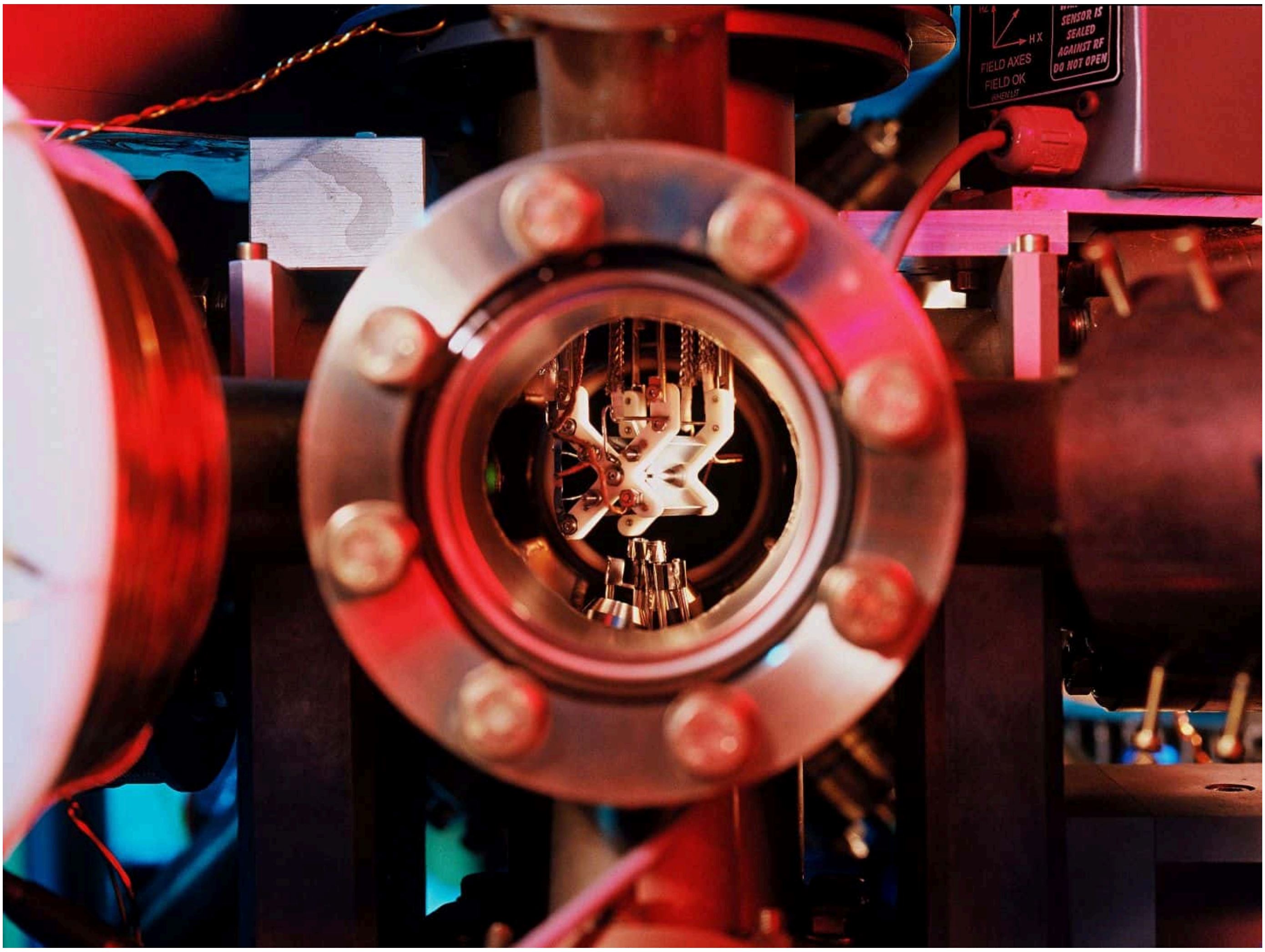
Advertisement

physicsworld

QUANTUM COMPUTING | RESEARCH UPDATE

# Can a classical computer tell if a quantum computer is telling the truth?

11 Mar 2024



Quantum verification: The trapped-ion quantum computer used in the experiment. (Courtesy: C Lackner/UIBK)

Quantum computers can solve problems that would be impossible for classical machines, but this ability comes with a caveat: if a quantum computer gives you an answer, how do you know it's correct? This is particularly pressing if you do not have direct access to the quantum computer (as in cloud computing), or you don't trust the person running it. You could, of course, verify the solution with your own quantum processor, but not everyone has one to hand.

