Researchers discover new quantum encryption method to foil hackers

April 2 2012

A research team led by University of Toronto Professor Hoi-Kwong Lo has found a new quantum encryption method to foil even the most sophisticated hackers. The discovery is outlined in the latest issue of *Physical Review Letters*.

Quantum cryptography is, in principle, a foolproof way to prevent hacking. It ensures that any attempt by an eavesdropper to read encoded communication data will lead to disturbances that can be detected by the legitimate users. Therefore, quantum cryptography allows the transmission of an unconditionally secure encryption key between two users, "Alice" and "Bob," in the presence of a potential hacker, "Eve." The encryption key is communicated using light signals and is received using photon detectors. The challenge is that Eve can intercept and manipulate these signals.

"Photon detectors have turned out to be an Achilles' heel for quantum key distribution (QKD), inadvertently opening the door to subtle side-channel attacks, most famously quantum hacking," wrote Dr. Charles Bennett, a research fellow at IBM and the co-inventor of quantum cryptography.

When quantum hacking occurs, light signals subvert the photon detectors, causing them to only see the photons that Eve wants Bob to see. Indeed, earlier research results by Professor Lo and independent work by Dr. Vadim Makarov of the Norwegian University of Science and Technology have shown how a clever quantum hacker can hack

commercial QKD systems.

Now, Professor Lo and his team have come up with a simple solution to the untrusted device problem. Their method is called "Measurement Device Independent QKD." While Eve may operate the photon detectors and broadcast measurement results, Bob and Alice no longer have to trust those measurement results. Instead, Bob and Alice can simply verify Eve's honesty by measuring and comparing their own data. The aim is to detect subtle changes that occur when quantum data is manipulated by a third party.

Specifically, in Measurement Device Independent QKD, the two users send their signals to an untrusted relay – "Charlie" – who might possibly be controlled by Eve. Charlie performs a joint measurement on the signals, providing another point of comparison.

"A surprising feature is that Charlie's detectors can be arbitrarily flawed without compromising security," says Professor Lo. "This is because, provided that Alice and Bob's signal preparation processes are correct, they can verify whether Charlie or Eve is trustworthy through the correlations in their own data following any interaction with Charlie/Eve."

A proof-of-concept measurement has already been performed. Professor Lo and his team are now developing a prototype measurement device independent QKD system, which they expect will be ready within five years.

As a result of implementing this new method, quantum cryptography's Achilles' heel in the fight against hackers has been resolved. Perhaps, a quantum jump in data security has now been achieved.

More information: link.aps.org/doi/10.1103/PhysRevLett.108.130503