FEATURE

Quantum Key Distribution

Data-carrying photons may be transmitted by laser and detected in such a way that any interference will be noticed

by Jennifer Ouellette

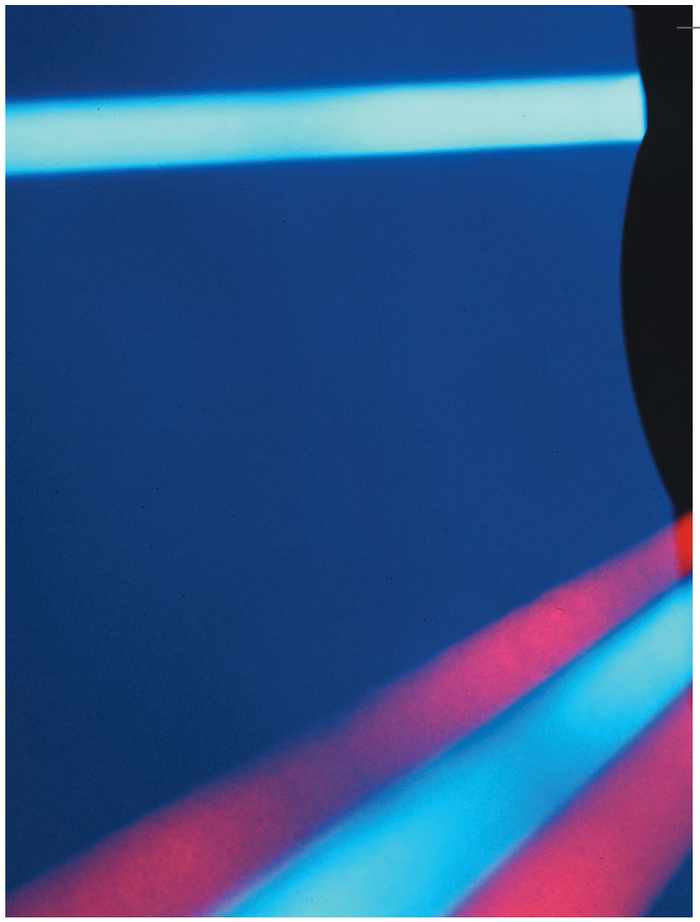
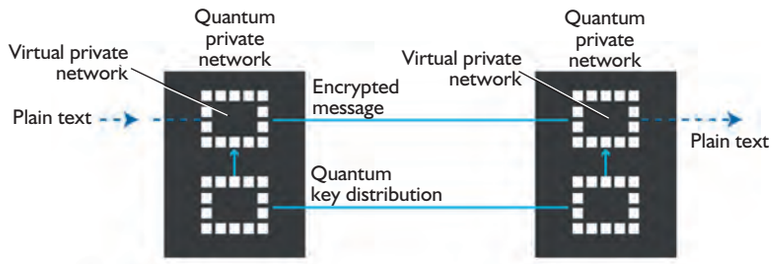


Figure 1. When blue light is pumped into a nonlinear crystal, entangled photon pairs (imaged here as a red beam with the aid of a diode laser) emerge at an angle of 3° to the blue beam, and the beams are sent into single-mode fibers to be detected. Because the entangled photons "know" each other, any interference will result in a mismatch when the two beams are compared.

Computing's exponential increase in power requires setting the bar always higher to secure electronic-data transmissions from would-be hackers. The ideal solution would transmit data in quantum bits, but truly quantum information processing may lie decades away. Therefore, several companies have focused on bringing one aspect of quantum communications to market—quantum key distribution (QKD), used to exchange secret keys that protect data during transmission. Two companies, MagiQ Technologies (New York, NY) and ID Quantique (Geneva, Switzerland), have released commercial QKD systems, and several others plan to enter the marketplace within two years.

"There is a continuous war between code makers and code breakers," says Alexei Trifonov, chief scientist with MagiQ. Cryptologists devise more difficult coding schemes, only to have them broken. Quantum cryptography has the potential to end that cycle. This is important to national security and modern electronic business transactions, which transmit credit card numbers and other sensitive information in encrypted form.

The Department of Defense (DoD) currently funds several quantum-cryptography projects as part of a $20.6 million initiative in quantum information. Globally, public and private sources will fund about $50 million in quantum-cryptography work over the next several years. Andrew Hammond, a vice president of MagiQ, estimates that the market for QKD systems will reach $200 million within a few years, and one day could hit $1 billion annually.



