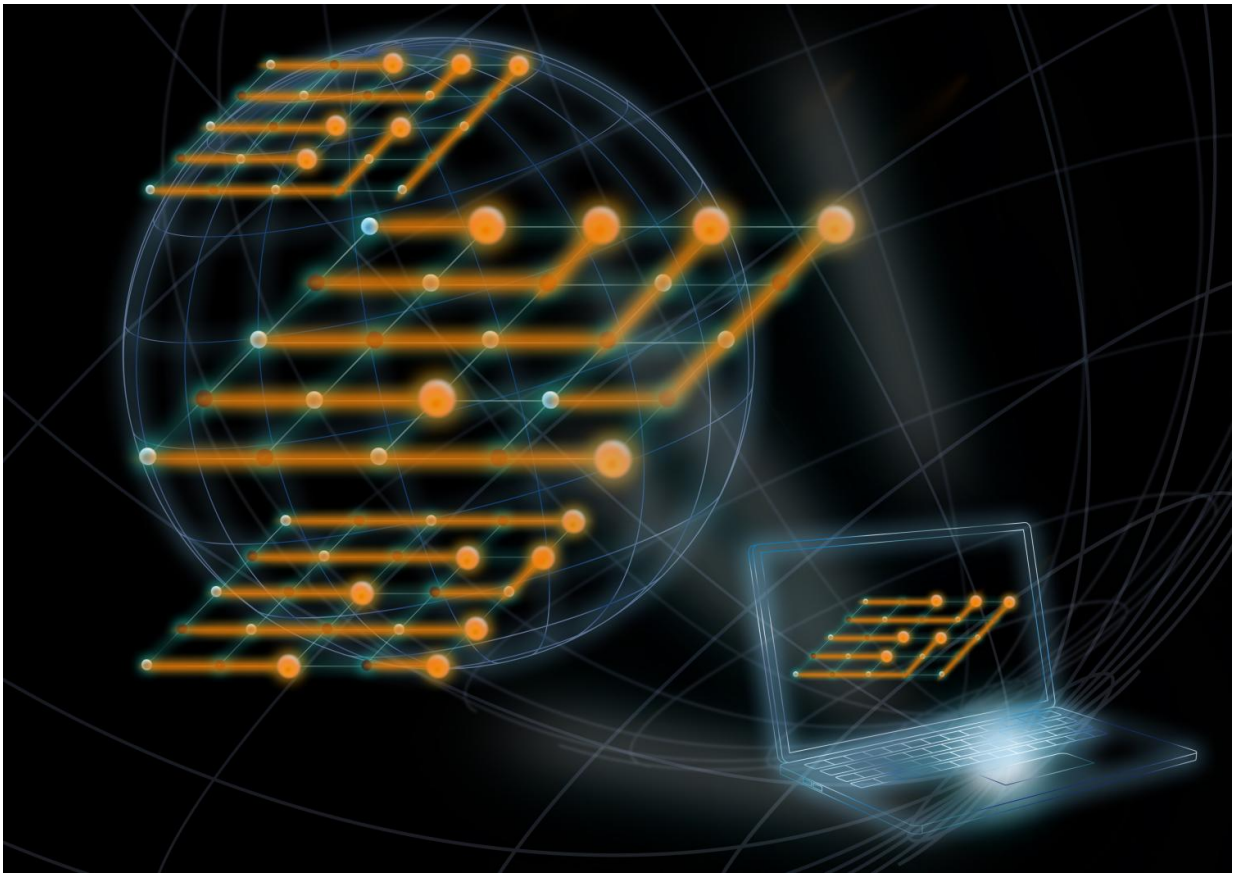
Why you might trust a quantum computer with secrets—even over the internet

July 12 2017



It may be possible to control a quantum computer over the internet without revealing what you are calculating, thanks to the many possible ways that information can flow through a computation. That's the conclusion of researchers in Singapore and Australia who studied the measurement-based model of quantum computing, reported 11 July in the open-access journal *Physical Review X*. Credit: Timothy Yeo / Centre for Quantum Technologies, National University of Singapore

Here's the scenario: you have sensitive data and a problem that only a quantum computer can solve. You have no quantum devices yourself. You could buy time on a quantum computer, but you don't want to give away your secrets. What can you do?

