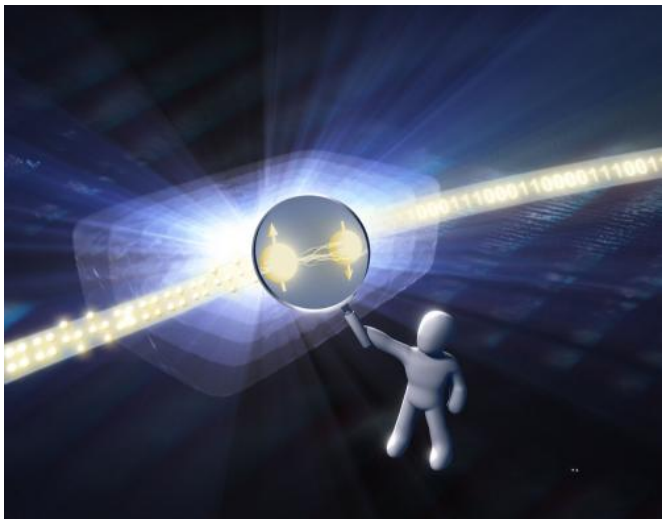
Physicists use blind quantum computing to verify results of quantum computer

30 September 2013, by Bob Yirka



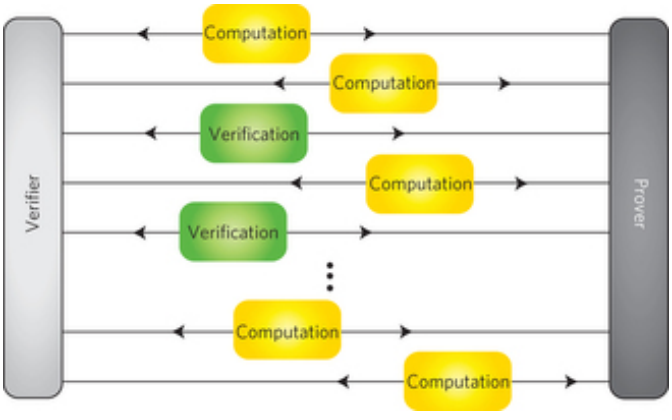
The image is an illustration of the fundamental question: can quantum computations be verified by entities that are inherently unable to compute the results themselves? Credit: EQUINOX GRAPHICS

(Phys.org) —A team of researchers working at the University of Vienna, has developed a technique for verifying results produced by a quantum computer. In their paper published in the journal *Nature Physics*, the researchers explain how their method uses one simple quantum computer to verify results produced by another that is far more powerful.

One of the perplexing puzzles that computer scientists have been struggling with is in figuring out how to prove that results obtained using advanced computers are correct. If a computer is used, for example, to perform a calculation and returns a result that can be had no other way, how can the answer be verified? That question has come up more and more often as scientists move closer to developing true quantum computers—machines that in all likelihood will be able to provide answers to all manner of mysterious questions. But how will we know that the answers they give us, are right?

One idea is to create two different types of computers that arrive at answers using completely different architectures, then set them both to work on the same problem to see if they agree. Such a scenario would be the ideal—unfortunately, at this point, it doesn't appear likely that a new type of architecture capable of keeping up with a quantum computer is likely to come along any time soon, thus, scientists have to look for other options. In this effort by the team in Vienna, the researchers are looking to use a second quantum computer to verify results given by a first, despite being far less powerful.

The team used a method known as blind quantum computing to test a single quantum computation by testing the correctness of measurements performed in obtaining the result. Going about it this way means the computer doing the testing, called the verifier, doesn't have to have the power of the computer being tested, called the server. Quantum blind testing involves using what are known as trap qubits—qubits that are entangled between both of the computers. Verifying (not testing, technically) is done by preparing the trap qubits in a way that is known to the verifier but not the server.



Schematic of a quantum computation with verification sub-routines. Credit: *Nature Physics* (2013) doi:10.1038/nphys2763

A measurement angle (again unknown to the server) for a trap qubit is chosen which is predetermined by the verifier—allowing it to detect measurement errors (called cheating) by the server. The location of the trap bits are chosen randomly, allowing for calculating the probability of cheating errors by the server at different processing points. The end result is a number that represents the probability that the result given by the more powerful quantum computer is correct. Thus, the method involves testing the way an answer is arrived at, rather than whether the answer is itself actually correct.

More information: Experimental verification of quantum computation, *Nature Physics* (2013) DOI: 10.1038/nphys2763

Abstract
Quantum computers are expected to offer substantial speed-ups over their classical counterparts and to solve problems intractable for classical computers. Beyond such practical significance, the concept of quantum computation opens up fundamental questions, among them the issue of whether quantum computations can be certified by entities that are inherently unable to compute the results themselves. Here we present the first experimental verification of quantum computation. We show, in theory and experiment, how a verifier with minimal quantum resources can test a significantly more powerful quantum computer. The new verification protocol introduced here uses the framework of blind quantum computing and is independent of the experimental quantum-computation platform used. In our scheme, the verifier is required only to generate single qubits and transmit them to the quantum computer. We experimentally demonstrate this protocol using four photonic qubits and show how the verifier can test the computer's ability to perform quantum computation.

Press release