MagiQ Technologies, Inc.

Figure 2. The basic system inputs plain text to a MagiQ quantum private network (QPN) unit, where a virtual private network transmits the encrypted message in conjunction with a quantum key. A parallel QPN unit translates the message back into plain text.

Key types

QKD was proposed roughly 20 years ago, but its premise rests on the formulation of Heisenberg's uncertainty principle in 1927. The very act of observing or measuring a particle—such as a photon in a data stream—changes its behavior (Figure 1). Any moving photon can have one of four orientations: vertical, horizontal, or diagonal in either direction. A standard laser can be modified to emit single photons, each with a particular orientation. Would-be hackers (eavesdroppers in cryptography parlance) can record the orientations with photon detectors, but doing so changes the orientation of some photons—and, thus, alerts the sender and receiver of a compromised transmission.

An encryption key—the code needed to encrypt or decipher a message—consists of a string of random bits.

University of Vienna/Volker Steger

Such a key is useless unless it is completely random, known only to the communicating parties, and changed regularly. In the one-time-pad approach, the key length must equal the message length, and it should be used only once. In theory, this makes the encrypted message secure, but problems arise in practice. In the real world, keys must be exchanged by a CD-ROM or some other physical means, which makes keys susceptible to interception. Reusing a key gives code breakers the opportunity to find patterns in the encrypted data that might reveal the key. Historically, the Soviet Union's accidental duplication of one-time-pad pages allowed U.S. cryptanalysts to unmask the spy Klaus Fuchs in 1949.

Rather than one-time-pad keys, many data-transmission security systems today use public-key cryptography, which relies on very long prime numbers to transmit keys. A typical public-key encryption scheme uses two keys. The first is a public key, available to anyone with access to the global registry of public keys, and the message is encrypted with it. The second is private, accessible only to the receiver. Both keys are needed to unscramble a message. The system's primary weakness is that a powerful computer could use the public key to learn the private key (see *The Industrial Physicist,* August 2000, pp. 29–33).

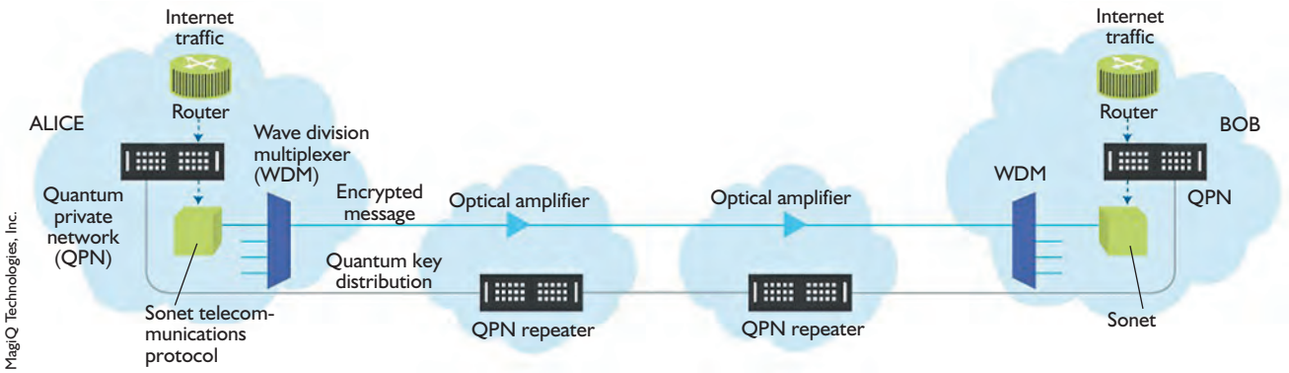
Quantum key distribution

A key distributed using quantum cryptography would be almost impossible to steal because QKD systems continually and randomly generate new private keys that both parties share automatically. A compromised key in a QKD system can only decrypt a small amount of encoded information because the private key may be changed every second or even continuously. To build up a secret key from a stream of single photons, each photon is encoded with a bit value of 0 or 1, typically by a photon in some superposition state, such as polarization.

