

Quantum cryptography at the speed of light: Researchers design first all-photonic repeaters

April 15 2015

Imagine having your MRI results sent directly to your phone, with no concern over the security of your private health data. Or knowing your financial information was safe on a server halfway around the world. Or sending highly sensitive business correspondence, without worrying that it would fall into the wrong hands.

Thanks to new research from engineers at the University of Toronto, these types of perfectly secure information exchanges are one step closer to reality. Published this week in *Nature Communications*, researchers have designed the first all-photonic quantum repeaters—protocols that ensure data can be carried reliably and securely across longer distances when using quantum cryptography.

Communication that uses [quantum cryptography](#) exploits the laws of quantum mechanics to relay information from one user to another, coded in the quantum states of [photons](#). But sending photons [long distances](#) over fibres is easier said than done—more than 90 per cent of photons are lost over distances greater than 50 kilometres, severely limiting the range of quantum communication.

To extend the range, much research has focused on developing 'quantum repeaters' to give photons a "boost" and reduce loss. These repeaters acted like mini quantum computers, storing the [entangled photons](#) and relaying their signals down the fibres—they needed to be kept at cool

temperatures and had low repeat rates, making them inconvenient and slow.

These new all-photon quantum repeaters from engineers at U of T relay photons over long distances using photons only, without the demanding requirements of matter quantum memories or an interface between matter and light at all.

Professor Hoi-Kwong Lo of The Edward S. Rogers Sr. Department of Electrical & Computer Engineering and the Department of Physics at the University of Toronto collaborated with Dr. Koji Azuma and Dr. Kiyoshi Tamaki of the Nippon Telegraph and Telephone Corporation in Japan on the project.

"There's a lot of interest in the community around designing a quantum Internet that will be more information-rich and more powerful, but these quantum states can also be fragile," says Professor Lo. "Our motivation was to design a means for communicating securely and reliably over long distances."

The team's proposed all-photon repeaters boast higher quantum-communication rates, use optical elements whose proof-of-principle demonstrations have already been made, and function at room temperature. The proposed all photonic quantum repeaters make essential use of highly entangled quantum states (called 'cluster states') and their useful property of fault-tolerance to losses.

All-photon repeaters could be used to network individual quantum computers, which remain unrealized and the domain of intense research around the globe.

"Imagine in the future we have various quantum computers around the world, run by different users," says Professor Lo. "We would want to

convey information between them, but current modes of communication are not safe against attacks or losses."

Quantum computers are on the way, but this technology has implications for another area that sounds like science fiction: quantum teleportation.

"The original question was whether we could transmit polarization over long distances, but that's boring—then researchers asked, can we do something fancier?" says Professor Lo. "And it turns out we can do quantum teleportation."

You won't be beaming from home to work any time soon, but researchers have already completed experimental demonstrations of beaming states of photons and even atoms from one location to another.

Provided by University of Toronto

Citation: Quantum cryptography at the speed of light: Researchers design first all-photonic repeaters (2015, April 15) retrieved 23 April 2024 from <https://phys.org/news/2015-04-quantum-cryptography-all-photonic.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.