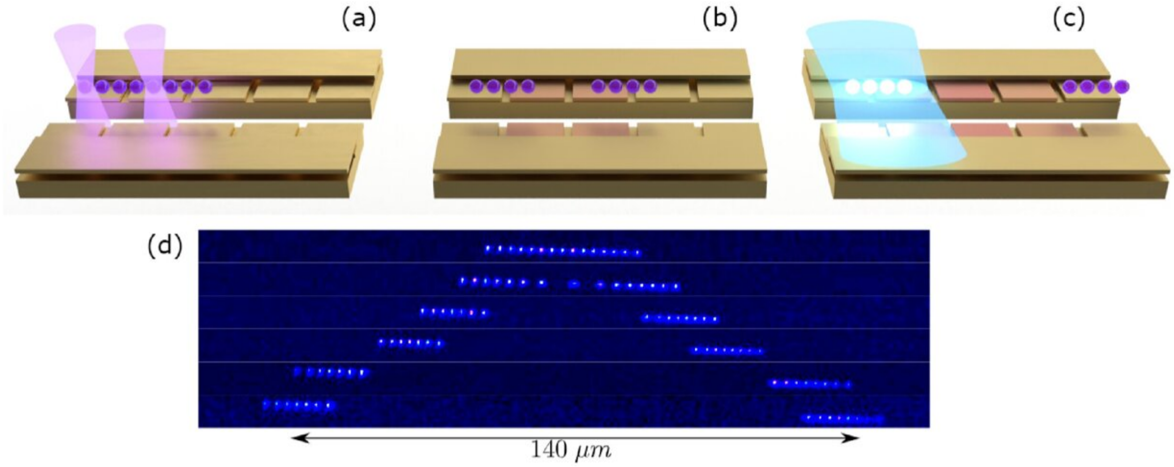
A new protocol to reliably demonstrate quantum computational advantage

August 30 2023, by Ingrid Fadelli



Credit: Vivian Uhlir, Zhu et al

Quantum computers, devices that perform computations by exploiting quantum mechanical phenomena, have the potential to outperform classical computers on some tasks and optimization problems. In recent years, research teams at both academic institutions and IT companies have been trying to realize this predicted better performance for specific problems, which is broadly known as "quantum advantage."

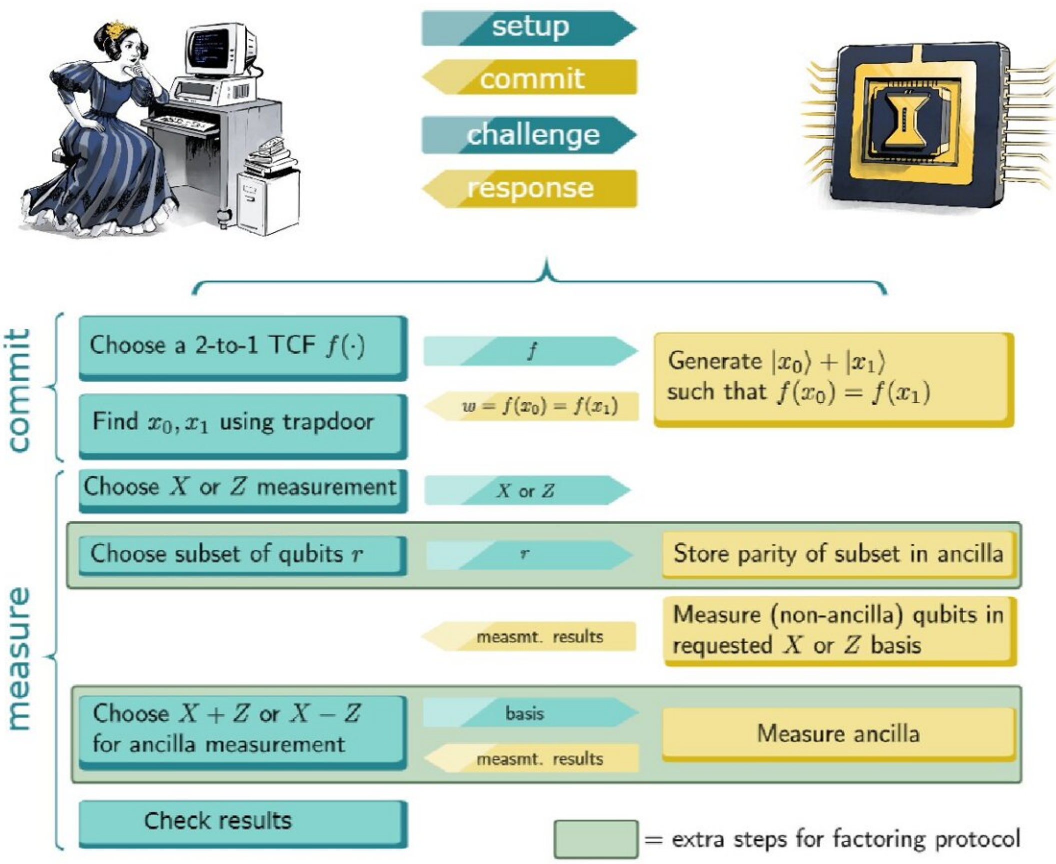
To reliably demonstrate that a quantum computer performs better than a classical computer, one should, among other things, collect precise measurements inside the computer and compare them to those collected in classical computers. Doing this, however, can sometimes be challenging, due to the distinct nature of these two types of devices.