These photons are emitted by a conventional laser as pulses of light so dim that most pulses do not emit a photon. This approach ensures that few pulses contain more than one photon. Additional losses occur as photons travel through the fiber-optic line. In the end, only a small fraction of the received pulses actually contain a photon. However, this low yield is not problematic for QKD because only photons that reach the receiver are used. The key is generally encoded in either the polarization or the relative phase of the photon (see sidebar, p.24).

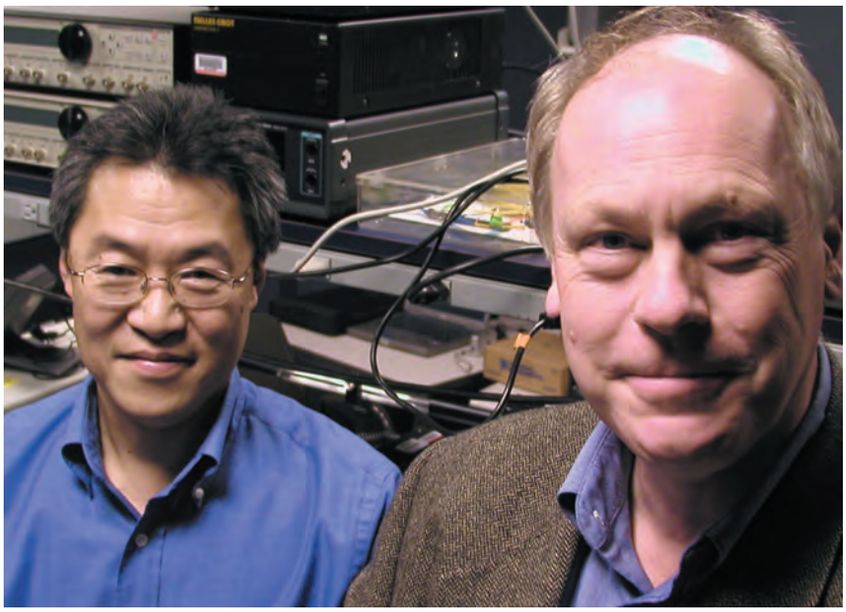
The most common standard protocol for QKD is called BB84, after its inventors, IBM's Charles Bennett and Gilles Brassard. Invented in 1984, it uses a stream of single photons to transfer a cryptographic key between two parties, who can use it to encode and decode data transmitted using standard high-speed techniques. Right now, single photons allow real-time data transmissions only at low speed, typically 100 bits/s—a hundred millionth the speed of today's fastest fiber-optic transmission systems. That explains why most companies have focused on commercializing QKD and not on data encryption.

Polarization-based encoding works best for free-space



MagiQ Technologies, Inc.

Figure 3. A more detailed network shows routers for concentrating and directing Internet traffic, Sonet telecommunications protocol, wave division multiplexers, optical amplifiers, and repeaters.



BBN Technologies

Figure 4. Henry Yeh, director of programs, and Chip Elliot, principal engineer, in the Quantum Laboratory at BBN Technologies, which operates the DARPA-funded world's first quantum key distribution network.

communication systems rather than fiber-optic lines. Data are transmitted faster in free-space systems, but they cannot traverse the longer distances of fiber-optic links. In July 2004, a team at the National Institute of Standards and Technology (NIST), working with Acadia Optronics (Rockville, MD), demonstrated the world's fastest quantum-cryptography system by sending a quantum key over a 730-m free-space link at rates of up to 1 megabit/s—1,000 times as fast as previously reported results. The NIST system uses an infrared laser to generate the photons and reflecting telescopes with 8-in. mirrors to send and receive the photons through air.

NIST's system differs from other existing QKD systems in how it identifies a photon from the sender, as opposed to photons from another source, such as the sun. The scientists record the exact time of each emission and look for a photon only when one is expected. The window of observation time must be very short, but NIST physicist Joshua Bienfang says that making frequent brief observations enables the team to generate new keys more often.

Fiber-optic links

Randomly generated keys are changed up to 1,000 times/s in MagiQ's OPN Security Gateway, which uses a secure fiber-optic link to transmit the changing key sequence up to 120 km as a stream of polarized photons. The company claims that linking its systems together can transmit a QKD several hundred kilometers (Figures 2 and 3).

Quantum properties other than polarization can encode the value of a bit for the quantum key, says Gregoire Ribordy, CEO of Swiss start-up ID Quantique. His company introduced the first commercial quantum-cryptography products in 2002: single-photon detectors and random-number generators, two essential components for quantum-cryptography systems. In 2003, the company partnered with two electronic-security firms to develop a commercial system.

