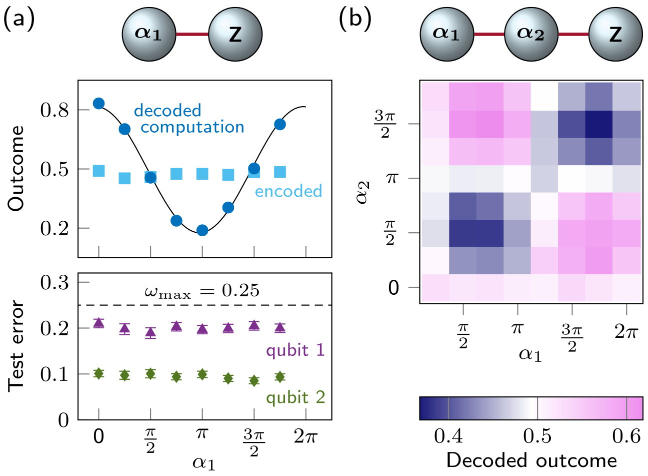

FIG. 4. Experimental results on an expanding linear cluster state, where the leading qubit is measured in the Z basis after (a) one and (b) two interaction steps between the client and the server. (a) While the server observes mixed outcomes (squares, ∼2000 test and computation rounds each), for each α_1, the client can decode the results using the secret keys. A fit to the decoded computation outcomes (circles) is shown to guide the eye. Error intervals indicate the binomial standard error. The test round errors are significantly below the threshold for verification of a two-node cluster state (dashed line). (b) The decoded outcome is shown for different blind measurement settings, (α_1, α_2), each comprising ∼3100 computation rounds (see Supplementary Material [32] for interleaved test round results).

Conclusion.—We have implemented a protocol for blindly delegating quantum computations to a trapped-ion quantum processor, using a client apparatus that requires only single-photon polarization measurements and classical communication. We have established bounds on information leakage through both the classical and quantum channels that are present in our implementation. We have shown that the size of the cluster state can be increased without increasing the number of physical qubits in the server and without modifications to the client hardware. If more memory qubits were added to the server [39,40], the computational space could be extended to higher-dimensional cluster states. We have taken steps to include verification into the protocol, and the measured test round error indicates that computations on two-node cluster states could be verified robustly and reliably. We predict that for a BQP decision problem with small inherent algorithmic error and $p_{\max} = 0.185$, the probability of accepting an incorrect result and that of rejecting any result would both be 10^{-5} after 24 000 repetitions, including 14 400 test rounds; every additional 1200 repetitions would halve this likelihood [32]. This approach is expected to provide both security and robustness for larger cluster states and other algorithms as long as the errors remain below the size-dependent threshold, $\omega_{\max} \approx 1 - (3/4)^{2/q}$, where q is the total number of qubits in the cluster state. The protocol that we have implemented does not incorporate error correction; to verify larger cluster states, the error per interaction step would need to be reduced. The infidelity of the ISWAP gate is the leading error source [21], but we note that in other systems, CZ gates between $^{88}\mathrm{Sr}^{+}$ and $^{43}\mathrm{Ca}^{+}$ with fidelity 0.998 have been demonstrated [41]. The state-of-the-art ion-photon entanglement fidelity of 0.979(1) (this apparatus) is limited primarily by technical imperfections in the optical setup (alignment).

In comparison with previous experimental implementations [11–14], which were based on purely photonic platforms without quantum memory, this Letter overcomes several major challenges associated with real-world BQC deployments. As quantum logic operations in the server are deterministic and the interaction with the client is heralded, our implementation eliminates the need for postselection, avoiding the associated efficiency, scalability, and security issues [11,12,14]. Here, photon losses in particular do not present a security threat, and the use of a memory qubit combined with fast and adaptive hardware facilitates true shot-by-shot randomization of all protocol parameters in real time.

Future realizations could involve a complex network of servers and clients. Photons could be routed to a number of clients using optical switches, and the distance to the server increased using frequency conversion of the photons to telecommunication wavelengths [42] or using recent developments in fiber technology [43]. The photonically interfaced trapped-ion quantum information platform demonstrated here paves the way for secure delegation of confidential quantum computations from a client with minimal quantum resources to a fully capable, but untrusted, quantum server.

We thank Sandia National Laboratories for supplying the HOA2 ion trap used in this experiment, and the developers of the experimental control system ARTIQ [44]. D. P. N. acknowledges support from Merton College, Oxford. D. L. acknowledges support from the ANR project No. SecNISQ. A. M. and D. M. acknowledge support from the U.S. Army Research Office (Grants No. W911NF-20-1-0015 and No. W911NF-18-1-0340). G. A. consults for Nu Quantum Ltd. and acknowledges support from Wolfson College, Oxford. R. S. is partially employed by Oxford Ionics Ltd. and acknowledges funding from an EPSRC Fellowship No. EP/W028026/1 and Balliol College, Oxford. C. J. B. is a director of Oxford Ionics and acknowledges support from a UKRI FL Fellowship. E. K. acknowledges support from EPSRC Grant No. EP/X026167/1. We acknowledge technical and financial support from VeriQloud (of which E. K. is a cofounder) during the initial design of this project, via an industry partnership grant from the NQIT Quantum Technology Hub EP/M013243/1. This work was supported by the UK EPSRC "Quantum Computing and Simulation" Hub EP/T001062/1, and the EU Quantum Technology Flagship Project AQTION (No. 820495).

