riverbed

WHITE PAPER

Preparing for the Quantum Era in Networking with Post-Quantum Cryptography

Contents

Executive Summary: The Quantum Computing Challenge to Cybersecurity

As enterprises operate across the globe, the resiliency of their business depends on their networks maintaining continuous network operations with high performance and secure delivery of data and applications from these locations, across the enterprise. Secure delivery of business critical, secret or confidential data depends on strong encryption and the operation of all security systems to maintain end-to-end security chains.

The rise of quantum computing poses a critical threat to traditional encryption systems, specifically those protecting data-in-transit and digital signatures in networking environments. Many encryption algorithms foundational to modern cybersecurity, such as RSA, Diffie-Hellman, and elliptic curve cryptography, depend on the difficulty of solving problems like integer factorization and discrete logarithms; these logarithms will become vulnerable once quantum computers can execute prime factorization in minutes, vs. what would take centuries using current computers. Governments are recognizing this threat and directing agencies to improve the security and integrity of software and network infrastructure critical to their resilient operations (See sidebar on page 5).

Without proactive measures by IT security professionals and network architects, quantum computing could compromise the confidentiality and integrity of sensitive data in the near future, potentially exposing governmental, financial, and personal information and subjecting organizations to the significant impact of those breaches.

Resilient Networking

Resilient networking is the ability to maintain continuous, high-performance network operations even in the face of unexpected disruptions. Resilient networking strengthens the business resiliency by focusing on high performance, security, and observability across network operations, enabling organizations to securely deliver apps and data at every scale and network condition. It involves:

- **Peak Performance:** Enables seamless delivery of apps and data across mobile, edge, data center, and cloud environments. It mitigates network challenges and scales from 5G to 500G, adapting to meet large-scale network demands and empower real-time decision-making to keep the business operating at its highest potential.
- **Secure Delivery:** Ensures secure data delivery from data storage—whether in the cloud or data center—straight to the edge. It safeguards data with encryption both at rest and in transit and makes possible near real-time data synchronization between central storage and the edge.
- **Visibility and AIOps:** Empowers IT teams with AI-enabled automations and remediations to prevent, identify and resolve issues before they affect digital experience and business outcomes.

In essence, resilient networking solutions help businesses stay connected, secure, and efficient, no matter what challenges they face.

Introduction

The cybersecurity landscape is rapidly evolving, and the arrival of quantum computing is set to disrupt the way we protect digital assets. Quantum computers, once fully realized, will be able to break current encryption methods that are foundational for securing data-in-transit (such as TLS/SSL, VPNs) and digital signatures (used to authenticate identities and transactions). The result: a potentially catastrophic loss of privacy, security, and business integrity.

In this white paper, we will explain why post-quantum cryptography solutions are essential, explore the risks involved, and outline how Riverbed can help organizations take proactive steps to secure their networks from the risk of quantum computing.

Why Current Encryption Methods Are at Risk

Quantum computing, leveraging principles of quantum mechanics, promises unprecedented computational power. Unlike classical computers, which process bits sequentially, quantum computers operate on qubits that enable massive parallelism. This capability poses a significant threat to current cryptographic protocols, which rely on the infeasibility of solving certain mathematical problems—a task quantum computers could accomplish exponentially faster.

Due to their cost and size, quantum computers capable of breaking encryption are likely to first be developed by technology companies, research institutions, or nation-states. Quantum computing will not simply show up on the doorstep one day, but rather these capabilities will evolve and increase over time. The point at which quantum computing will be able to break current encryption methods is hard to predict. But what we do know is QuEra plans to launch a quantum computer with 30 logical qubits this year, and a more advanced machine with over 10,000 physical qubits in 2026. Microsoft and Atom Computing plan to launch a commercial quantum computer in 2025.

In the wrong hands, these powerful machines could pose a serious threat to sovereign state national security, making it crucial to prepare now for the upcoming post-quantum cryptographic standards. Organizations must act now to implement post-quantum era encryption and avoid exposure to imminent risks.

The Problem: Vulnerabilities of Data-in-Transit

Every time data is sent across the network—whether it is personal information, corporate emails, or financial transactions—it is typically protected by encryption mechanisms like TLS/SSL (Transport Layer Security) or VPNs (Virtual Private Networks). These mechanisms rely on public-key encryption algorithms, such as RSA and ECC, to safeguard data as it travels from one endpoint to another.

However, quantum computers using quantum algorithms – for example Shor's algorithm will be able to efficiently solve the mathematical problems these encryption methods rely on, effectively rendering traditional encryption obsolete. This means encrypted communications, which are currently considered safe, will be decryptable by a sufficiently advanced quantum computer.

It is important to note that encryption vulnerabilities do not require a fully realized quantum computer. Attacks could occur on encrypted data that is intercepted today and stored until effective quantum computers become available. This is called a harvest-and-decrypt attack and it poses a critical risk to long-term data security.