Researchers at NIST/University of Maryland, UC Berkeley, Caltech and other institutes in the United States recently introduced and tested a new protocol that could help to reliably validate the advantage of quantum computers. This protocol, introduced in *Nature Physics*, relies on mid-circuit measurements and a cryptographic technique.

"The ultimate inspiration behind this research, in my opinion, is the question of whether computational advantages provided by quantum computers can be efficiently validated," Daiwei Zhu, one of the researchers who carried out the study, told Phys.org. "In other words, if quantum computers become more powerful than any classical simulation, how can we validate its output via cross-examinations?

"This is a challenge faced by probably all the current demonstrations of quantum advantage. Recent breakthroughs found an answer to this question using the idea of cryptographic interactive proof. "

Cryptographic interactive proofs are essentially interactive protocols through which a classical computer can validate a far more powerful quantum computer via a series of questions and instructions. The protocols used by Zhu and his colleagues were first presented in previous studies by researchers at UC Berkeley (published in *Nature Physics*) and Caltech (published in *Journal of the ACM*). In their recent study, Zhu's team performed a proof-of-principle demonstration of these protocols, using an ion trap quantum computer.



Credit: Vivian Uhlir, Zhu et al

"We arranged the qubits into several segments according to their functions (at what stage do they need to be readout) throughout the interactive computation," Zhu explained. "At each readout stage, we split the target segments apart from the rest of the qubits and shuttle them away to perform readout. This way the coherence/quantum information stored in other segments are preserved for the rest of the computation."

The procedure followed by Zhu and his colleague produced readouts of the target segments (i.e., qubits that they were interested in examining).

These segments were then interactively checked against quantum computations performed, to validate quantum advantage.

"On one hand, we successfully integrated mid-circuit measurements into arbitrary quantum circuits with sufficiently high overall fidelity using long ion chains," Zhu said. "This could be applied to many other interactive algorithms. On the other hand, our demonstration, when suitably scaled to larger systems, promises the efficient verification of quantum computational advantage."

The new protocols introduced and evaluated by this team of researchers has notable advantages over other existing methods to test quantum advantage. For instance, compared to Shor's algorithm, which is also efficiently verifiable, their protocol can be implemented with one order of magnitude fewer quantum gate operations.

In the future, the new interactive protocol could be implemented and evaluated in other experiments. In addition, Zhu and his colleagues hope to devise additional interactive protocols to assess other aspects and dimensions of quantum computing.

"From a theoretical perspective, we are now interested in applying interactive protocols to other tasks such as certifiable random number generation, remote state preparation and verifying arbitrary quantum computations," Zhu added. "Experimentally, using the mid-circuit measurement capability, we are also excited to explore new phenomena, like entanglement phase transitions, as well as the demonstration of coherent feedback protocols, including quantum error correction."

More information: Daiwei Zhu et al, Interactive cryptographic proofs of quantumness using mid-circuit measurements, *Nature Physics* (2023). DOI: 10.1038/s41567-023-02162-9