New approach enhances quantum-based secure communication

September 4 2013

University of Calgary's Wolfgang Tittel researched how QKD-secured communication networks -- in banking, health care, government and other sectors -- would be much more secure than networks currently protected by encrypting secret information. Credit: Riley Brandt, University of Calgary.

University of Calgary scientists have overcome an 'Achilles' heel' of quantum-based secure communication systems, using a new approach that works in the real world to safeguard secrets.

The team's research – published in the journal *Physical Review Letters* back-to-back with similar work by a group from Hefei, China – also removes a big obstacle to realizing future applications of quantum communication, including a fully functional quantum network.

"I hope that our new quantum key distribution (QKD) system shows to people who take security seriously that QKD has many advantages and is a viable approach to safeguarding secret information," says Wolfgang Tittel, professor of physics and astronomy and the Alberta Innovates Technology Futures Strategic Research Chair in Quantum Secured Communication.

Tittel's co-authors on the scientific paper are his then-PhD students Joshua Slater, Philip Chan and Itzel Lucio-Martinez, and then-Masters student Allison Rubenok.

QKD-secured communication networks – in banking, health care, government and other sectors – would be much more secure than networks currently protected by encrypting secret information with mathematical algorithms that ultimately may be solved or 'broken' and the secrets revealed, Tittel says.

In QKD-secured communication, two parties exchange photons (individual quantum particles of light) to create a shared random secret key known only to them that can be used encrypt and decrypt messages.

Due to fundamental principles of quantum mechanics, an eavesdropper trying to learn the secret key would inevitably change it, thereby alerting the communicating parties about the intrusion. In this case, the key would be discarded.

Conversely, if the key hasn't been corrupted during distribution, it is not known to an eavesdropper and can then be used for encryption.

However, recent research has shown that "there is really a danger" of an eavesdropper shining laser light into the fibre optic cable used by the communicating parties, interfering with their photon detectors and rendering the key distribution insecure without them knowing it, Tittel says.

In overcoming that vulnerability, the University of Calgary team implemented a recently discovered new QKD protocol, which involves the two communicating parties sending their photons to a 'middle man,' who does a joint measurement on the two photons. This tells him only if the two parties have the same key, but provides no information about the key itself.

So even if an eavesdropper tries to attack the system through the parties' photon detectors, the key distribution either would either remain secure or the system would alert the parties to the intruder so they wouldn't use that particular key, Tittel says.

Moreover, being able to jointly measure two photons sent by the communicating parties is "an important step" toward creating a "quantum repeater," technology that would enable transmission on a QKD-secured network over distances greater than the maximum 200 kilometres now possible, he notes.

The university team successfully tested its new QKD system over a fibre optic cable connecting the University's Foothills Hospital campus and SAIT Polytechnic with the university's main campus, as well as more than 100 kilometres of cable in the laboratory.

"Being able to implement this new protocol will have a big impact," Tittel predicts. "I believe it is the next generation of QKD-secured communication."

Provided by University of Calgary