Bits of Uncertainty

Blazing a quantum trail to absolute secrecy

By IVARS PETERSON

Lake Geneva

Picture Perfect/C. Bowman

Enveloped by mountains, Lake Geneva straddles the border between France and Switzerland. Ferry routes, lakeshore railways, and winding roads connect the cities, towns, and resorts along its edge.

Optical fiber cables forge another kind of link, snaking along the bottom of the lake to carry telephone signals between communities separated by the clear, unusually blue water.

One such telecommunications cable served recently as a conduit for a physics experiment involving quantum mechanics and secret messages. Researchers in the basement of a building in Nyon, Switzerland, sent extremely faint pulses of infrared light along 22.7 kilometers of optical fiber to a basement in Geneva, where the pulses were successfully detected.

This achievement represented an important step in the development of quantum cryptography, which offers a completely safe, public means of transmitting secret information. The technique opens up a secure communications channel no eavesdropper can tap without being noticed. It's a case of James Bond meeting Werner Heisenberg.

The method's success rests on the Heisenberg uncertainty principle of quantum physics. Eavesdropping requires observation: in effect, the hijacking of some portion of an information-carrying signal. When the information carriers are quantum objects such as photons, the intervention inevitably disturbs the entire system in a detectable way.

Only a decade ago, quantum cryptography was considered a crazy theoretical notion based on peculiar effects of interest only to those concerned about the philosophical foundations of quantum mechanics. Now, a series of experiments, including the Lake Geneva demonstration, has shown that quantum cryptography actually works.

"It's a potentially practical, emerging technology," says Richard J. Hughes of the Los Alamos (N.M.) National Laboratory.

With its security guaranteed by the laws of physics, this cryptographic technique might someday protect the communication of sensitive data, whether military secrets or bank transactions.

Cryptography aims to provide methods allowing two parties to communicate in a form that's unintelligible to a third party. One way to achieve such privacy is for both the sender and the intended recipient to share a key—typically a string of random numbers, often binary—for creating and deciphering the secret message.

The trouble with this procedure is that the two parties must initially meet to decide on a key or take the risk of having the key hand-delivered by a courier or transmitted over a telephone line. Either way, the logistics are cumbersome and the exchanges potentially insecure, especially because keys are lengthy and changed regularly to increase security.

Quantum cryptography offers an ideal mechanism for handling secret keys. It permits users to generate a key of any length at the moment it's required for encrypted communication.

The trick is to use quantum particles to carry the information. They have pairs of characteristics that can't be measured simultaneously to arbitrarily high precision. For example, determining an electron's precise position means that its velocity can't be measured with equivalent accuracy and vice versa.

Measured properties of photons display a similar duality. Light can be described in terms of both photons (particles) and oscillating electric fields (waves). The direction of oscillation of a field is known as the light's polarization, generally designated by an angle.

It's possible to generate a photon in any one of an infinite number of polarization states. However, the rules of quantum mechanics specify that a polarization measurement, performed by sending a photon through a polaroid filter set at some angle, can distinguish only the two polarization states parallel or perpendicular to the filter.

Determinations of photon polarization came into play in 1984, when Charles H. Bennett of the IBM Thomas J. Watson Research Center in Yorktown Heights, N.Y., and Gilles Brassard of the University of Montreal proposed an ingenious scheme for generating secret cryptographic keys.

Suppose the sender can transmit photons in four possible polarizations: 0° (horizontal), 45° (diagonal), 90° (vertical), and 135° (diagonal).

Secret messages

To generate a cryptogram, the sender first rewrites the message as a string of binary numbers according to a conversion table (A = 01000001, B = 0100010, and so on). This string is then added to an equally long sequence of random bits (the secret key), using the following rules of binary modular arithmetic: 0+0 = 0, 0+1 = 1+0 = 1, and 1+1 = 0. The sender transmits the resulting sequence, which is the encrypted message.

