riverbed

SOLUTION BRIEF

Secure Data Against Quantum Risk

Post-Quantum Encryption with RiOS 10

Executive Summary

Encryption, at its most basic form, employs algorithms using difficult-to-solve math problems to convert plaintext into ciphertext. Current encryption methods such as RSA, Diffie-Hellman, and elliptic curve cryptography use math problems that are practically impossible to break with computers available today. Quantum computing is expected to solve these math problems in minutes.

While this is still beyond the known capabilities of existing quantum computers,[1] quantum capabilities are progressing faster than expected.[2] This suggests that the security timeline for current encryption systems may need to be revised. Proactive investment in post-quantum cryptography is not just prudent—it's becoming urgent.

Post-quantum cryptography (PQC), also known as quantum safe or quantum resistant cryptography, is a set of cryptographic algorithms designed to remain secure against quantum computers. As the transition to any new security approach requires significant time and planning, organizations must begin preparations today to mitigate the potential security threat of quantum computing.

> Gartner VP Analyst Bart Willemsen warned that "quantum computing will weaken asymmetric cryptography by 2029." Given that cryptographic upgrades often span multiple years, he urged organizations to begin strategic planning now, especially for infrastructure with hard-coded crypto dependencies.[3]
>
> CSOonline.com

[1] Initial quantum computing capabilities are available today from QuEra Computing on AWS Bracket, Dwave, Nvidia, while other organizations are also working in this area.

[2] CSOonline.com: "Breaking RSA encryption just got 20x easier for quantum computers"

[3] ibid

Introduction

Quantum computing is a revolutionary technology that leverages the principles of quantum mechanics to perform computations far beyond the capabilities of classical computers.

Quantum computing utilizes quantum bits (qubits) that can exist in multiple states simultaneously, thanks to superposition and entanglement. This allows quantum computers to process a vast number of possibilities at once, making them exponentially more powerful for certain tasks compared to classical computers

Today's computers use binary bits, which are like tiny switches that can be either on (1) or off (0). These bits help the computer do all its calculations and tasks. Quantum computing is like a super-powered version of this. Instead of just being on or off, the tiny switches (called qubits) in a quantum computer can be both on and off at the same time. This is because they use the strange rules of quantum mechanics, which is a branch of physics that deals with the tiniest particles in the universe.

Because qubits can be in multiple states at once, quantum computers can solve certain problems much faster than regular computers. It's like being able to read a whole book in a blink of an eye instead of page by page.

Post-Quantum Cryptography on RiOS 10

When data is moved across a network, it can be especially vulnerable to cyber attacks, and with more and more data moving between edge, data centers and cloud, often driven by data-hungry AI applications, the threat is increasing. Secure networking at scale has never been more important.

Riverbed RiOS 10 now supports **PQC** with **hybrid key exchange** which uses both traditional **elliptic curve cryptography** (ECC) and "Kyber" (**Module Lattice Key Encapsulation Mechanism** or ML-KEM) key exchange algorithms when negotiating **Transport Layer Security** (TLS) v1.3 secure connection. Combining both algorithms provides the existing proven ECC-based algorithms and the newer quantum resistant ones. This ensures the benefits of **Perfect Forward Secrecy** (PFS) in preventing the "**Harvest Now, Decrypt Later**," a cyber threat method of stealing data today and waiting for the availability of quantum computing to break common encryption methods mentioned above.

The use of ML-KEM has been standardized for use in TLS v1.3 and fits cleanly by using the "Supported Groups" extension. This is limited to the handshake negotiation used to initiate a secured connection, after which it is typical for **Advanced Encryption Standard** (AES) symmetric encryption to be used for encrypting traffic which is already considered quantum resistant.

PQC Technical Specifications on RiOS 10

- RiOS 10 currently[4] provides PQC support for the following named groups:
  - ☐ X25519MLKEM768
  - ☐ SecP256r1MLKEM768
  - ☐ SecP384r1MLKEM1024
  - ☐ ML-KEM-512
  - ☐ ML-KEM-768
  - ☐ ML-KEM-1024

Move Forward with Post-Quantum Era Encryption

The quantum computing revolution is imminent, and the threat it poses to current cryptographic systems cannot be overstated. The encryption that protects data-in-transit must be quantum-resistant to avoid catastrophic breaches.

Organizations must act now to adopt post-quantum era encryption to future-proof their networks. Solutions like RiOS 10, which post-quantum era cryptography, offer a pathway to secure and compliant digital infrastructure in a rapidly evolving cybersecurity landscape.

[4] Initial support applies to the Riverbed inner channel between SteelHeads. RiOS 10 also has planned support for PQC between client/server and SteelHeads.

riverbed

About Riverbed

Riverbed, the leader in AIOps for observability, helps organizations optimize their user's experiences by leveraging AI automation for the prevention, identification, and resolution of IT issues. With over 20 years of experience in data collection and AI and machine learning, Riverbed's open and AI-powered observability platform and solutions optimize digital experiences and greatly improves IT efficiency. Riverbed also offers industry-leading Acceleration solutions that provide fast, agile, secure acceleration of any app, over any network, to users anywhere. Together with our thousands of market-leading customers globally – including 95% of the FORTUNE 100 – we are empowering next-generation digital experiences. Learn more at riverbed.com.