Enabling Unconditional Security of Critical Data in the Quantum Era

Growing cyber security threats in the quantum era

Data security continues to be a critical concern for individuals, businesses, and governments, as sensitive information is increasingly being stored and transmitted electronically. And with the global average total cost of a data breach at $4.35M in 2022—an all-time high according to IBM, protecting the confidentiality, integrity, and availability of data as it traverses the network is essential to mitigate data security risks.

While these data security concerns are important, advances in quantum computing introduce a new paradigm in data security: *Time-Value of Information.* The concern is best illustrated with the ongoing threat that follows the concept of 'harvest now, decrypt later', which is used to describe a threat model in cryptography where an attacker steals encrypted data with the intention of decrypting it in the future when a method to quickly decrypt the data becomes available. For organizations with data that retains its value over time, such as Intellectual Property and data with military or national security implications, the rapid advances in the computational power of quantum computers make this approach to stealing sensitive data particularly worrisome. Hence the need for a solution that provides unconditional security of critical data against quantum computer attacks.

How will quantum computers affect today's encryption systems?

Today's symmetric key encryption algorithms, like AES, continue to provide adequate data security. However, quantum computers pose a significant threat to many classical key exchange algorithms, which are used to securely establish a shared secret key between two parties for the purpose of encrypting confidential information. One of the key features of quantum computers is their ability to perform factorization and discrete logarithm computations much faster than classical computers. This means that they would be capable of breaking today's widely used key exchange algorithms, including the RSA and Diffie-Hellman algorithms, which rely on the difficulty of these mathematical problems. As such, organizations dealing with information that will maintain its value over the next 5-10 years must be aware of the threat posed by quantum computers when they become powerful enough to break current cryptographic algorithms and need to mitigate that threat accordingly.

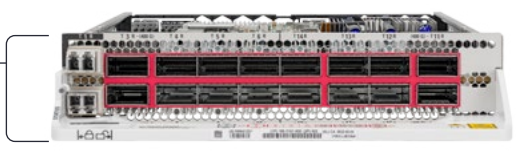
In-flight data security today and in the quantum era

Today, large amounts of critical data are in-flight as high-bandwidth communications occur beyond the walls of the data center, traversing a larger, potentially worldwide network. A comprehensive IT security approach must therefore encompass a robust in-flight encryption solution as part of its holistic security strategy. By encrypting data as it leaves the security of the private cloud, operators can protect this data from unauthorized intercept as it traverses the network, crossing varying security levels as it reaches its destination. Ciena's WaveLogic™ Encryption solutions leverage industry-leading coherent technology to enable flexible and customizable wire-speed optical encryption for securing all in-flight data, all the time. With Ciena's Waveserver® 5 operators benefit from programmable wavelength capacities from 200 Gb/s to 800 Gb/s, scaling up to 6.4 Tb/s of encrypted capacity per chassis. Additionally, by combining standards compliant algorithms and a locally provisioned pre-shared key (PSK), the solution provides resistance to quantum computer attacks against key exchange algorithms.

Ciena's Waveserver 5

6.4 Tb/s of encrypted capacity in 2RU

Waveserver 5 Encryption Module



1.6 Tb/s of encrypted capacity per module

Quantum Key Distribution (QKD) systems are a type of quantum communication technology that allow two parties to securely share a secret key. The key can then be used by symmetric encryption algorithms like AES to provide a secure communication channel. QKD exploits a fundamental principle of quantum physics—observation causes perturbation—to generate cryptographic keys over fiber optic networks with provable security: An eavesdropper intercepting the key generation process on the QKD quantum channel will necessarily translate into a perturbation that can be detected by the sender and recipient. ID Quantique's Cerberis XG platform is IDQ's fourth-generation QKD system that supports any kind of network topology, such as point-to-point, relay, ring, and star networks.

IDQ's Cerberis XG QKD System

Enabling unconditional security of critical data in the quantum era

As we approach the quantum era, the interworking of QKD systems with encryption systems is an active field of research and development in the industry, supported by an ETSI standard defining the API for the QKD key interface. This interface was leveraged as part of a joint demonstration performed by Ciena and IDQ that combines Ciena's sixth-generation always-on optical encryption technology with IDQ's Cerberis XG QKD system to showcase how quantum-secured optical channels can enable network operators to detect and defend against eavesdroppers across metro applications, including Data Center Interconnects.

The demo features Ciena's Waveserver 5 platform powered by proven 800 Gb/s encryption leveraging open APIs to communicate with IDQ's QKD system. The optical data channel is encrypted at the OTN layer using the symmetric keys generated by the QKD technology, enabling a solution that is mathematically proven to provide unconditional security of all critical in-flight data and that is highly resilient against eavesdropping attempts.