Quantum Network Set to Send Uncrackable Secrets

Next week in Vienna, European scientists and engineers will put the bizarre and abstruse laws of quantum mechanics to a practical, everyday use. Researchers will demonstrate a network for transmitting uncrackable encoded messages in quantum-mechanical packets of light. Such quantum networks could soon link banks or government offices, some researchers say. “This is a moment when research turns into technology,” says Chip Elliott, a network engineer at BBN Technologies in Cambridge, Massachusetts, who 5 years ago led efforts to build the more primitive DARPA network. Still, he cautions, “it’s too early to say whether there are customers for this.”

The product of a 4-year, €11.4 million collaboration funded by the European Union, the network will connect six sites across the city through eight existing fiber-optic links, all belonging to industrial giant Siemens. It will distribute the numerical “keys” for scrambling secret messages.

A message can be encrypted by converting it into a string of 0s and 1s and scrambling those bits by compounding them with a key, a random string of 0s and 1s. If only the sender, Alice, and the receiver, Bob, know the key, then only they can read the message. The trick is to transmit the key without its being seen by an eavesdropper, Eve. So-called quantum key distribution exploits the fact that it’s impossible to measure a photon without also altering it.

For example, Alice can send Bob individual photons polarized horizontally to signify 0 or vertically to signify 1. Thanks to quantum weirdness, she can also send photons polarized both ways at the same time. If Eve tries to
measure the light particles, that very act will “collapse” the two-way-at-once photons into either vertical or horizontal ones. Bob and Alice can detect that by comparing some randomly chosen bits.

A few companies make quantum systems to connect two users through a single link. The Vienna project weaves six disparate systems into an automated network. “You just make a connection to one node and can connect to any other user,” says Andreas Poppe, a physicist at the Austrian Research Centers in Vienna.

In fact, the network will not be a fully quantum network, which would let Alice pass photons to Bob across any number of nodes. That would require devices called “quantum repeaters” that are at least a few years away. In the Vienna network, each user generates a key that is stored as classical (nonquantum) 0s and 1s in the node he or she links to. Those classical bits flow from node to node as needed, quantum mechanically encrypted as they cross each link. “What our network assumes is that you can trust each of the intermediate nodes,” says Andrew Shields, a physicist with Toshiba Research Europe in Cambridge, U.K.

Nobody will be invited to try to hack the network, either. That’s because hackers would likely ignore the quantum mechanics and attack the system’s conventional parts, which wouldn’t test the new concept, Poppe says.

Still, researchers hope the demonstration will signal the emergence of the new technology, especially for private networks. Some experts are skeptical. “I think the impact on the actual practice of cryptography is likely to be small,” says Ronald Rivest, a computer scientist at the Massachusetts Institute of Technology in Cambridge. Current techniques, which rely not on shared secret keys but on mathematical manipulations that are practically impossible to work backward, already work well, says Rivest, who predicts that the niche for the quantum systems will be small.

Network developers hope for more. “I think, on our scale of things, it will be a historic day,” says physicist Nicolas Gisin of the University of Geneva, Switzerland. The question is, will technologists and market analysts see it that way, too?

—ADRIAN CHO
Quantum Cryptography

Quantum-Encrypted Network Debuts in Vienna

A team of international researchers and Siemens Austria unveiled the first commercial network protected by quantum encryption at a Development of a Global Network for Secure Communication based on Quantum Cryptography (SECOQC) conference in Vienna, BBC Radio reports. The network connected six different locations in Vienna and one in the neighboring town of St. Poelten, and involved nearly 125 miles of fiber-optic cable.

While standard network security encryption is based on complex mathematical equations that are extremely difficult to crack, it is vulnerable to parties who possess sufficient computing resources and time. The promise of quantum encryption is its reliance on the laws of quantum theory, which has been shown to be inherently unbreakable.

“All quantum security schemes are based on the Heisenberg Uncertainty Principle, on the fact that you cannot measure quantum information without disturbing it,” Gilles Brassard, a computer scientist at Montreal University and a pioneer of quantum cryptography, told BBC Radio. “Because of that, one can have a communications channel between two users on which it’s impossible to eavesdrop without creating a disturbance. An eavesdropper would create a mark on it. That was the key idea.”

The Vienna network used extremely faint beams of light, equal to single photons being fired a million times a second, which raced between the nodes. When an intruder tried to eavesdrop on the quantum exchange, the photons scrambled, and the rise in the error rate at the node detectors announced the attack. The network shut down without being compromised, and the network connections were rerouted via other nodes without any interruption in connectivity.

The SECOQC researchers believe a business-viable network is possible in three years.