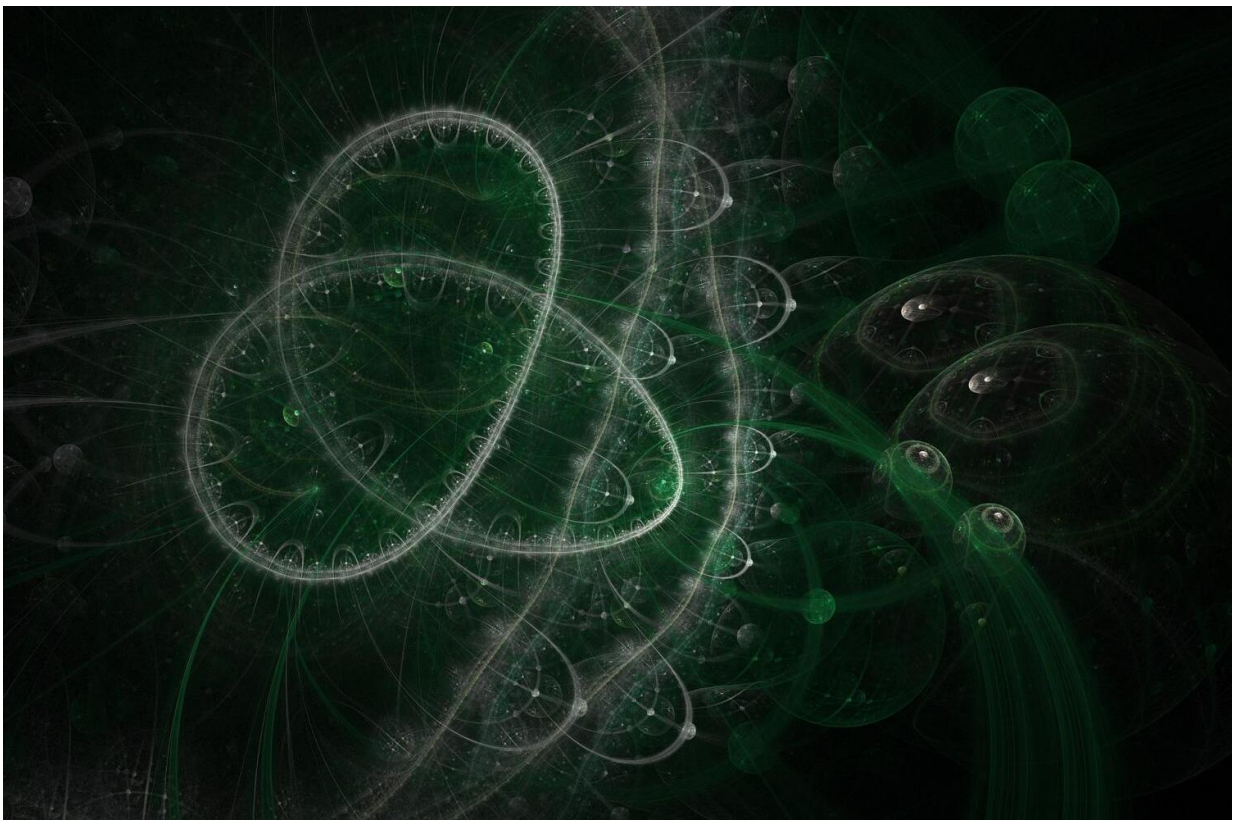
The quantum computers of the future will work equally well with encrypted and unencrypted inputs

December 14 2016



Credit: CC0 Public Domain

When future users of quantum computers need to analyze their data or run quantum algorithms, they will often have to send encrypted

information to the computer.

Because of this requirement, researchers from DTU Physics and the University of Toronto have investigated whether a quantum computer can work equally well with encrypted and unencrypted signals. The results indicate that the efficiency remains almost unchanged.

The development of a universal quantum computer is generally considered the ultimate goal within the area of physics called quantum information theory. If this goal is achieved it will enable huge progress within a long list of research fields where quantum effects are important. This could for example by in designing new medicine or new types of materials for construction or electronics.

Inspired by the history of the development of the classical computer, the researchers expect that the first generation of quantum computers will be large, expensive and difficult to operate and maintain.

For these reasons it is also expected that these devices will, at least initially, only be available to large organizations and governments.

Can a blind quantum computer be useful?

This leads to the idea of delegated quantum computing, where a user obtains access to a centralized quantum computer through a network, often thought of as a quantum version of the internet. If the user wants the request forwarded to the quantum computer to be secret, even to the quantum computer itself, she is able to encrypt them. The question is then if a quantum computer that is working in the dark, because the input is encrypted, is as efficient as when it is working on the plain input.

A universal quantum computer consists of a number of so-called gates.

More generally, a gate is a logical operation. Both quantum and ordinary computers make use of gates, though they behave quite differently. A classical logical operation could for example be an AND gate. This gate takes two inputs and returns an output based on the inputs. For example to inputs, each with the value 1, would return the output 1.

It is possible to show mathematically which types of gates are necessary to give a quantum computer with the required properties, and the researchers have now investigated some of these gates to see how they react to the encryption procedure.

By comparing the gate output for an encrypted and unencrypted input, the researchers have been able to measure how large an effect the encryption has on the gate output, and thusly the efficiency of the quantum computer. It turns out that there is no significant reduction in this efficiency. In other words, a quantum computer works equally well with encrypted and unencrypted signals.

More information: Kevin Marshall et al. Continuous-variable quantum computing on encrypted data, *Nature Communications* (2016). DOI: 10.1038/ncomms13795

Provided by Technical University of Denmark