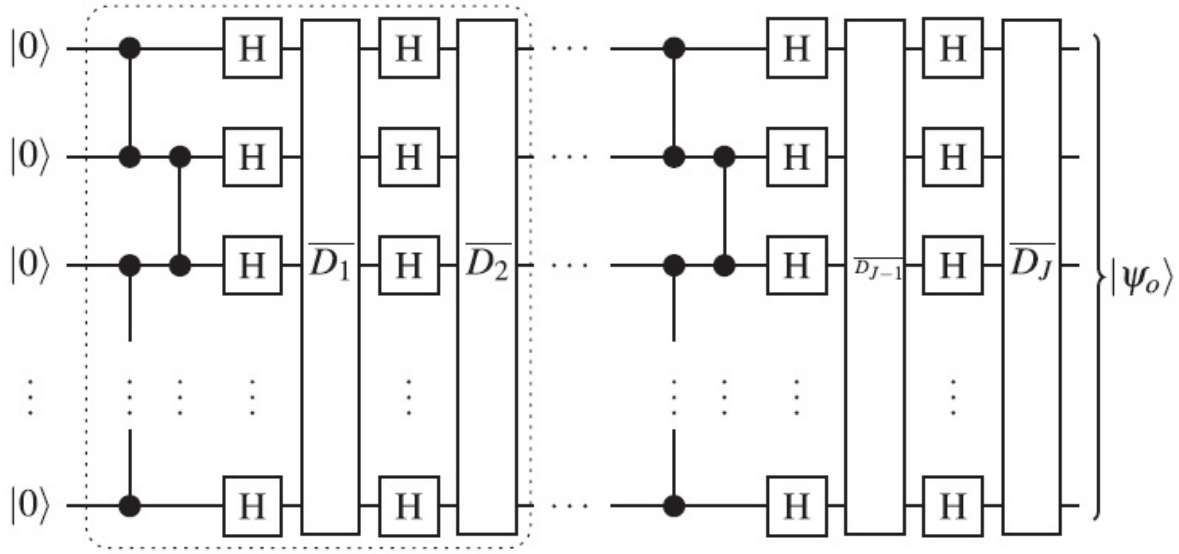
Blind quantum computing method surpasses efficiency 'limit'

June 12 2015, by Lisa Zyga



Blind quantum computation with teleportation protocol. The dotted-line square shows the repeating pattern of operations. Credit: Pérez-Delgado and Fitzsimons. ©2015 American Physical Society

(Phys.org)—Demonstrating that limits were made to be broken, physicists have overcome what was previously considered to be a natural and universal limit on the efficiency of a quantum cryptography task called blind quantum computing. The new method offers significant efficiency improvements and, in some cases, requires exponentially

fewer communication resources to implement than previous methods did.

The physicists, Carlos A. Pérez-Delgado and Joseph F. Fitzsimons at the Singapore University of Technology and Design, have published a paper on the improved blind quantum computing method in a recent issue of *Physical Review Letters*. Fitzsimons is also with the Centre for Quantum Technologies at the National University of Singapore.

As its name suggests, in blind quantum computing, a computer performs a task blindly—the input, computation, and output remain unknown to the computer. The scientists explain that this capability "allows a user to delegate a computation to an untrusted server while keeping the computation hidden." As the technology develops, it is expected to provide greater security than classical protocols for a variety of applications.

Like all computing tasks, blind quantum computing requires a minimum number of qubits, gates, and other communication resources in order to perform a computation. Recent research has suggested that there is a natural lower limit on these communication requirements, which is based on the so-called "no-programming theorem." Because this lower bound suggests that blind quantum computing protocols will always require a certain minimum amount of resources, it effectively limits the efficiency with which these protocols can be carried out.

Teleportation for error correction

In the new paper, the physicists have shown that this limit holds only in certain scenarios, and it can be overcome by using a technique called "iterated gate teleportation." The technique is based on standard gate teleportation, in which quantum states are rapidly transmitted from one gate to another by taking advantage of quantum entanglement between

the gates. In the iterated version, additional gate teleportation steps are repeatedly carried out to correct errors based on the results of the preceding teleportation steps.

"The really important part of gate teleportation is that it provides a way to perform the desired computation on one half of an entangled state before the desired input is even known, resulting in a special resource state," Fitzsimons told *Phys.org*. "Once you have the input, you can perform a special set of measurements between the input and the resource state. For one possible outcome of the measurements, the effect is to perform the encoded computation on the chosen input. However, it is impossible to control which measurement outcome you get, and any other outcome results in some unwanted error which needs to be corrected. Our iterated teleportation protocol is simply using teleportations to correct errors introduced by previous teleportation steps in such a way that the errors diminish each round and eventually disappear."

The physicists showed that just a few of these additional teleportation steps can correct errors that would otherwise need to be corrected using many more resources. In this way, the technique exponentially reduces the amount of communication requirements, even below the minimum required by the no-programming theorem limit.

"To me, at least, this is quite a surprising result, as it had been previously proved that for deterministic computation, programs encoded using quantum states are no shorter than those encoded using classical bits," Fitzsimons said. "It is natural to think that, in order to delegate a computation, it is necessary to describe the program to be implemented, and hence the required communication would scale with the size of the program.

"It turns out, however, that this is not the case. Our protocol gets around

this limit by encoding a large number of gates into each quantum state, and then adaptively correcting for any errors introduced by teleportation. If you think about this in terms of a program, the program itself would have to contain the quantum states to correct for every possible measurement result, resulting in exponential overhead. This explains why our result is not in tension with the no-programming theorem: our protocol essentially reads only a small portion of the full program, though which portion that is cannot be predetermined."

The future of blind quantum computing

The physicists expect that the iterated gate teleportation approach can be applied to computing tasks other than blind quantum computing, offering potential efficiency improvements in these areas, as well.

"It is also possible to extend blind quantum computation protocols to include tests which ensure that the desired computation has been performed correctly," Fitzsimons said. "This isn't something that is very practical at the moment, since in order for it to be really useful, we first need to have relatively large quantum computers. To date, blind and verifiable quantum computation has only been experimentally demonstrated in four-qubit systems. However, as the technology progresses we expect that the importance of securely running programs on remote quantum servers will become increasingly important, just as cloud computing has emerged in the classical world. The advantage of blind quantum computing and verification protocols is that they offer a type of security which simply is not possible using purely classical protocols."

In the future, the researchers plan to further develop blind quantum computing protocols for new cryptographic applications.

"The term quantum cryptography has become synonymous with quantum

key distribution," Fitzsimons said. "Although my group has fairly diverse research interests, a unifying theme is that we are interested in finding new quantum protocols for cryptographic tasks beyond key distribution. Delegated computation is proving to be a great source of new cryptographic problems, and so a lot of our efforts are focused there. Perhaps the most important question for us at the moment is whether there exist blind quantum computing protocols which do not require any quantum communication or entanglement between parties. I am very grateful to the National Research Foundation which generously supports our research in this area."

More information: Carlos A. Pérez-Delgado and Joseph F. Fitzsimons. "Iterated Gate Teleportation and Blind Quantum Computation." *Physical Review Letters*. DOI: 10.1103/PhysRevLett.114.220502
Earlier version at arXiv:1411.4777 **[quant-ph]**