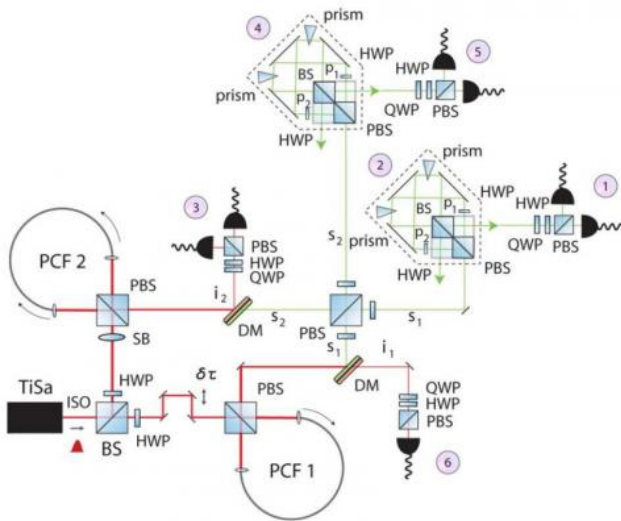


Simon's algorithm run on quantum computer for the first time—faster than on standard computer

17 November 2014, by Bob Yirka



Experimental setup. Credit: arXiv:1410.3859 [quant-ph]

(Phys.org) —A team of researchers working in South Africa has reported that they've successfully run Simon's algorithm on a quantum computer for the first time. In their paper published in *Physical Review Letters*, the team describes how they ran the algorithm, the results they found and what doing so means for the future of quantum computing.

A quantum computer is a computing device that relies on quantum bits ([qubits](#)) rather than the standard digital bits that have been used by most every computing device made. It's believed that such a computer would be able to run certain algorithms faster or more efficiently than standard computers due to their ability to take advantage of quantum mechanics properties such as entanglement and superposition. Until now, however, it's not been possible to run algorithms created specifically for such machines, to test out

this theory.

In this new effort, the team ran what is known as Simon's [algorithm](#), for Daniel Simon, who, twenty years ago, came up with an algorithm designed specifically to run faster on a quantum computer than it would, on a standard computer. Its purpose is to figure out whether a black box returns a unique output for every possible input. The team ran the simplest version of the algorithm on a quantum computer that used just six qubits, and report that it took just two iterations to solve the problem, where it would take a normal computer three. That may not seem like much, but it is believed that as more qubits are added, the larger the difference would be between the two approaches, which means, the quantum computer would be able to solve the algorithm much faster, or technically, more efficiently than standard computers. That's the good news. The bad news is that thus far, there is no practical benefit to running Simon's algorithm—its sole purpose is to show that for one algorithm, the quantum computer does better.

But that's not the end of the story, showing that one such algorithm can return a result more quickly on a [quantum](#) computer offers researchers hope that other algorithms, such as Shor's algorithm (which can be used to factor large numbers into their primes—an important part of encryption schemes) could be run much faster as well.

More information: Experimental Realization of a One-Way Quantum Computer Algorithm Solving Simon's Problem, *Phys. Rev. Lett.* 113, 200501 – Published 11 November 2014
[dx.doi.org/10.1103/PhysRevLett.113.200501](https://doi.org/10.1103/PhysRevLett.113.200501) . On Arxiv: arxiv.org/abs/1410.3859

ABSTRACT

We report an experimental demonstration of a one-way implementation of a quantum algorithm solving Simon's problem—a black-box period-finding problem that has an exponential gap between the classical and quantum runtime. Using an all-optical setup and modifying the bases of single-qubit measurements on a five-qubit cluster state, key representative functions of the logical two-qubit version's black box can be queried and solved. To the best of our knowledge, this work represents the first experimental realization of the quantum algorithm solving Simon's problem. The experimental results are in excellent agreement with the theoretical model, demonstrating the successful performance of the algorithm. With a view to scaling up to larger numbers of qubits, we analyze the resource requirements for an n -qubit version. This work helps highlight how one-way quantum computing provides a practical route to experimentally investigating the quantum-classical gap in the query complexity model.

© 2014 Phys.org

APA citation: Simon's algorithm run on quantum computer for the first time—faster than on standard computer (2014, November 17) retrieved 16 January 2021 from <https://phys.org/news/2014-11-simon-algorithm-quantum-timefaster-standard.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.