Cloud Computing under the Cover of Quantum

A secure method for cloud-based quantum computing harnesses the power of quantum physics to keep data confidential.

By **Michael Schirber**

Progress in quantum technology has been swift, but we still are far from the day when everyone will have a quantum computer in their house or at their business. The early stages of quantum computing will likely rely on a quantum version of the "cloud," where users send data and computing tasks to a state-of-the-art quantum machine hosted by Google, IBM, or another company. But is that approach secure? It can be, thanks to the impenetrable secrecy of quantum-based protocols. A recent experiment demonstrates a version of "blind quantum computing" using trapped ions [**1**].

Plugging into a cloud-based quantum computer could be made more secure using a "blind" protocol that hides a client's data and programs.
Credit: Oxford University

The protocol is scalable, meaning it offers potential to be incorporated into larger and larger quantum computing systems.

Quantum computers have the potential to be game changers in computationally intensive tasks such as drug discovery and material design. In these highly competitive sectors, there would be concerns about using a cloud-based quantum computer. "A company searching for a new wonder drug or for a high-performance battery material wouldn't want to reveal confidential secrets," explains Peter Drmota of the University of Oxford, UK. However, it has been shown—in theory—that one can perform computations on a remote quantum computer while hiding the data and the operations done on such data. "Blind quantum computing could give a client confidence to use whoever's quantum computer," Drmota says.

Several groups have previously explored blind quantum computing using photonic schemes. The main disadvantage of these setups is that they are probabilistic, which means that quantum entanglement operations sometimes fail and sometimes succeed, so users must run multiple trials and postselect the desired output. "The lack of deterministic entangling operations makes it challenging to perform blind quantum computing using only photons," says Joe Fitzsimons from Horizon Quantum Computing, a company developing integration software for quantum computers. Fitzsimons, who was not involved in the present study, says that the community has been waiting for a demonstration of blind quantum computing using matter-based—as opposed to photon-based—qubits.

Drmota and his colleagues have delivered such a demonstration

with a simple blind quantum computing setup that uses just two trapped ions: a strontium ion and a calcium ion. The strontium ion acts as the network qubit that sends photons to a "client," while the calcium ion—with its long coherence times—works as a memory qubit. Together the two ions form the "server" of the quantum cloud system.

The team's blind computing protocol begins by having the network qubit send a photon to the client over an optical fiber. The photon's polarization is dependent on the network ion's electronic state, which means the two objects are quantum entangled. The client uses that entanglement to "steer" the ion's state through measurements of the photon's state (see **Synopsis: Quantum Steering That's Robust to Loss and Noise**). Specifically, the client measures the polarization of the photon, choosing secretly the orientation of the polarization measuring device. Through this measurement, the client prepares the state of the network qubit. "The state of the entire system 'collapses' into a particular state that only the client knows," says team member Dominik Leichtle from Sorbonne University in France. "Since the server doesn't know about the measurement, it doesn't know which state the network qubit ends up in."

The server is able, however, to process the network qubit's information by performing a laser-based process that entangles the network qubit with the memory qubit. The memory qubit stores information that can be used in subsequent iterations of the protocol. The client continues the computation by sending a message over a normal communication line to the server, directing it to measure the spin of the network qubit along a particular axis and to send the results back to the client. The whole process then repeats, with the server sending another photon to the client.

To further ensure the security of the protocol, the team encodes information using a so-called one-time-pad encryption. In this approach, the client generates a list of random numbers that are added as extra rotations to the instructions sent to the server. "Everything that goes out from the client is gibberish, and everything returned to the client is gibberish," Drmota says. Thanks to this encryption, the server is unaware of what the data mean and even of what the operations are. But the client can decrypt the gibberish with its list of random numbers.

The client also has a way to check that the computation is being done correctly. Such verification is important for instilling trust in a quantum computer that is out of our hands or is susceptible to errors, Leichtle says. Previous work devised verification methods, but they typically required a lot of computer resources. Leichtle and his colleagues developed a more efficient protocol, which involves interspersing the real data with dummy data and performing tests on these dummy inputs [**2**]. The researchers implemented this protocol on the two-ion system and showed that a client could verify that the quantum computations are reliable.

In this first demonstration, the team showed that the client can direct the server to perform a simple quantum operation called a qubit rotation. After analyzing and decrypting the data, the client recovered a fringe pattern, which was the expected result. The trapped-ion system can be made more powerful—computing more difficult operations—by introducing more memory qubits. Connecting all these qubits together will not be simple, but quantum-information scientists have shown that they can connect several tens of trapped ions together, and proposals for 1000-ion systems have been made (see **Synopsis: Efficient Control of Trapped Ions**). Drmota and Leichtle say that, as this hardware advances, their blind quantum computing algorithm can "scale" accordingly. "What we mean by 'scalable' is that the interface and the client apparatus don't change no matter how big the server becomes," Drmota says.

"The recent demonstration of blind quantum computing using trapped ions and photonic detection represents a significant milestone toward scalable and secure quantum communication," says quantum-information expert Anne Broadbent from the University of Ottawa, Canada. "As we move closer to practical deployment, these developments pave the way for a quantum Internet that ensures privacy and verifiability." Fitzsimons agrees, adding that the researchers overcame significant technical challenges to connect matter qubits to a photon-based communication network. "However, the current demonstration is still limited to a small number of qubits and further work will be needed to make blind quantum computing available on quantum processors with higher qubit counts," he says.

Michael Schirber is a Corresponding Editor for *Physics Magazine* based in Lyon, France.

REFERENCES

1. P. Drmota *et al.*, "Verifiable blind quantum computing with trapped ions and single photons," **Phys. Rev. Lett. 132, 150604 (2024).**
2. D. Leichtle *et al.*, "Verifying BQP computations on noisy devices with minimal overhead," **PRX Quantum 2, 040302 (2021).**