[1] A. Sarma, R. Chatterjee, K. Gili, and T. Yu, Quantum unsupervised and supervised learning on superconducting processors, Quantum Inf. Comput. **20**, 541 (2019).

[2] J. Alcazar, V. Leyton-Ortega, and A. Perdomo-Ortiz, Classical versus quantum models in machine learning: Insights from a finance application, Mach. Learn. **1**, 035003 (2020).

[3] T. Proctor, K. Rudinger, K. Young, E. Nielsen, and R. Blume-Kohout, Measuring the capabilities of quantum computers, Nat. Phys. **18**, 75 (2022).

[4] D. Amaro, C. Modica, M. Rosenkranz, M. Fiorentini, M. Benedetti, and M. Lubasch, Filtering variational quantum algorithms for combinatorial optimization, Quantum Sci. Technol. **7**, 015021 (2022).

[5] J. J. M. Kirsopp, C. Di Paola, D. Z. Manrique, M. Krompiec, G. Greene-Diniz, W. Guba, A. Meyder, D. Wolf, M. Strahm, and D. Muñoz Ramo, Quantum computational quantification of protein–ligand interactions, Int. J. Quantum Chem. **122**, e26975 (2022).

[6] A. Broadbent, J. Fitzsimons, and E. Kashefi, Universal blind quantum computation, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science* (2009), pp. 517–526, 10.1109/FOCS.2009.36.

[7] J. F. Fitzsimons and E. Kashefi, Unconditionally verifiable blind quantum computation, Phys. Rev. A **96**, 012303 (2017).

[8] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, Verification of quantum computation: An overview of existing approaches, Theory Comput. Syst. **63**, 715 (2019).

[9] C. Badertscher, A. Cojocaru, L. Colisson, E. Kashefi, D. Leichtle, A. Mantri, and P. Wallden, Security limitations of classical-client delegated quantum computing, in *Advances in Cryptology—ASIACRYPT 2020*, edited by S. Moriai and H. Wang (Springer International Publishing, New York, 2020), pp. 667–696, 10.1007/978-3-030-64834-3_23.

[10] A. Cojocaru, L. Colisson, E. Kashefi, and P. Wallden, On the possibility of classical client blind quantum computing, Cryptography **5**, 3 (2021).

[11] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Demonstration of blind quantum computing, Science **335**, 303 (2012).

[12] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, Experimental verification of quantum computation, Nat. Phys. **9**, 727 (2013).

[13] K. A. G. Fisher, A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. J. Resch, Quantum computing on encrypted data, Nat. Commun. **5**, 3074 (2014).

[14] C. Greganti, M.-C. Roehsner, S. Barz, T. Morimae, and P. Walther, Demonstration of measurement-only blind quantum computing, New J. Phys. **18**, 013020 (2016).

[15] Y. Li, P. C. Humphreys, G. J. Mendoza, and S. C. Benjamin, Resource costs for fault-tolerant linear optical quantum computing, Phys. Rev. X **5**, 041007 (2015).

[16] W. Pfaff, B. J. Hensen, H. Bernien, S. B. van Dam, M. S. Blok, T. H. Taminiau, M. J. Tiggelman, R. N. Schouten, M. Markham, D. J. Twitchen, and R. Hanson, Unconditional quantum teleportation between distant solid-state quantum bits, Science **345**, 532 (2014).

[17] D. Hucul, I. V. Inlek, G. Vittorini, C. Crocker, S. Debnath, S. M. Clark, and C. Monroe, Modular entanglement of atomic qubits using photons and phonons, Nat. Phys. **11**, 37 (2015).

[18] N. Kalb, A. A. Reiserer, P. C. Humphreys, J. J. W. Bakermans, S. J. Kamerling, N. H. Nickerson, S. C. Benjamin, D. J. Twitchen, M. Markham, and R. Hanson, Entanglement distillation between solid-state quantum network nodes, Science **356**, 928 (2017).

[19] P.-J. Stas, Y. Q. Huan, B. Machielse, E. N. Knall, A. Suleymanzade, B. Pingault, M. Sutula, S. W. Ding, C. M. Knaut, D. R. Assumpcao, Y.-C. Wei, M. K. Bhaskar, R. Riedinger, D. D. Sukachev, H. Park, M. Lončar, D. S. Levonian, and M. D. Lukin, Robust multi-qubit quantum network node with integrated error detection, Science **378**, 557 (2022).

