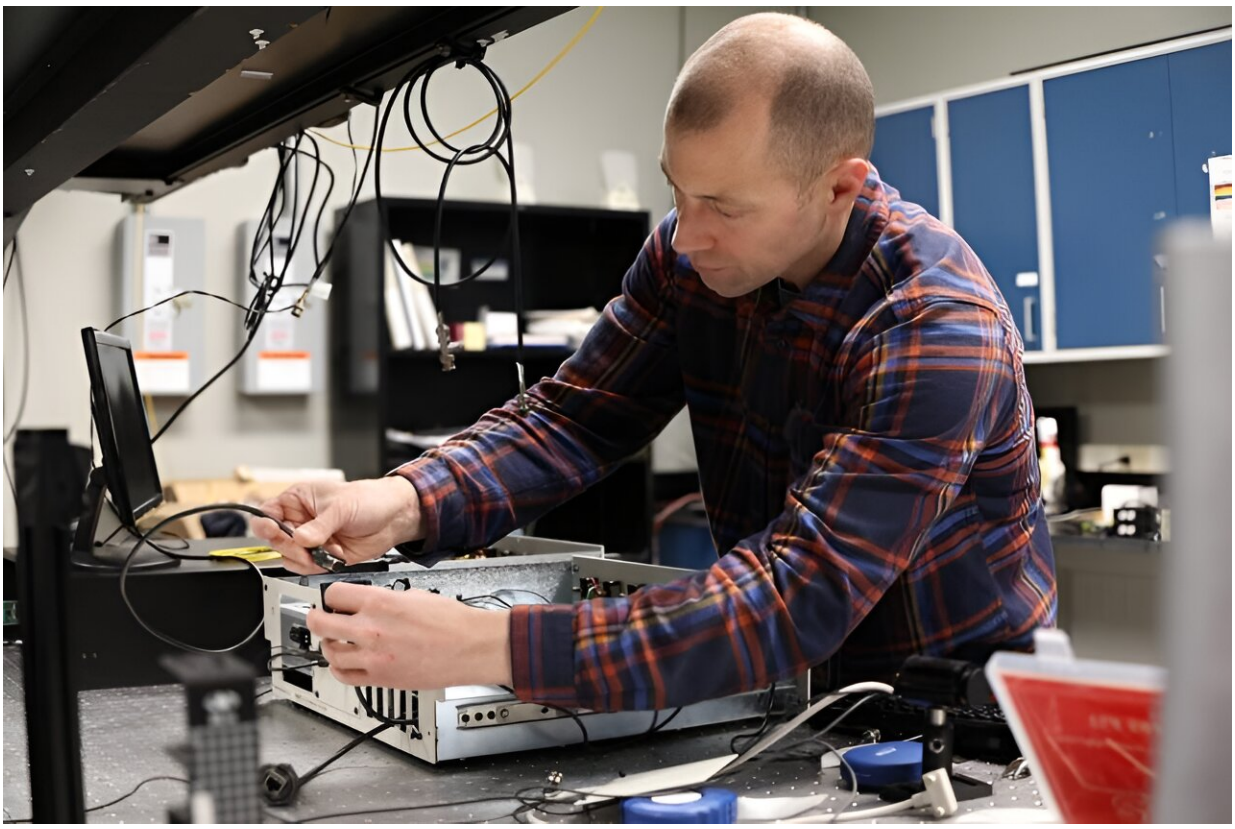
Researchers achieve quantum key distribution for cybersecurity in novel experiment

March 13 2024, by Reece Brown



ORNL researcher Brian Williams prepares for a demonstration of a quantum key distribution system. Credit: Genevieve Martin/ORNL, U.S. Dept. of Energy

Researchers at the Department of Energy's Oak Ridge National

Laboratory have demonstrated that advanced quantum-based cybersecurity can be realized in a deployed fiber link.

Their results, published in *CLEO 2023*, validate an earlier proof-of-principle laboratory experiment by ORNL scientists in 2015.

The team transmitted a quantum signal for quantum key distribution—a secure approach to sharing a secret key—using a true local oscillator. A local oscillator quells the effects of noise scattered from other data transmitted in the same fiber-optic network, and the work demonstrated coexistence between the quantum and conventional data signals.

The signal traveled across ORNL's fiber-optic network encoded in continuous variables that described the properties of light particles, or photons, in amplitude and phase. Using continuous variables of photons for encoding allows an almost infinite number of settings for distributing randomness that can be used for cybersecurity and enables compatibility with existing classical communications systems.

The ORNL team's experiment not only broke new ground in information security but leveraged existing fiber-optic infrastructure, which would enable cheaper, easier adoption.

The experiment resolved major roadblocks to implementing quantum key distribution while enhancing security, said Nicholas Peters, head of ORNL's Quantum Information Science Section and the study's principal investigator.

"Quantum key distribution is a cryptographic protocol where two parties can generate a secure key that only they know," Peters said. "In this experiment, this is done by using lasers to generate weak optical pulses between two points, usually referred to as Alice and Bob."

When the receiving party measures a pulse, measurements can reveal whether an eavesdropper intercepted and corrupted the message. In past experiments without a true local oscillator, this optical pulse was transmitted along with the local oscillator. Previous methods created the potential for vulnerabilities not addressed in current best practices defined by the underlying concept of security. The new method relies on optical signals generated by independent lasers at the transmitting and receiving points.

"Basically, we're looking at interference," said Brian Williams, lead author of the study and an ORNL quantum research scientist. "It's like throwing a rock into a lake and creating ripples. That's similar to the wavelike nature of a photon that we are looking at. If two rocks are thrown in, they create weird patterns in the water. We're doing a similar interference-based measurement on that quantum signal, but only the part that matches up with the laser gets detected. This requires a very narrow energy resolution."

Excess noise erodes the rate of the key that can be distributed. Too much noise, and a fraction of the potential key is consumed to protect confidentiality.

"The goal is to get the best possible signal-to-noise ratio," Williams said. "By using a narrow energy laser as your local oscillator, it acts as a filter for the background noise and improves the signal-to-noise ratio."

Future efforts will focus on reproducing the experiment's results under a wider range of network scenarios.

More information: Brian P. Williams et al, Continuous-variable quantum key distribution with true local oscillator, *CLEO 2023* (2023).

DOI: 10.1364/CLEO_FS.2023.FF1A.2

Provided by Oak Ridge National Laboratory