Why Is This an Urgent Issue?

Quantum Computing Is Advancing Rapidly

While large-scale, fault-tolerant quantum computers are not yet a reality, progress in the field is accelerating. Due to their cost and size, quantum computers capable of breaking encryption are likely to first be developed by technology companies, research institutions, and nation-states. In the wrong hands, these powerful machines will pose a serious threat to governments, national defense, financial institutions, health care systems and many other entities that hold critical, financial, legal and personal data, making it crucial to prepare now for the upcoming post-quantum cryptographic standards.

According to Vijoy Pandey, SVP and GM at Cisco, "Breaking RSA or ECC encryption with a quantum computer requires running something called Shor's algorithm at scale. The biggest question has always been around how many physical qubits you need to run Shor's. For years that number was in the millions, which made the threat feel distant. The 2021 Gidney-Ekera paper, the prior gold standard, put it at ~20 million qubits.

"On March 31 on this year, a team from Caltech and Oratomic, including John Preskill, one of the architects of quantum error correction, published a paper bringing that number down to 10,000–14,000 physical qubits on a neutral-atom architecture. For context: some neutral-atom labs have already demonstrated arrays of 6,100 qubits. Which means that the gap between theory and practice just went from roughly 3,000x to about 2x."

The threat of quantum computing to current encryption methods has reached the attention of the White House, as seen in the Executive Order 14144 of January 16, 2025. It directs the U.S. Cybersecurity & Infrastructure Security Agency's (CISA) Post-Quantum Cryptography (PQC) initiative is coordinating efforts with interagency and industry partners to address the threats posed by quantum computing and support critical infrastructure and government network operators during the transition to post-quantum cryptography.

US Presidential Executive Order on Cyber Security Emphasizing Quantum Readiness

"Alongside their benefits, quantum computers pose significant risk to the national security, including the economic security, of the United States. Most notably, a quantum computer of sufficient size and sophistication—also known as a cryptanalytically relevant quantum computer (CRQC)—will be capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world. In National Security Memorandum 10 of May 4, 2022 (Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems), I directed the Federal Government to prepare for a transition to cryptographic algorithms that would not be vulnerable to a CRQC."

Executive Order 14144 of January 16, 2025
"Strengthening and Promoting Innovation in the Nation's Cybersecurity"

The European Union issued a similar directive in April 2024 to coordinate an implementation roadmap for Post-Quantum Cryptography.

Post-Quantum Cryptography Solutions

The U.S. National Institute of Standards and Technology (NIST) has selected four algorithms during the PQC Standardization Process that can withstand a quantum computer attack. The public-key encapsulation mechanism selected was CRYSTALS-KYBER, along with three digital signature schemes: CRYSTALS-Dilithium, FALCON, and SPHINCS+. It is intended that these algorithms will be capable of protecting sensitive U.S. Government information well into the foreseeable future, ensuring the continued confidentiality and integrity of digital communications and signatures.

NIST Recommended Algorithms

- **CRYSTALS-Kyber:** Recommended for key encapsulation and secure transmission of data.
- **CRYSTALS-Dilithium:** Suitable for digital signatures and authentication.
- **FALCON:** A lightweight alternative for digital signatures in constrained environments.
- **SPHINCS+:** A stateless hash-based scheme that provides long-term 2^{128} (two to the power of 128) security against quantum attackers.

Riverbed RiOS 10 on SteelHead: The Post-Quantum Cryptography Solution

At Riverbed, we understand the urgency of preparing for the quantum future. Our state-of-the-art networking products have been built with post-quantum era encryption as a core feature, enabling you to ensure data-in-transit remains secure in the face of emerging quantum threats.

RiOS 10

Riverbed SteelHead solutions offer a comprehensive solution for business resiliency, by accelerating applications and data across the enterprise for thousands of customers globally. It enhances network performance, reduces costs, and improves user experience across distributed enterprise environments.

RiOS 10 integrates post-quantum era algorithms, allowing organizations to seamlessly secure their networks against quantum risks while maintaining compatibility with existing infrastructure.

> "But it would be prudent to assume that hostile actors may be scooping up large amounts of encrypted data and may be storing it away for future decryption. That is at least a sensible working assumption."
>
> Robert Hannigan, Chairman, BlueVoyant

For governments, financial services companies, healthcare providers, and other industry segments concerned about privacy today and tomorrow, Riverbed understands the need to step up security in a looming quantum computing threat to your data. By adopting RiOS 10, you can mitigate future risk, comply with emerging cybersecurity standards, and build trust with clients and partners, ensuring that sensitive data remains secure even in the age of quantum computing.

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.

Learn More

To learn more about Riverbed, please visit riverbed.com/products.

riverbed

About Riverbed

iverbed, 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.