

Robust quantum encryption demonstrated over high-speed internet network

Over a fiber-optic line with state-of-the-art throughput, light carrying the classical information of internet users was joined by photons serving as quantum cryptographic keys.

By **Matt von Hippel**

A collaboration of three companies has demonstrated an exchange of data protected by both quantum cryptographic keys and a next-generation encryption scheme over a high-speed internet link while maintaining the network's regular commercial traffic. The recent demonstration is a key step in showing that an internet capable of supporting advanced quantum encryption is feasible for widespread use, according to Ravishankar Ramanathan, who studies quantum cryptography at the University of Hong Kong and was not involved with the demonstration.

Much of today's internet data are encrypted through the RSA protocol, which is difficult to crack because of how hard it is to factor large numbers. Quantum computers are expected to change that, making it possible to break the codes that keep most data secure. (See the interview with Peter Shor that appeared last year in *PT* about the factoring algorithm named for him.)

To avoid the problem, researchers have explored two options. One, called quantum key distribution (QKD), was proposed by Charles Bennett and Gilles Brassard in 1984. In QKD, a message is paired with a quantum state that serves as a key for decoding. By



▲ Researchers used specialized servers to generate and measure the photons that served as carriers of quantum cryptographic keys. (Photo courtesy of Toshiba.)

sharing a few measurements of the state with the recipient, the sender can verify that the key wasn't measured by an eavesdropper. (For more on QKD, see the 2021 *PT* article "A quantum leap in security," by Marcos Curty, Koji Azuma, and Hoi-Kwong Lo.) Another method, called

postquantum cryptography (PQC), involves designing new encryption schemes, based on different mathematical assumptions, that are expected to be harder for a quantum computer to crack. (See *PT*'s 2023 article on NIST's efforts to finalize new encryption standards.)

For sensitive data, it's possible to use both QKD and PQC to secure messages with physics and mathematics. "Using a hybrid approach—QKD to generate the keys and PQC to encrypt and authenticate the data stream—is a robust, multilayered solution," says Ramanathan.

Several previous demonstrations of the hybrid approach over standard internet lines have focused on the distance of the transmission, specifically the ability to keep photons in a coherent quantum state for hundreds of kilometers over infrastructure that can easily be updated to use new PQC protocols. The new demo is over a much smaller distance: a 21.8-kilometer link between Chicago and Hammond, Indiana.

The new demo, by researchers with the companies Ciena, Quantum Corridor, and Toshiba, competes on throughput. Whereas other hybrid QKD networks have classical traffic at 400 gigabits per second or 800 gigabits per second, this network carries 1.6 terabits per second. The researchers had to manage traffic on different wavelengths to support both the demo and Quantum Corridor's commercial customers. They used Ciena technology to encrypt the signals with PQC and multiplex them across the different wavelengths. Toshiba's QKD servers generated and measured the quantum states that served as keys.

"Until this demo, if you wanted the physical security of QKD, you had to accept lower overall data throughput on the line," says Ramanathan. "The reason why this speed matters is that it proves to the big players—like AWS, Google, or Microsoft—that connect AI clusters and cloud computing hubs that they do not have to throttle their massive AI data pipelines to achieve hybrid quantum safety."

Because it requires specialized sources and detectors, QKD is expensive to implement and so may be limited to high-value links in the near term. And longer-distance links currently require trusted relays, a vulnerability that worries organizations like the National Security Agency. Ciena is optimistic that its technology will be applicable to other geographic areas and network types, says Paulina Gomez, the company's director of portfolio marketing.

Future demos may also expand to different QKD methods. The new demonstration used the original Bennett and Brassard algorithm, but some experts, including Ramanathan, advocate for newer algorithms that are resilient to a wider range of attacks. Toshiba has demonstrated one such procedure, called twin-field QKD, where photon keys are distributed from two different locations.

PT



MAKE A DIFFERENCE IN SCIENCE & SOCIETY

CONGRESSIONAL SCIENCE POLICY FELLOWSHIP

Help infuse science into the policy-making process. As a fellow, you will spend a year providing analytical expertise and scientific advice to Congress, informing important societal issues. Scientists of all career stages are welcome to apply.

Apply Now!



APS Deadline: November 4th

AIP Deadline: December 1st