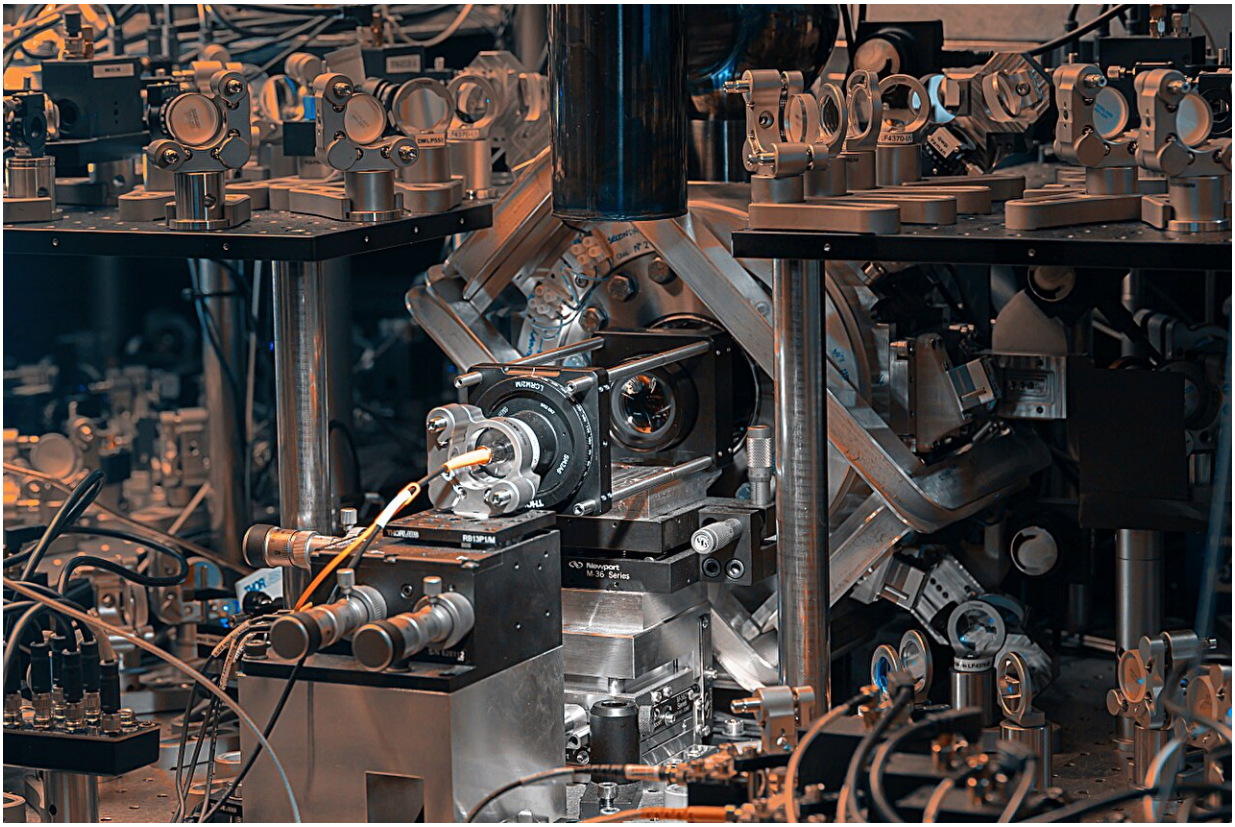
The experimental demonstration of a verifiable blind quantum computing protocol

April 13 2024, by Ingrid Fadelli



Photograph of the photonically networked trapped-ion quantum processor server at the University of Oxford, Credits: David Nadlinger.

Quantum computers, systems that process and store information leveraging quantum mechanical phenomena, could eventually

outperform classical computers on numerous tasks. Among other things, these computers could allow researchers to tackle complex optimization problems, speed up drug discovery and better protect users against cyber-security threats.

Despite their advantages, most existing quantum computers are still only accessible to a limited number of people worldwide. Computer scientists have thus been trying to develop approaches that could facilitate their widespread use in the near term, for instance using cloud-based systems that allow remote access to quantum servers.

While cloud-based approaches could broaden people's access to quantum computing, they also pose significant privacy and security risks, as the information and activity of users could be maliciously accessed. In recent years, some studies introduced approaches that could overcome these limitations, allowing servers to conceal a client's algorithms, as well as the information fed or produced by a cloud-based quantum computing system.

