Corporate collaboration bolsters quantum encryption

June 27 2023, by Peter Grad

Credit: CC0 Public Domain

Toshiba Europe and global telecommunications corporation Orange say they have achieved a significant advance in securing network communications from ever-more powerful computer attacks.

Security experts have been warning that a new generation of quantum

computers is likely only a few years away from attaining the ability to crack today's stringent public key encryption codes.

Some experts say quantum computers will be strong enough to crack the widely adopted RSA-2048 encryption standard for secure online transactions within about 15 years. The Cloud Security Alliance had a more dire—and precise—prediction: Encryption safeguards will be overtaken by April 14, 2030. That date has been dubbed Y2Q, in a nod to Y2K, the label given to the worldwide chaos once predicted would occur the moment computers changed over from the year 1999 to 2000.

Quantum Key Distribution (QKD) has been viewed as a promising approach to protecting highly sensitive transmissions. But its implementation has faced obstacles such as the requirement of new fiber installation and increased costs.

In a paper published in May on the preprint server *arXiv*, the companies stated their new findings "could help network operators reduce the cost of implementing QKD by removing the need to invest in dedicated quantum fiber infrastructure."

Using a method called wavelength division multiplexing (WDM) allows the use of existing fiber networks, they said. WDM uses different wavelengths of light and special filters to avoid interference and reduce noise.

"Through the tests, researchers from Toshiba and Orange demonstrated the effective co-propagation of the classical and quantum signals with high secret bit rates, allowing them to co-exist while still being capable of effectively delivering keys at distances of up to 44 miles," the firms stated. "[This shows] great promise for deployments in metro networks in built-up areas."

Laurent Leboucher, Orange group CTO, said, "Together with Toshiba, we showed that it is possible to introduce new security functions in the operators' networks without requiring the use of dedicated fibers. With this cost-effective approach, we pave the way towards a digital fortress, guaranteeing the security of our customers' most valuable data."

QKD has been embraced by the encryption community because of its unique reliance on the laws of physics to detect any effort to tap into transmissions. A hacker attempting to eavesdrop will alter the state of transmission photons that will immediately interrupt the transmission and reissue a new encryption key.

The Quantum-Safe Security Working Group supports the use of QKD "to protect and future-proof data against developments to computer power, new attack strategies, weak random number generators, and the emergence of quantum computers."

The researchers noted they developed a new metric that acknowledges it is power, not the number of channels, that has the most impact on efficiency. This, they said, holds promise of aiding future studies in network and service planning.

"These results show the possibility to deploy commercial QKD system[s] on currently existing fully filled WDM links with 100 Gb/s and 400 Gb/s channels in data center interconnection (DCI) applications," they said.

More information: P. Gavignet et al, Co-propagation of 6 Tb/s (60*100Gb/s) DWDM & QKD channels with ~17 dBm aggregated WDM power over 50 km standard single mode fiber, *arXiv* (2023). DOI: 10.48550/arxiv.2305.13742