

Hackers beware -- new technique uses photons, physics to foil codebreakers

February 22 2006

For governments and corporations in the business of transmitting sensitive data such as banking records or personal information over fibre optic cables, a new system demonstrated by University of Toronto researchers offers the protective equivalent of a fire-breathing dragon.

"Quantum cryptography is trying to make all transmissions secure, so this could be very useful for online banking, for example," says Professor Hoi-Kwong Lo, an expert in physics and electrical and computer engineering at U of T's Centre for Quantum Information and Quantum Control and the senior author of a new study about the technique. "The idea can be implemented now, because we actually did the experiment with a commercial device."

The study describes the first experimental proof of a quantum decoy technique to encrypt data over fibre optic cable. In quantum cryptography, laser light particles (photons) carry complex encryption keys through fibre optic cables, dramatically increasing the security of transmitted data. Conventional encryption is based on the assumed complexity of mathematical problems that traditional computers can solve. But quantum cryptography is based on fundamental laws of physics -- specifically, Heisenberg's Uncertainty Principle, which tells us that merely observing a quantum object alters it.

The technique varies the intensity of photons and introduces photonic "decoys," which were transmitted over a 15-kilometre telecommunication fibre. After the signals are sent, a second broadcast

tells the receiving computer which photons carried the signal and which were decoys. If a hacker tries to "eavesdrop" on the data stream to figure out the encryption key, the mere act of eavesdropping changes the decoys -- a clear sign to the receiving computer that the data has been tampered with.

The study appears in the Feb. 24 issue of *Physical Review Letters*.

Source: University of Toronto

Citation: Hackers beware -- new technique uses photons, physics to foil codebreakers (2006, February 22) retrieved 23 April 2024 from <https://phys.org/news/2006-02-hackers-beware-technique-photons.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.