ID Quantique's system encodes data in the phase of the photon instead of its polarization state. An interferometer splits beams of light and then recombines them at the output end, and it can do the same with a single photon. Although a photon cannot split in two, its dual wave–particle nature allows it to travel through both arms of the interferometer as a wave, only becoming a particle again when it recombines and is detected at the output end. It takes but a slight change in the length of one interferometer arm to randomly alter a photon's phase.

In 2002, scientists at Northwestern University developed a quantum-cryptography method capable of sending encrypted data over a fiber-optic line at 250 megabits/s, almost 1,000 times as fast as prior quantum technology. The team used standard lasers and existing optical technology to transmit large bundles of photons; other techniques used in quantum cryptography rely on single photons, which are harder to detect.

BBN Technologies (Cambridge, MA) operates the world's first quantum cryptographic network, which links several different kinds of QKD systems (Figure 4). Some use off-the-shelf optical lasers and detectors to emit and detect single photons; others use entangled pairs of photons. This DARPA-funded network runs between BBN, Harvard, and Boston University, a city-sized schematic designed to test the robustness of such systems in real-world applications (Figure 5). It allows multiple users at each organization to tap into a fiber-optic loop secured by a quantum-cryptography system. BBN will soon add a free-space QKD link and an entangled-photon QKD system.

KEEPING ALICE AND BOB SECURE

Alice wishes to send a secret message to Bob using a quantum-encryption system. The system uses lasers to generate individual photons polarized in one of two modes: vertical/horizontal, or diagonally ± 45°. Within each mode, one orientation represents a digital value of 0, the other, 1.

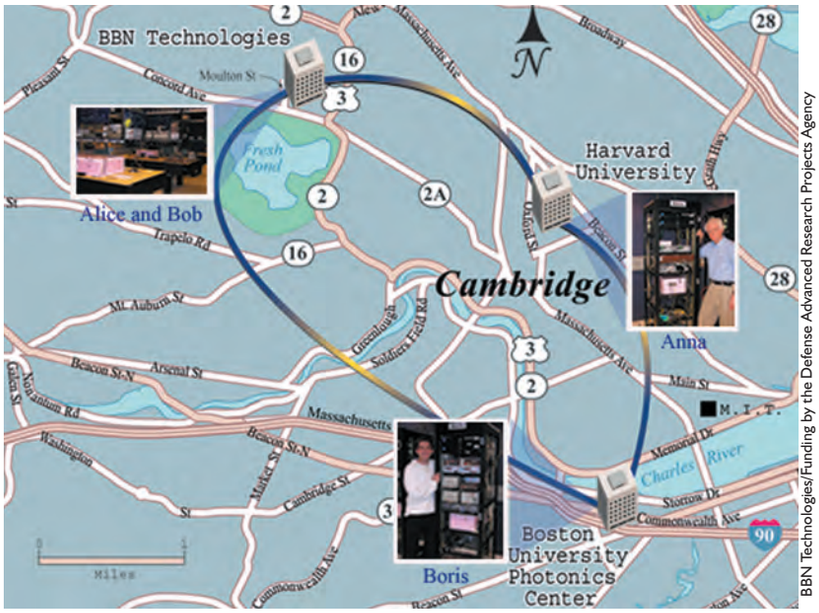
As the sender, Alice randomly chooses both a mode and an orientation (digital value) for each photon sent over the quantum channel. As the receiver, Bob randomly chooses between the two modes when he tries to detect a photon. If he chooses the same mode that Alice used for a given photon, he will correctly measure its orientation and determine its digital value. Choosing a different mode from Alice will give him the wrong value for that photon.

So Alice uses another channel to tell Bob the mode she used for each photon, but does not tell him its digital value. Bob can then ignore all the instances where he measured a photon in the wrong mode, and tells Alice which ones he measured correctly—also not telling her their digital value. Alice in turn can discard all the photons Bob didn't measure correctly. Those measured correctly now make up the encryption key, which Bob and Alice share.

