Doing more with less: Steering a quantum path to improved internet security

January 7 2015

Credit: Wikipedia

Research conducted at Griffith University in Queensland, Australia, may lead to greatly improved security of information transfer over the internet.

In a paper published in the online journal *Nature Communications*, physicists from Griffith's Centre for Quantum Dynamics demonstrate the potential for "quantum steering" to be used to enhance data security over long distances, discourage hackers and eavesdroppers and resolve issues of trust with communication devices.

"Quantum physics promises the possibility of absolutely secure information transfer, where your credit card details or other personal data sent over the internet could be completely isolated from hackers," says project leader Professor Geoff Pryde.

"In an ideal world, such perfectly secure long distance communication between any two parties is simple. They could share strongly entangled quantum systems—such as particles of light called photons—to generate truly random and uncrackable codes.

"Unfortunately, in the real world the two parties cannot share sufficiently strong entanglement over long distances due to transmission and detection losses. As the photons travel through the communication network, some are lost, thus providing a loophole for outsiders to attack their code."

A backup solution—and the focus of the Griffith research—is quantum steering, where a measurement made on one party's quantum system changes, or steers, the system held by another.

Professor Pryde says that, despite being a weaker form of entanglement, quantum steering operates paradoxically to maintain communication security while tolerating greater real-world loss and removing the need

for absolute trust in devices.

"Quantum entanglement is a wonderful resource for safe and secure communication, but you need to verify it is really there to be certain any eavesdroppers are kept out of the loop," he says.

"Our new technique does so without requiring any trust in the communication devices and it should work in long distance scenarios where standard methods fail."

The Griffith team used special photon quantum states to program a measurement apparatus at each step of sending the code.

Because of "Heisenberg's uncertainty principle" - which states one can never be certain of both the position and speed of a microscopic particle—a hacker cannot reliably determine these quantum states even if they have hacked an apparatus. Remarkably, this means it can still be used securely.

In the experimental demonstration, measurement devices representing the two parties were constructed and received entangled photons from a quantum source. Another photon source, representing the referee, was used to prepare the quantum states for programming one apparatus.

After many runs of the protocol, the referee could use the measurement results from both parties to perform a mathematical test for genuine quantum steering, as derived by Griffith theoretical physicist Dr Michael Hall.

"The team showed that the quantum-refereed steering protocol can match tests for strong entanglement, in not requiring trust in the measuring devices, and has the further advantage of being robust to noise," says Dr Hall, adding that researchers hope to use the technique in

a full quantum secure coding demonstration.

Provided by Griffith University