Making quantum encryption practical

21 May 2013, by Larry Hardesty

One of the many promising applications of quantum mechanics in the information sciences is quantum key distribution (QKD), in which the counterintuitive behavior of quantum particles guarantees that no one can eavesdrop on a private exchange of data without detection.

As its name implies, QKD is intended for the distribution of cryptographic keys that can be used for ordinary, nonquantum cryptography. That's because it requires the transmission of a huge number of bits for each one that's successfully received. That kind of inefficiency is tolerable for key distribution, but not for general-purpose communication.

Also, because QKD depends on the properties of individual light particles—photons—it's very vulnerable to signal loss, which is inevitable over large enough distances. Although QKD systems have been built—some commercially—they generally work across distances of only 100 miles or so.

In a series of recent papers, researchers in the Optical and Quantum Communications Group at MIT's Research Laboratory of Electronics described a new quantum communication protocol that could solve both of these problems. It's much more resilient to signal loss than QKD, and it sends only one bit for every one received.

In the latest issue of *Physical Review Letters*, they describe the first experimental implementation of their system, which bore out all their theoretical predictions.

At present, the protocol does have one major caveat: It's secure only against so-called passive eavesdroppers, who simply siphon light from an optical transmission, and not against active eavesdroppers, who maliciously inject their own light into a communication channel. Security against passive eavesdropping is probably adequate for some optical communication systems, but if the researchers can figure out how to thwart active eavesdroppers, too, their protocol could be used to secure optical data transmission over long distances.

Cascading correlations

Like all quantum information schemes, the new protocol exploits the central mystery of quantum physics: the ability of tiny particles of matter to inhabit mutually exclusive states at the same time. Electrons, for instance, have a property called spin, which describes how they act in a magnetic field. Spin can be either up or down, but it can also be in a strange quantum state known as superposition, in which it's up and down simultaneously.

According to Jeffrey Shapiro, the Julius A. Stratton Professor of Electrical Engineering and one of the co-directors of the Optical and Quantum Communications Group, quantum particles are capable of a greater degree of correlation than objects described by classical physics. A coin, for instance, can be either face-up or face-down. If you glue a second coin to it, face-to-face, the states of the two coins are correlated: If one is up, the other is down, and vice versa.

In the same way, if two electrons are orbiting the nucleus of an atom at the same distance, their spins are correlated: If one is up, the other must be down. But there's a third possibility: If one is up and down at the same time, so is the other.

This kind of mutual dependency, even in particles separated by great distances, is known as entanglement. But entanglement is very fragile: It begins to break down as soon as particles start interacting with their immediate environments. The key to the new protocol, Shapiro explains, is that even if the entanglement between two light beams breaks down, and their degree of correlation falls back within classical limits, it can still remain much higher than it would be if the beams had a merely classical correlation to begin with.

Bring the noise

Following cryptographic convention, the RLE researchers describe their protocol in terms of a secure communication between Alice and Bob, with an eavesdropper, named Eve, trying to listen in. Alice creates two entangled light beams and sends one of them to Bob, keeping the other one circulating locally.

"In classical physics, there's a maximum amount of correlation you can get between two events," Shapiro says. In the new protocol, however, the entangled beams "have a correlation that exceeds—by orders of magnitude—the classical limit."

As one of those beams travels toward Bob, interactions with the environment begin to break the entanglement, introducing degradations of signal quality that engineers call "noise." Bob then adds information to the beam, amplifies it—which adds much more noise—and sends it back. Alice uses the beam she kept circulating locally to decode Bob's transmission.

Eve, on the other hand, extracts some of the signal that Alice sends Bob and uses that to decode Bob's transmission. Because Bob's transmission is so noisy, its correlation with Eve's sample signal is much lower than it is with the signal Alice kept.

"My experiment can show for the communication between Alice and Bob, if Bob sends one megabit of information, about one bit gets flipped," says Zheshen Zhang, a postdoc at RLE and first author on the new paper. "For the eavesdropper, about half of the bits get flipped."

"The first distinction between this and what other people have done in the past is that Jeff's protocol is a direct secure-communication protocol," says Saikat Guha, a senior scientist at Raytheon subsidiary BBN Technologies who works on quantum optical communications and imaging. "This is not a key distribution protocol."

As for whether the system will work over long distances, "we don't have all the answers yet, but this does seem to have better promise than some of the standard QKD protocols," Guha says. "In the standard QKD protocols, one big requirement is to have quantum repeaters, which are devices that are not yet available. People are working on it, but there aren't any quantum repeaters. So you can't do standard QKD over standard fiber for more than a couple hundred kilometers at the most."

Guha observes that the RLE researchers' protocol isn't secure against active eavesdropping, but says, "I think it's very promising that it will be adapted to active eavesdropping. It's just that the analysis hasn't been done."

"We're working on the theory for active eavesdropping," Shapiro adds.

The paper is titled "Entanglement's Benefit Survives an Entanglement-Breaking Channel."

More information:
prl.aps.org/accepted/15071Y4aP …a04f9c67f2cf08bc2cdc

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology