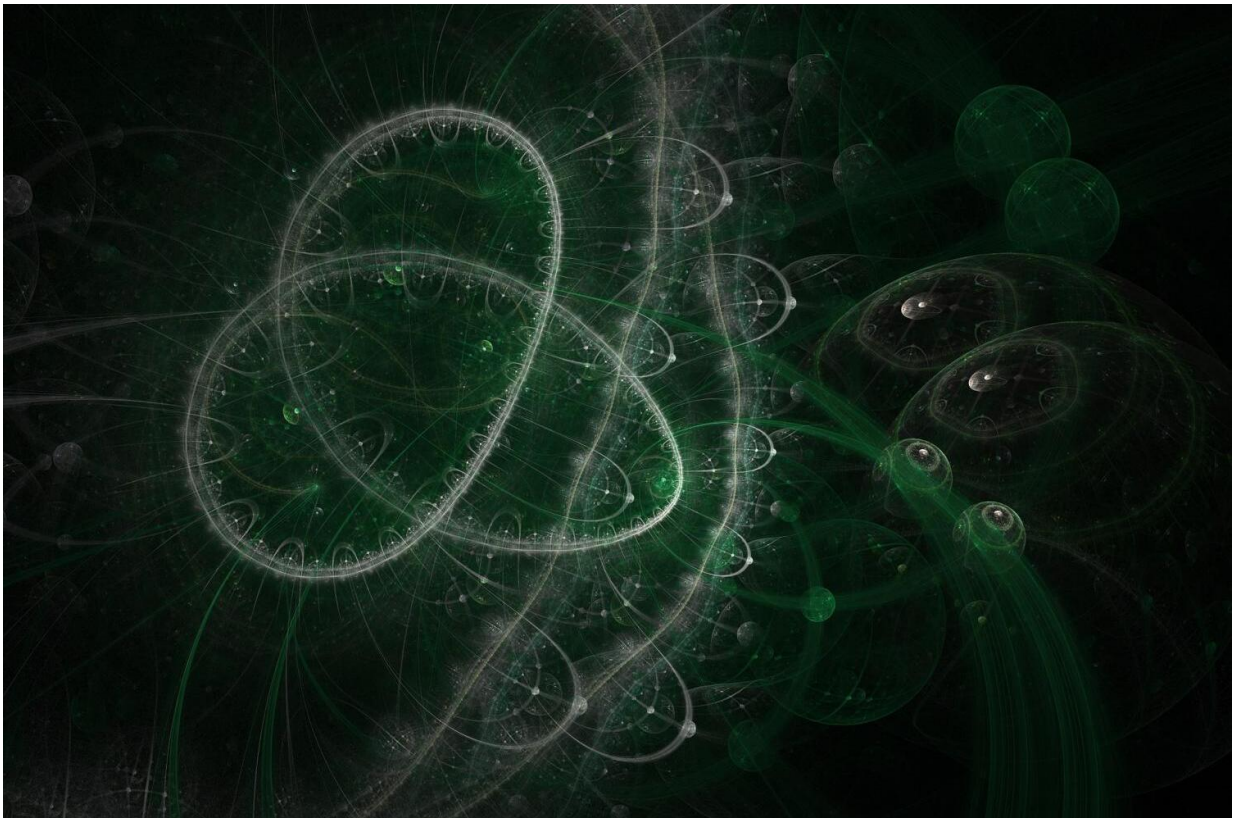
Blind quantum computing for everyone

August 11 2017, by Lisa Zyga



Credit: CC0 Public Domain

(Phys.org)—For the first time, physicists have demonstrated that clients who possess only classical computers—and no quantum devices—can outsource computing tasks to quantum servers that perform blind quantum computing. "Blind" means the quantum servers do not have full information about the tasks they are computing, which ensures that the

clients' computing tasks are kept secure. Until now, all blind quantum computing demonstrations have required that clients have their own quantum devices in order to delegate tasks for blind quantum computing.

The team of physicists, led by Jian-Wei Pan and Chao-Yang Lu at the University of Science and Technology of China, have published a paper on the demonstration of blind quantum computing for classical clients in a recent issue of *Physical Review Letters*.

"We have demonstrated for the first time that a fully classical client can delegate a quantum computation to untrusted quantum servers while maintaining full privacy," Lu told *Phys.org*.

The idea behind blind quantum computing is that, while there are certain computing tasks that quantum computers can perform exponentially better than classical computers, quantum computing still involves expensive, complex hardware that will make it inaccessible for most clients. So instead of everyone owning their own quantum computing devices, blind quantum computing makes it possible for clients to outsource their computing tasks to quantum servers that do the job for them. Ensuring that the quantum computing is performed blindly is important, since many of the potential applications of quantum computing will likely require a high degree of security.

Although several blind quantum computing protocols have been performed in the past few years, they have all required that the clients have the ability to perform certain quantum tasks, such as prepare or measure qubit states. Eliminating this requirement will provide greater access to blind quantum computing, since most clients only have classical computing systems.

In the new study, the physicists experimentally demonstrated that a classical client can outsource a simple problem (factoring the number

15) to two quantum servers that do not fully know what problem they are solving. This is because each server completes part of the task, and it is physically impossible for the servers to communicate with each other. To ensure that the quantum servers are performing their tasks honestly, the client can give them "dummy tasks" that are indistinguishable from the real task to test their honesty and correctness.

The researchers expect that the new method can be scaled up for realizing secure, outsourced quantum computing, which could one day be implemented on quantum cloud servers and make the power of quantum computing widely available.

"Blind quantum computing protocol is an important privacy-preserving technique for future secure quantum cloud computing and secure quantum networks," Lu said. "Applying our implemented blind quantum computing protocol, classical clients could delegate computation tasks to servers 'in the cloud' blindly and correctly without directly owning quantum devices. It saves resources and makes scalable quantum computing possible."

In the future, the physicists want to make blind quantum computing even easier for clients by further reducing the requirements.

"We plan to study more robust blind quantum computing protocols with fewer required resources and fewer constraints theoretically and experimentally," Lu said. "We will also explore blind quantum computing for more application scenarios, such as multi-user blind quantum computing, publicly verifiable quantum computing, and secure multi-party quantum computing."

More information: He-Liang Huang et al. "Experimental Blind Quantum Computing for a Classical Client." *Physical Review Letters*. DOI: 10.1103/PhysRevLett.119.050503 , Also at arXiv:1707.00400

[quant-ph]

© 2017 Phys.org

Citation: Blind quantum computing for everyone (2017, August 11) retrieved 14 July 2024 from https://phys.org/news/2017-08-quantum.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.