Message	H	E	L	P
Message (in binary)	01001000	01000101	01001100	01010000
Secret key	10100010	10101010	10100101	01110101
Encrypted message	11101010	11101111	11101001	00100101
Decrypted message	01001000	01000101	01001100	01010000

Using the same secret key, the recipient recovers the original digital text by adding the digits of the key (following the same rules as above) to the transmitted sequence.

— I. Peterson

The recipient has a choice of two possible measurements. One measurement distinguishes between the horizontal and vertical polarizations, and the other distinguishes between the two diagonal states.

However, a measurement that distinguishes between the horizontal and vertical polarizations gives a completely random result when applied to photons in either of the two diagonal states and vice versa. Thus, a horizontally polarized photon passing through an angled analyzer emerges randomly in one or the other of the two possible diagonal polarizations.

To generate a cryptographic key, the initiating party uses a procedure like the one described in the sidebar (below), starting with the transmission of a stream of photons. Of course, in real life, computers would handle the entire transaction.

An eavesdropper monitoring the system would have to intercept the photons, make measurements, then retransmit the particles. Quantum mechanics doesn't allow the spy to copy the states while forwarding the originals to the receiver.

Without knowing in advance what type of measurement the receiver intends to make, the eavesdropper is bound to introduce errors, which the sender and receiver can readily detect by checking whether their signals come through as expected.

The whole procedure hinges on the fact that the state of a quantum object doesn't have a specific value until it is observed or measured in some way. An eavesdropper's activities produce irreversible changes in quantum states.

At first glance, quantum cryptography appears highly impractical.

The technique involves using individual polarized photons, and these extremely faint signals can be readily drowned out if transmitted in daylight through air. Optical fibers have the disadvantage that distortions and bends in the fiber change a photon's polarization.

Moreover, various kinds of environmental noise, such as static in detectors and along communications channels, can potentially mask an eavesdropper's activities.

Despite these difficulties, Bennett, Brassard, and their coworkers built the first working system in 1989. Operating at a rate of 10 bits per second, their computer-controlled, shoebox-sized, light-tight setup had polarized photons, generated by tiny diode lasers, traveling about 30 centimeters in air (SN: 6/20/90, p. 342).

The same year Bennett's group built its first system, Artur K. Ekert and David Deutsch of the University of Oxford in England proposed an alternative mechanism for establishing a secret key, this time without transferring any information between the sites.

The scheme works because, in certain situations, quantum objects that have interacted in the past or have a common origin can go on affecting each other in the future, even though they are physically far apart (SN: 4/10/93, p. 229). Such quantum correlations can be established when pairs of photons or subatomic particles are created at the same instant and go off in different directions.

"I never thought something regarded as a philosophical curiosity [in fundamental quantum theory] would ever be made practical—used to protect the security of data transfers," Ekert says. "From my perspective, it's simply amusing."

Rapid progress in quantum optics during the early 1990s brought greatly improved photon sources, photodetectors, and optical fibers. These developments set the stage for a new round of experiments, beginning with a series by John G. Rarity and Paul R. Tapster of the Defense Research Agency in Malvern, England, and their collaborators.

The researchers used techniques that involve optical interference, focusing on a photon's phase (how far it has gone in its oscillation cycle) rather than its polarization. Using optical fiber interferometers, they succeeded in transmitting both single photons and pairs of correlated photons for distances of up to 10 km.

In 1993, Antoine Muller, Nicholas Gisin, and their colleagues at the University of Geneva demonstrated that it was possible to send polarized photons over an optical fiber using only commercially available equipment. They guided photons

Exchanging the secret key

Quantum cryptography enables two people to exchange a secret key. The sender transmits photons in one of four polarizations (→, ↗, ↑, or ↖) chosen at random (step 1). The recipient randomly chooses a measurement technique (step 2), distinguishing either between horizontal and vertical polarizations (+) or between diagonal polarizations (x), and records the results (3). Blank spaces indicate photons not received or detected because of noise or other difficulties. The recipient then tells the sender the type of measurement used in each case (4), and the sender indicates which results were correct (5).