Researchers at University of Oxford recently set out to experimentally test a proposed approach for realizing verifiable blind quantum computing. Their paper, published in *Physical Review Letters*, validates the promise of this approach for enhancing the safety of cloud-based quantum computing platforms.

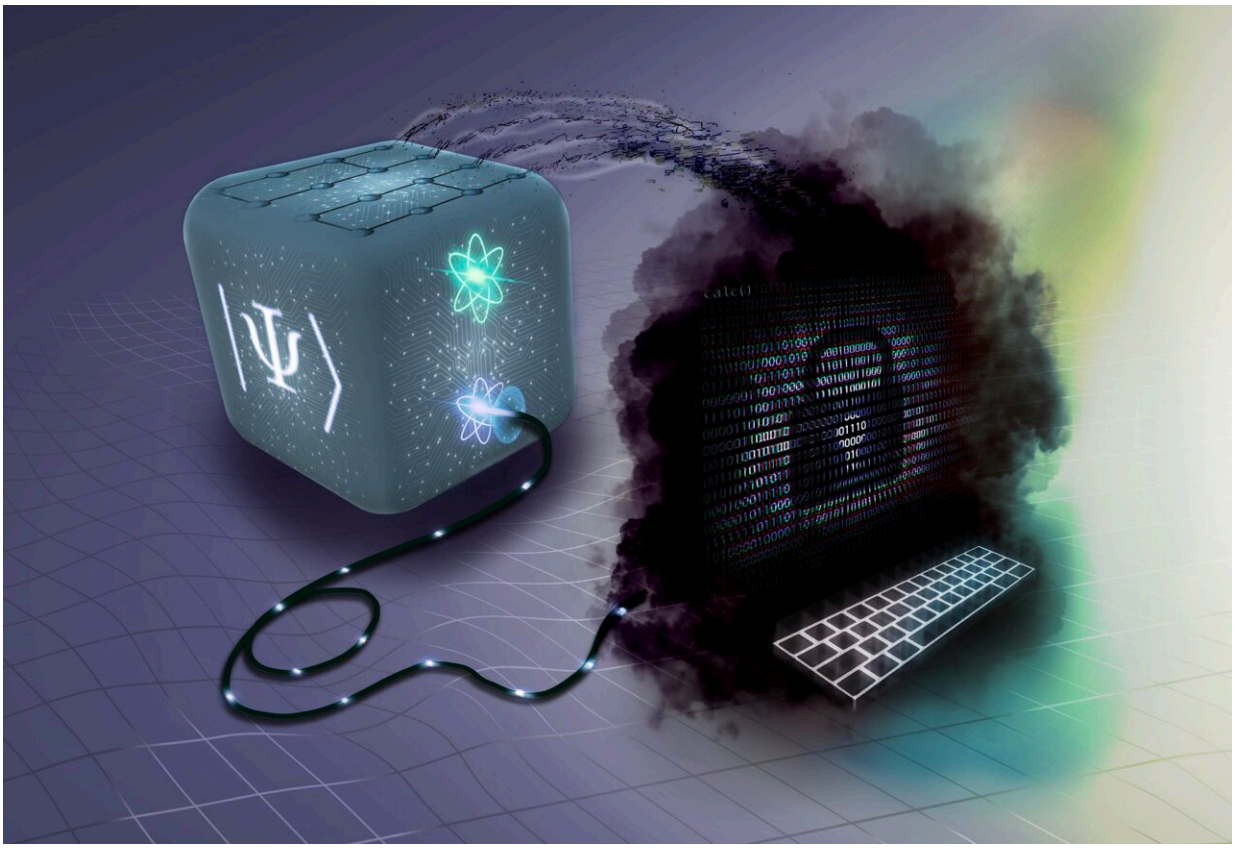
"At the University of Oxford, we have been building one of the most sophisticated quantum networks in the world," Gabriel Araneda, co-author of the paper, told Phys.org.

"We have been able to demonstrate several milestones in the field of quantum networking, including the first complete realization of a device-independent quantum key distribution between remote systems, and the first quantum network of remotely entangled atomic clocks."

In their recent paper, Araneda, Peter Drmota and their collaborators specifically focused on the task of safely delegating quantum computations performed by a client to an untrusted quantum server via a network link.

"Blind quantum computing has been proposed as a solution to secure cloud computing, where clients can delegate computations to a quantum server without revealing the algorithm or the processed data," Drmota said. "Moreover, the client can verify whether the result obtained from the server is correct—a significant challenge if a problem cannot be approached efficiently by any other means."

Until a few years ago, theoretical proposals for realizing secure cloud-based quantum computing did not take the imperfections of devices into account. As quantum computers are known to have numerous inherent imperfections, these proposals ultimately proved ineffective and vulnerable to noise.



Artistic rendering of blind quantum computing. Credits: Helene Hainzer.

A paper by Dominik Leichtle and his colleagues at Sorbonne University and Edinburgh University introduced an efficient blind verification protocol for delegating quantum computations. As part of their study, Drmota and his colleagues at Oxford University set out to apply this protocol in an experimental setting, using a system of trapped ions connected to a client-accessible photonic detection system via a quantum fiber link.

"The protocol for blind quantum computing is difficult to implement because every step incurs a correction to be applied to subsequent steps," David Nadlinger, co-author of the paper, explained. "It is therefore

interactive and requires real-time feedforward of information to keep the computation in line with the intended algorithm."

Previous realizations of the blind quantum computing protocol utilized photons both for performing computations and for communicating with clients. These purely photonic implementations were unable to perform entangling gates deterministically and lacked real-time feedforward information.

This means that they required the post-selection of outcomes, which greatly reduces their effectiveness for real-world applications. Drmota and his colleagues realized the blind quantum computing protocol differently and were able to overcome these issues.

"We employ a robust memory qubit in our server, which can be entangled deterministically with a second qubit and allows us to store quantum information while the devices perform the real-time feedforward operations," Drmota said.

"The primary objective of this experiment was to eliminate the efficiency and security limitations of earlier implementations. We achieve deterministic protocol success by using fast, adaptive hardware at the client and a memory qubit at the server that can be entangled deterministically with the network qubit."

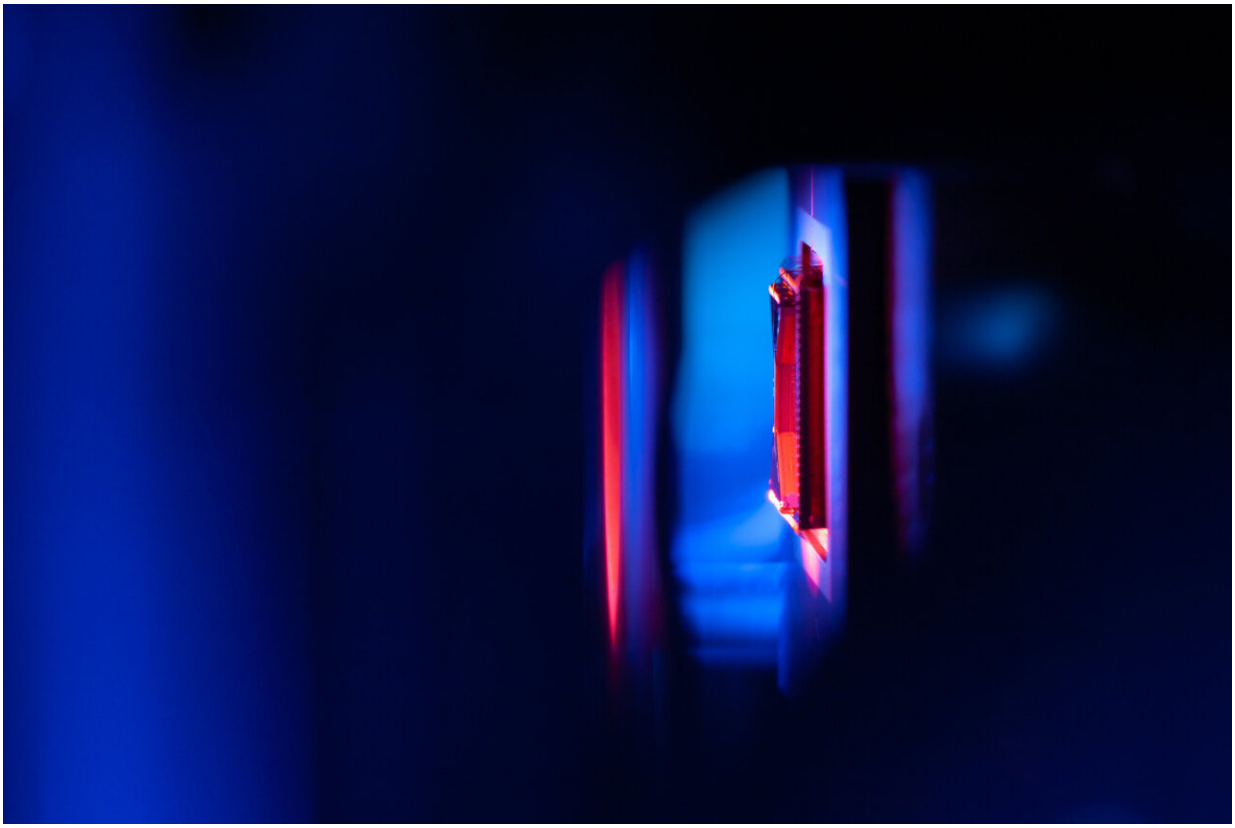
To perform their experiment, the researchers used a trapped-ion quantum processor that was networked to a client's device via a fiber-optic quantum link. Their developed system essentially relies on a network qubit entangled with single photons that are sent to clients via an optical fiber, as well as a memory qubit that stores the current state of a computation.

