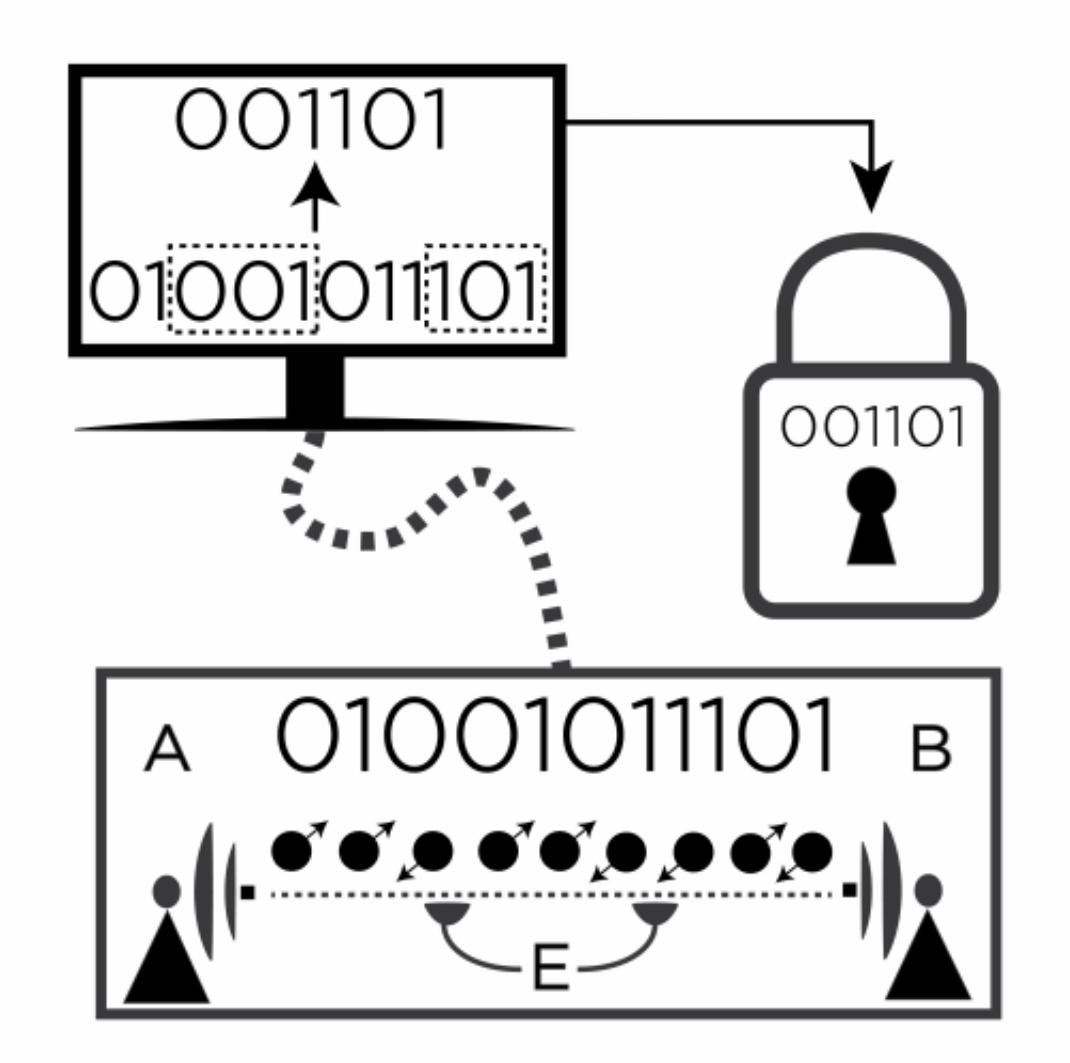
Computing a secret, unbreakable key

May 20 2016



Credit: University of Waterloo

What once took months by some of the world's leading scientists can

now be done in seconds by undergraduate students thanks to software developed at the University of Waterloo's Institute for Quantum Computing, paving the way for fast, secure quantum communication.

Researchers at the Institute for Quantum Computing (IQC) at the University of Waterloo developed the first available software to evaluate the security of any protocol for Quantum Key Distribution (QKD).

QKD allows two parties, Alice and Bob, to establish a shared secret key by exchanging photons. Photons behave according to the laws of quantum mechanics, and the laws state that you cannot measure a quantum object without disturbing it. So if an eavesdropper, Eve, intercepts and measures the photons, she will cause a disturbance that is detectable by Alice and Bob. On the other hand, if there is no disturbance, Alice and Bob can guarantee the security of their shared key.

In practice, loss and noise in an implementation always leads to some disturbance, but a small amount of disturbance implies a small amount of information about the key is available to Eve. Characterizing this amount of information allows Alice and Bob to remove it from Eve at the cost of the length of the resulting final key. The main theoretical problem in QKD is how to calculate the allowed length of this final secret key for any given protocol and the experimentally observed disturbance.

A mathematical approach was still needed to perform this difficult calculation. The researchers opted to take a numerical approach, and for practical reasons they transformed the key rate calculation to the dual optimization problem.

"We wanted to develop a program that would be fast and user-friendly. It also needs to work for any protocol," said Patrick Coles, an IQC

postdoctoral fellow. "The dual optimization problem dramatically reduced the number of parameters and the computer does all the work."

The paper, Numerical approach for unstructured quantum key distribution, published in *Nature Communications* today presented three findings. First, the researchers tested the software against previous results for known studied protocols. Their results were in perfect agreement. They then studied protocols that had never been studied before. Finally, they developed a framework to inform users how to enter the data using a new protocol into the software.

"The exploration of QKD protocols so far concentrated on protocols that allowed tricks to perform the security analysis. The work by our group now frees us to explore protocols that are adapted to the technological capabilities" noted Norbert Lütkenhaus, a professor with IQC and the Department of Physics and Astronomy at the University of Waterloo.

More information: Numerical approach for unstructured quantum key distribution, *Nature Communications* 7, Article number: 11712 DOI: 10.1038/ncomms11712 , www.nature.com/ncomms/2016/160 … ull/ncomms11712.html

Provided by University of Waterloo