Writing in *Physical Review X* on 11 July, researchers in Singapore and Australia propose a way you could use a quantum computer securely, even over the internet. The technique could hide both your data and program from the computer itself. Their work counters earlier hints that such a feat is impossible.

The scenario is not far-fetched. Quantum computers promise new routes to solving problems in cryptography, modelling and machine learning, exciting government and industry. Such problems may involve confidential data or be commercially sensitive.

Technology giants are already investing in building such computers—and making them available to users. For example, IBM announced on 17 May this year that it is making a quantum computer with 16 quantum bits accessible to the public for free on the cloud, as well as a 17-qubit prototype commercial processor.

Seventeen qubits are not enough to outperform the world's current supercomputers, but as quantum computers gain qubits, they are expected to exceed the capabilities of any machine we have today. That should drive demand for access.

"We're looking at what's possible if you're someone just interacting with a quantum computer across the internet from your laptop. We find that it's possible to hide some interesting computations," says Joseph Fitzsimons, a Principal Investigator at the Centre for Quantum

Technologies (CQT) at the National University of Singapore and Associate Professor at Singapore University of Technology and Design (SUTD), who led the work.

Quantum computers work by processing bits of information stored in quantum states. Unlike the binary bits found in our regular (i.e., classical) computers, each a 0 or 1, qubits can be in superpositions of 0 and 1. The qubits can also be entangled, which is believed to be crucial to a quantum computer's power.

The scheme designed by Fitzsimons and his colleagues brings secrecy to a form of quantum computing driven by measurements.

In this scheme, the quantum computer is prepared by putting all its qubits into a special type of entangled state. Then the computation is carried out by measuring the qubits one by one. The user provides step-wise instructions for each measurement: the steps encode both the input data and the program.

Researchers have shown previously that users who can make or measure qubits to convey instructions to the quantum computer could disguise their computation. The new paper extends that power to users who can only send classical bits - i.e. most of us, for now.

This is surprising because some computer science theorems imply that encrypted quantum computation is impossible when only classical communication is available.

The hope for security comes from the quantum computer not knowing which steps of the measurement sequence do what. The quantum computer can't tell which qubits were used for inputs, which for operations and which for outputs.

"It's extremely exciting. You can use this unique feature of the measurement-based model of quantum computing—the way information flows through the state—as a crypto tool to hide information from the server," says team member Tommaso Demarie of CQT and SUTD.

Although the owner of the quantum computer could try to reverse engineer the sequence of measurements performed, ambiguity about the role of each step leads to many possible interpretations of what calculation was done. The true calculation is hidden among the many, like a needle in a haystack.

The set of interpretations grows rapidly with the number of qubits. "The set of all possible computations is exponentially large - that's one of the things we prove in the paper—and therefore the chance of guessing the real computation is exponentially small," says Fitzsimons. One question remains: could meaningful computations be so rare among all the possible ones that the guessing gets easier? That's what the researchers need to check next.

Nicolas Menicucci at the Centre for Quantum Computation and Communication Technology at RMIT University in Melbourne, Australia, and Atul Mantri at SUTD, are coauthors on the work.

"Quantum computers became famous in the '90s with the discovery that they could break some classical cryptography schemes—but maybe quantum computing will instead be known for making the future of cloud computing secure," says Mantri.

More information: Atul Mantri et al, Flow Ambiguity: A Path Towards Classically Driven Blind Quantum Computation, *Physical Review X* (2017). DOI: 10.1103/PhysRevX.7.031004

Provided by National University of Singapore