Quantum Computing/Quantum Resistant Cryptography

Kelli Hall
Cybersecurity Services Manager
Technica Corporation

Challenge:

- Data protected by Rivest-Shamir-Adleman (RSA), Diffie-Hellman and other asymmetric encryption algorithms/methods are at risk from emerging quantum computers. Those methods are current techniques of key agreement procedures also known as key exchange protocols, regardless of Layer-1 encryption, MACsec, IPsec or TLS
- Emergence of quantum computers with ultra-high processing power poses a significant threat to established methods of securing communications networks by breaking the asymmetric crypto algorithms
- Attackers today can read and store the dataflow including the key exchange, waiting until the quantum computer exists and decrypt stored data
- Enterprises need to begin security measures now

Solution:

- Develop an optical transport solution protected by post-quantum cryptography (PQC) based key establishing mechanism
- Combine post-quantum cryptography with a classical key exchange algorithm that can be deployed over any optical transport network forming a crypto-agile hybrid solution
- Ready for software updates to comply with emerging specifications, including NIST's PQC standardization with NSA approvals
- Demonstrate practices to ease migration from public-key cryptographic algorithms to replacement algorithms that are resistant to quantum computer-based attacks

Technica's technology partner, ADVA, is pioneering lowest-latency, high-bitrate transmission systems and taking a significant step towards quantum-safe security. ADVA is the first company to commercialize a quantum-safe optical transport solution and introduce a crypto-agile packet network product. Both solutions can be operated with selected PQC and upgraded to NIST-selected PQC algorithms via Software. Integrating all security functions into a crypto module creates a future-proof security solution by removing quantum risk.

As the industry's first optical transport solution secured by PQC, ADVA's quantum-safe FSP 3000 ConnectGuard™ optical encryption solution protects data against cyberattacks, including those from quantum computers that could break today's cryptographic algorithms. The security technology relies on a hybrid key exchange system, combining PQC algorithms with classical encryption methods for crypto-agility, ready for future software updates.

This quantum-safe encryption technology provides organizations a safeguard for their networks before danger materializes. Data will be protected even from cybercriminals' intent on harvesting information stored today and exploiting it tomorrow. This solution provides long-term security for data in motion and can be upgraded later to comply with emerging specifications, including the NIST's PQC standardization.

As recommended by leading cybersecurity authorities, the PQC-protected solution utilizes the traditional Diffie-Hellman protocol and combines it with a new algorithm based on the quantum-safe McEliece cryptosystem. This technology merger produces encryption keys that even powerful quantum computers are unable to crack, delivering data integrity with quantum-safe Layer 1 AES-256 protection. The solution ensures minimal impact on latency, throughout and performance, and is also easily deployable over long-haul and multi-operator links. Most importantly, it works over any distance and in any optical transport network.

Organizations are aware of the security threat that quantum computing represents today. With many experts anticipating powerful commercially available quantum computers in the next decade, it's now universally understood that the danger to encrypted data and content is real, and the stakes are high. Integrating PQC security into the encryption solution protects networks and data today against tomorrow's threats.