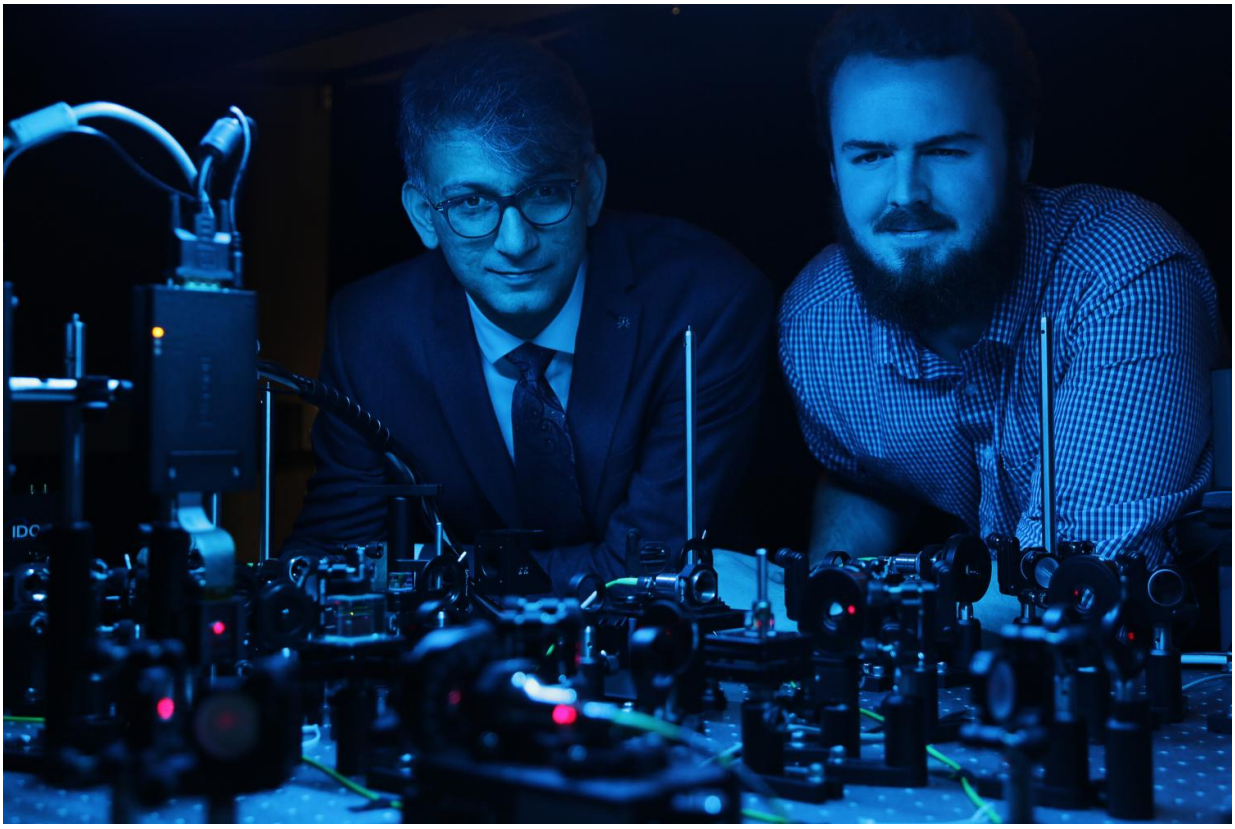
Protecting quantum computing networks against hacking threats

February 3 2017, by Dave Weatherall



Professor Ebrahim Karimi, a member of uOttawa's Department of Physics and holder of the Canada Research Chair in Structured Light, and doctoral student Frédéric Bouchard observe the setup they used to clone the photons that transmit information, called qudits. Credit: University of Ottawa

As we saw during the 2016 US election, protecting traditional computer

systems, which use zeros and ones, from hackers is not a perfect science. Now consider the complex world of quantum computing, where bits of information can simultaneously hold multiple states beyond zero and one, and the potential threats become even trickier to tackle. Even so, researchers at the University of Ottawa have uncovered clues that could help administrators protect quantum computing networks from external attacks.

"Our team has built the first high-dimensional quantum cloning machine capable of performing quantum hacking to intercept a secure quantum message," said University of Ottawa Department of Physics professor Ebrahim Karimi, who holds the Canada Research Chair in Structured Light. "Once we were able to analyze the results, we discovered some very important clues to help protect quantum computing networks against potential hacking threats."

Quantum systems were believed to provide perfectly secure data transmission because until now, attempts to copy the transmitted information resulted in an altered or deteriorated version of the original information, thereby defeating the purpose of the initial hack. Traditional computing allows a hacker to simply copy and paste information and replicate it exactly, but this doesn't hold true in the quantum computing world, where attempts to copy quantum information-or qudits-result in what Karimi refers to as "bad" copies. Until now.

For the first time, Professor Karimi's team was able to clone the photons that transmit information, namely the single carriers of light known as qubits, as well as quantum theory allows, meaning that the clones were almost exact replicas of the original information. However, in addition to undermining what was previously thought to be a perfect way of securely transmitting information, the researchers' analyses revealed promising clues into how to protect against such hacking.

"What we found was that when larger amounts of quantum information are encoded on a single photon, the copies will get worse and hacking even simpler to detect," said Frédéric Bouchard, a University of Ottawa doctoral student and lead author of an open access publication that appeared this month in the renowned journal *Science Advances*. "We were also able to show that cloning attacks introduce specific, observable noises in a secure quantum communication channel. Ensuring photons contain the largest amount of information possible and monitoring these noises in a secure channel should help strengthen quantum computing networks against potential hacking threats."

Karimi and his team hope that their quantum hacking efforts could be used to study quantum communication systems, or more generally to study how quantum information travels across quantum computer networks. To read their paper, visit the *Science Advances* website.

More information: High-dimensional quantum cloning and applications to quantum hacking, *Science Advances* 03 Feb 2017, DOI: 10.1126/sciadv.1601915

Provided by University of Ottawa