"The client operates a much simpler device: a photon detector,

specifically built to measure the polarization of the incoming photons in an arbitrary switchable basis," Araneda said.

"The measurement of the photon collapses the wavefunction of the entangled state between the photon and the network qubit, thus 'steering' the state of the network qubit into a state known exclusively to the client."

The process through which the state of the quantum qubit is "steered" into a state only known to clients is referred to as "remote state preparation." This process is what ultimately leads to the server being 'blind' to the state of its own qubits.



Photograph of the ion trap inside the vacuum chamber as part of the quantum server", credits: David Nadlinger.

"The availability of a memory qubit in the server with coherence times exceeding 10 seconds enables the client to react in real-time to intermediate results obtained from the server by adjusting the basis of the polarization analyzer mid-computation," the researchers explained.

"Combined with the ability to deterministically entangle the qubits in the server, every attempt at a computation succeeds deterministically and no post-selection is required."

The researchers' demonstration of a blind verification protocol could soon open new possibilities for the implementation of cloud-based quantum computing services. As quantum computers are advanced technologies that are difficult to deploy on a large-scale, their reliable remote operation will most likely be the most viable route to enable their widespread use in the short-term.

"Our experiment shows how quantum computing costumers can access the processing power of remote quantum computers privately and securely," Drmota said. "Using a quantum link from home, by means of a simple measurement device, all the processed data and the algorithm itself can be protected by the laws of quantum mechanics. Furthermore, we show how the client can verify that the results obtained from the server are correct."

The recent work by Drmota and his collaborators is a significant contribution to the rapidly advancing field of quantum computing. Other research teams could soon draw inspiration from their proposed approach, which could lead to further proposals and developments.

"From the technical point of view, interfacing three different qubits, a photon, a calcium ion, and a strontium ion, is challenging and comes

with significant experimental complexity," the researchers said.

"We managed to combine all the necessary tools to implement blind quantum computing in a realistic setting, where all the client's hardware is controlled independently from the server and the computations are executed with real-time feedforward of classical information while quantum information is stored on a memory qubit."

In their next studies, Drmota and his collaborators plan to continue building on their system. For instance, they could extend their approach to perform larger computations, using previously proposed systems that can be upscaled (i.e., increasing the number of memory qubits and the fidelity of local operations).

"The distance between the server and the client could also be extended to city-scale networks using proven techniques to convert the photons to telecommunication wavelengths," Araneda added.

"Moreover, the number of clients can also be increased by using optical switches, routing the photons emitted by the quantum processor to different clients. In collaboration with Prof. Elham Kashefi and the UK National Quantum Computing Centre, we are going to explore future avenues for verifying quantum computations on different experimental platforms that admit state-of-the-art levels of noise."

More information: P. Drmota et al, Verifiable Blind Quantum Computing with Trapped Ions and Single Photons, *Physical Review Letters* (2024). DOI: 10.1103/PhysRevLett.132.150604