So, is there a way for a *classical* computer to verify the outcome of a quantum computation? Researchers in Austria say the answer is yes. Working at the University of Innsbruck, the Austrian Academy of Sciences and Alpine Quantum Technologies GmbH, the team experimentally executed a process termed Mahadev's protocol, which is based on so-called post-quantum secure functions. These functions involve calculations that are too complex for even a quantum computer to crack, but with a "trapdoor" that allows a classical machine with the correct key to solve them easily. The team say these trapdoor calculations could verify the trustworthiness of a quantum computation using only a classical machine.

### Honest Bob?

To understand how the protocol works, assume we have two parties. One of them, traditionally known as Alice, has the trapdoor information and wants to verify that a quantum computation is correct. The other, known as Bob, does not have the trapdoor information, and needs to prove that the calculations on his quantum computer can be trusted.

As a first step, Alice prepares a specific task for Bob to handle. Bob then reports the outcome to Alice. Alice could verify this outcome herself with a quantum computer, but if she wants to use a classical one, she needs to give Bob further information. Bob uses this information to entangle several of his main quantum bits (or qubits) with additional ones. If Bob performs a measurement on some of the qubits, this determines the state of the remaining qubits. While Bob does not know the state of the qubits in advance of the measurements, Alice, thanks to her trapdoor calculations, does. This means Alice can ask Bob to verify the qubits’ state and decide, based on his answer, whether his quantum computer is trustworthy.

BLUEFORS
Gas Handling System Generation 2
The Next Era of Cryogenics and Quantum Technology Starts Here
Learn More

**Relieved Alice**

The team ran this protocol on a quantum processor that uses eight trapped $^{40}\text{Ca}^{+}$ ions as qubits. The measurements Bob makes relate to the energy of the qubits’ quantum states. To obtain a signal above background noise, the researchers ran the protocol 2000 times for each data point, ultimately proving that Bob’s answers could be trusted.

The researchers call their demonstration a proof of concept and acknowledge that more work is needed to make it practical. Additionally, a full, secure verification would require more than 100 qubits, which is out of scope for most of today’s processors. According to Barbara Kraus, one of the team’s leaders and now a quantum algorithms expert at the Technical University of Munich, Germany, even the simplified version of the protocol was challenging to implement. This is because verifying the output of a quantum computation is experimentally much more demanding than doing the computation, as it requires entangling more qubits.

Nonetheless, the demonstrated protocol contains all the steps required for a complete verification, and the researchers plan to develop it further. “An important task concerning the verification of quantum computations and simulations is to develop practical verification protocols with a high security level,” Kraus tells *Physics World*.

Andru Gheorghiu, a quantum computing expert from the Chalmers University of Technology in Sweden who was not involved in the research, calls it an important first step towards being able to verify general quantum computations. However, he notes that it currently only works for verifying a simple, one-qubit computation that could be reproduced with an ordinary laptop. Still, he says it offers insights into the challenges of trying to scale up to larger computations.

The research appears in *Quantum Science and Technology*.

**Martijn Boerkamp** is a science writer based in the Netherlands

Copyright © 2024 by IOP Publishing Ltd and individual contributors

EXPLORE PHYSICS WORLD

About us
Our team
Our portfolio
Advertising
Contact us
Feedback
Sign in
Register

MORE INFORMATION

Institute of Physics
Join the Institute
Modern Slavery Act
Privacy and Cookies
IOP Publishing
Copyright
Terms and Conditions
Disclaimer

OUR MISSION

*Physics World* represents a key part of IOP Publishing's mission to communicate world-class research and innovation to the widest possible audience. The website forms part of the ***Physics World* portfolio**, a collection of online, digital and print information services for the global scientific community.

BACK TO TOP