1.	↗	↑	↖	→	↑	↑	→	→	↖	↗	↑	↖	↗	↗	↑
2.	+	x	x	+	+	x	x	+	x	+	x	x	x	x	+
3.	↑		↖	→	↑	↗	↗	→	↖	↑	↖	↖		↗	↑
4.	+		x	+	+	x	x	+	x	+	x	x		x	+
5.			✓	✓	✓			✓	✓			✓		✓	✓
6.			↖	→	↑			→	↖			↖		↗	↑
7.			1	0	1			0	1			1		0	1
8.			1	0				0				1			1

The sender and receiver keep only the data from the correctly measured photons, discarding all the rest (6). These data are then interpreted as a binary sequence (7) according to the coding scheme: → = ↗ = 0 and ↑ = ↖ = 1. This sequence becomes the secret key.

To check for errors or the presence of an eavesdropper, the sender and receiver can perform a series of tests on subsets of their data (8). For example, they can check whether they both get the same digit when the bits in their respective subsets are added together according to the rules of binary modular arithmetic (1+0+0+1+1 = 1).

— I. Peterson

from a diode laser to a photon counter at the other end of an optical fiber more than 1 km long, successfully compensating for polarization changes caused by the fiber.

In their most recent experiment, the researchers sent polarized photons 22.7 km along a standard commercial optical cable used for telecommunications. The team now plans to put together a demonstration unit incorporating complete quantum key generation and error correction capabilities, Muller says.

Hughes and his coworkers at Los Alamos can already generate keys automatically with their quantum cryptography setup. Based on photon phase rather than polarization, their system spans 14 km of optical fiber normally used as part of a data network linking different parts of the Los Alamos complex.

"We're now able to generate actual key material—secret sets of binary numbers," Hughes says.

A user can type a short message at a computer at the sending end. The computer decides how much key material is needed, orchestrates the generation of this amount, encrypts the message, and sends it over an unprotected Internet link to a receiving computer. In the meantime, the receiving computer has acquired, over the same Internet link, the key needed to recover the original message.

The researchers hope eventually to increase the transmission distance to 50 km. "We've also started a project on quantum cryptography in free space—no fibers," Hughes says. "It sounds very unpromising at first. You send an awful lot of photons and don't get many through.

"But these shared secret key bits are so valuable that even getting a relatively small number—a few thousand—through would be very useful."

James D. Franson and his coworkers at the Johns Hopkins University Applied Physics Laboratory in Laurel, Md., have been working on sending polarized photons through open air in broad daylight. Their method of doing quantum cryptography, invented by Franson, involves a combination of photon polarization and interference effects.

"We have now demonstrated the ability to transmit secure messages between two buildings and over distances of roughly 500 feet in this way," Franson says.

"That's astounding when you think about it," he notes. An ordinary 100-watt lightbulb produces roughly 10^{20} photons per second, and there are far more photons bouncing around outdoors.

"For a long time, people thought there was no way someone could send just one photon through such swarms of other photons and detect it, but we indeed do that," Franson says. The method relies on the use of filters coupled with precise timing information to pinpoint the lone photons.

For longer distances, the researchers need to improve their optical system, using elements with larger diameters and greater sensitivities. Ultimately, to get an even greater range, it may be possible to send signals to and receive them from a satellite in low orbit.

Most of the theoretical questions concerning quantum cryptography have now been settled. Moreover, a series of experiments has demonstrated that the technique works under a variety of conditions.

"Not so long ago, we could say there were no applications at all for some of the weird quantum effects we deal with," Franson says. "In a few years, quantum cryptography has come to the point where it's really an engineering issue."

"It's now not so much whether it can be done but whether it needs to be done," he adds.

Quantum cryptography can evolve into a viable technology if it can compete effectively with conventional cryptography. "Someone has to decide they want to spend a fair bit of money to commercialize the product," Hughes says. □