If Eve attempts to eavesdrop on Bob and Alice, her attempt to read the data stream will alter it. When Eve's receiver intercepts Alice's transmission, the photon is converted to electrical energy as it is measured, which destroys it. Eve must generate a new quantum message to send to Bob, guessing at the digital values for many of the photons, which creates errors in the string of values used in the encryption key. Bob and Alice can find these errors by comparing small quantities of their key's digital values. If they find a statistically significant number of differences, they will know there is an eavesdropper and can discard the key.

Other companies are also investing in quantum-cryptography systems. IBM's Almaden Research Center, the NEC Research Institute, Toshiba, and Hewlett-Packard are on the brink of introducing products. In March 2004, NEC scientists in Japan sent a single photon over a 150-km fiber-optic link, breaking the transmission-distance record for quantum cryptography.

To date, most commercially viable QKD systems rely on fiber-optic links limited to 100 to 120 km. At longer distances, random noise degrades the photon stream. Quantum keys cannot travel far over fiber-optic lines, and, thus, they can work only between computers directly connected to each other. The only way to achieve such a system with total security in a networking environment and at greater distances is to add quantum repeaters—rudimentary quantum computers—to regenerate the bits. NEC and Hewlett-Packard are developing components needed to make quantum repeaters a reality.



BBN Technologies/Funding by the Defense Advanced Research Projects Agency

Figure 5. This network allows users at BBN Technologies, Harvard University, and Boston University to tap into a fiber-optic loop secured by a quantum-cryptography system.

Entangled photons

To date, physicists have not developed an ideal single-photon source. In a small number of instances, more than one photon is emitted, making the system vulnerable. A hacker could tap the system and measure one of the photons to discover what polarization the sender is using, and then send the other onto the receiver—all without revealing his or her presence.

That explains why entangled photons present an attractive future option. When two photons become entangled, if one is vertically polarized, the other is always polarized horizontally. The polarization of a single photon cannot be known until it is measured, and the measurement will automatically determine the polarization of the other photon, even if it is several hundred meters away. Albert Einstein dubbed this "spooky action at a distance." A QKD system using entangled photons would have a critical advantage: the key comes into existence simultaneously at both sender and receiver nodes, eliminating the possibility of interception.

Entangled-state quantum cryptography works by generating entangled-photon pairs and distributing them through fibers or free space so that each arrive at the receiver's detectors simultaneously. Once measured, the photons assume one of four polarization states at random. Entanglement works over fiber-optic lines, but there are inevitable losses, which limits transmission distance. Free-space techniques extend the entanglement to distances in the range of 24 km.

Last April, a team from the University of Vienna, Austria's ARC Seibersdorf Research (Seibersdorf), and Ludwig-Maximilians University (Munich, Germany) performed the first quantum-secured transfer of money using entangled photons. The scientists installed a 1.45-km fiber-optic line under Vienna's streets to link a transmitter at city hall to a receiver at the headquarters of an Austrian bank. They used a crystal with nonlinear optical properties to split photons with wavelengths of 405 nm into pairs of entangled photons with wavelengths of 810 nm. Using the key, the team safely transferred funds from city hall to the bank.

In April 2004, the European Union launched the SECOQC project, which involves 41 participants from 12 countries: Austria, Belgium, Canada, the Czech Republic, Denmark, France, Germany, Italy, Russia, Sweden, Switzerland, and the United Kingdom. Participants have pledged 11.4 million euro ($14.8 million U.S.) in funding over the next four years to create a secure quantum network globally. One of the project's eight goals is to develop a suitable QKD system. The techniques under consideration are the University of Vienna's entangled-photon scheme, ID Quantique's attenuated pulsed-laser source of single photons, and free-space links. The last would also enable key distribution using modulated coherent states rather than photon counting.

Faster detectors

Future developments will focus on faster photon detectors, a major factor limiting the development of practical systems for widespread commercial use. Chip Elliott, BBN's principal engineer, says the company is working with the University of Rochester and NIST's Boulder Laboratories in Colorado to develop practical superconducting photon detectors based on niobium nitride, which would operate at 4 K and 10 GHz. Laboratory models can already detect billions of photons per second—several hundred orders of magnitude faster than today's commercial photon detectors.

The ultimate goal is to make QKD more reliable, integrate it with today's telecommunications infrastructure, and increase the transmission distance and rate of key generation. "It's one thing to achieve quantum cryptography in the laboratory on a multimillion dollar government-funded project," says MagiQ's Trifonov. "It's quite another to make it reasonably cost-effective for commercial applications."