[20] T. Wilk, S. C. Webster, A. Kuhn, and G. Rempe, Single-atom single-photon quantum interface, Science **317**, 488 (2007).

[21] P. Drmota, D. Main, D. P. Nadlinger, B. C. Nichol, M. A. Weber, E. M. Ainley, A. Agrawal, R. Srinivas, G. Araneda, C. J. Ballance, and D. M. Lucas, Robust quantum memory in a trapped-ion quantum network node, Phys. Rev. Lett. **130**, 090803 (2023).

[22] D. Leichtle, L. Music, E. Kashefi, and H. Ollivier, Verifying BQP computations on noisy devices with minimal overhead, PRX Quantum **2**, 040302 (2021).

[23] R. Raussendorf and H. J. Briegel, A one-way quantum computer, Phys. Rev. Lett. **86**, 5188 (2001).

[24] M. A. Nielsen, Cluster-state quantum computation, Rep. Math. Phys. **57**, 147 (2006).

[25] A. M. Childs, D. W. Leung, and M. A. Nielsen, Unified derivations of measurement-based schemes for quantum computation, Phys. Rev. A **71**, 032318 (2005).

[26] T. Morimae and K. Fujii, Blind quantum computation protocol in which Alice only makes measurements, Phys. Rev. A **87**, 050301(R) (2013).

[27] J. F. Fitzsimons, Private quantum computation: An introduction to blind quantum computing and related protocols, npj Quantum Inf. **3**, 23 (2017).

[28] D. Aharonov, M. Ben-Or, E. Eban, and U. Mahadev, Interactive proofs for quantum computations, arXiv:1704.04487.

[29] A. Broadbent, How to verify a quantum computation, Theory Comput. **14**, 1 (2018).

[30] A. Mantri, T. F. Demarie, and J. F. Fitzsimons, Universality of quantum computation with cluster states and (x, y)-plane measurements, Sci. Rep. **7**, 42861 (2017).

[31] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and W. K. Wootters, Remote state preparation, Phys. Rev. Lett. **87**, 077902 (2001).

[32] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.132.150604 for details on experimental methods, the apparatus, and a quantitative analysis of information leakage from the client to the server, which includes Refs. [33–36].

[33] T.-M. Tomescu, Qubit encryption by rotation of polarization states, Master's thesis, University of Oxford, 2019.

[34] J. G. Ziegler and N. B. Nichols, Optimum settings for automatic controllers, Trans. ASME **64**, 759 (1942).

[35] B. N. Simon, C. M. Chandrashekar, and S. Simon, Hamilton's turns as a visual tool kit for designing single-qubit unitary gates, Phys. Rev. A **85**, 022323 (2012).

[36] J. Řeháček, Z. Hradil, E. Knill, and A. I. Lvovsky, Diluted maximum-likelihood algorithm for quantum tomography, Phys. Rev. A **75**, 042108 (2007).

[37] B. B. Blinov, D. L. Moehring, L.-M. Duan, and C. Monroe, Observation of entanglement between a single trapped atom and a single photon, Nature (London) **428**, 153 (2004).

[38] L. J. Stephenson, D. P. Nadlinger, B. C. Nichol, S. An, P. Drmota, T. G. Ballance, K. Thirumalai, J. F. Goodwin, D. M. Lucas, and C. J. Ballance, High-rate, high-fidelity entanglement of qubits across an elementary quantum network, Phys. Rev. Lett. **124**, 110501 (2020).

[39] K. Wright *et al.*, Benchmarking an 11-qubit quantum computer, Nat. Commun. **10**, 5464 (2019).

[40] J. Keller, T. Burgermeister, D. Kalincev, A. Didier, A. P. Kulosa, T. Nordmann, J. Kiethe, and T. E. Mehlstäubler, Controlling systematic frequency uncertainties at the 10^{-19} level in linear coulomb crystals, Phys. Rev. A **99**, 013405 (2019).

[41] A. C. Hughes, V. M. Schäfer, K. Thirumalai, D. P. Nadlinger, S. R. Woodrow, D. M. Lucas, and C. J. Ballance, Benchmarking a high-fidelity mixed-species entangling gate, Phys. Rev. Lett. **125**, 080504 (2020).

[42] V. Krutyanskiy, M. Meraner, J. Schupp, V. Krcmarsky, H. Hainzer, and B. P. Lanyon, Light-matter entanglement over 50 km of optical fibre, npj Quantum Inf. **5**, 72 (2019).

[43] E. N. Fokoua, S. A. Mousavi, G. T. Jasion, D. J. Richardson, and F. Poletti, Loss in hollow-core optical fibers: Mechanisms, scaling rules, and limits, Adv. Opt. Photonics **15**, 1 (2023).

[44] S. Bourdeauducq *et al.*, m-labs/artiq: 6.0 (Version 6.0) (2021), 10.5281/zenodo.1492176.