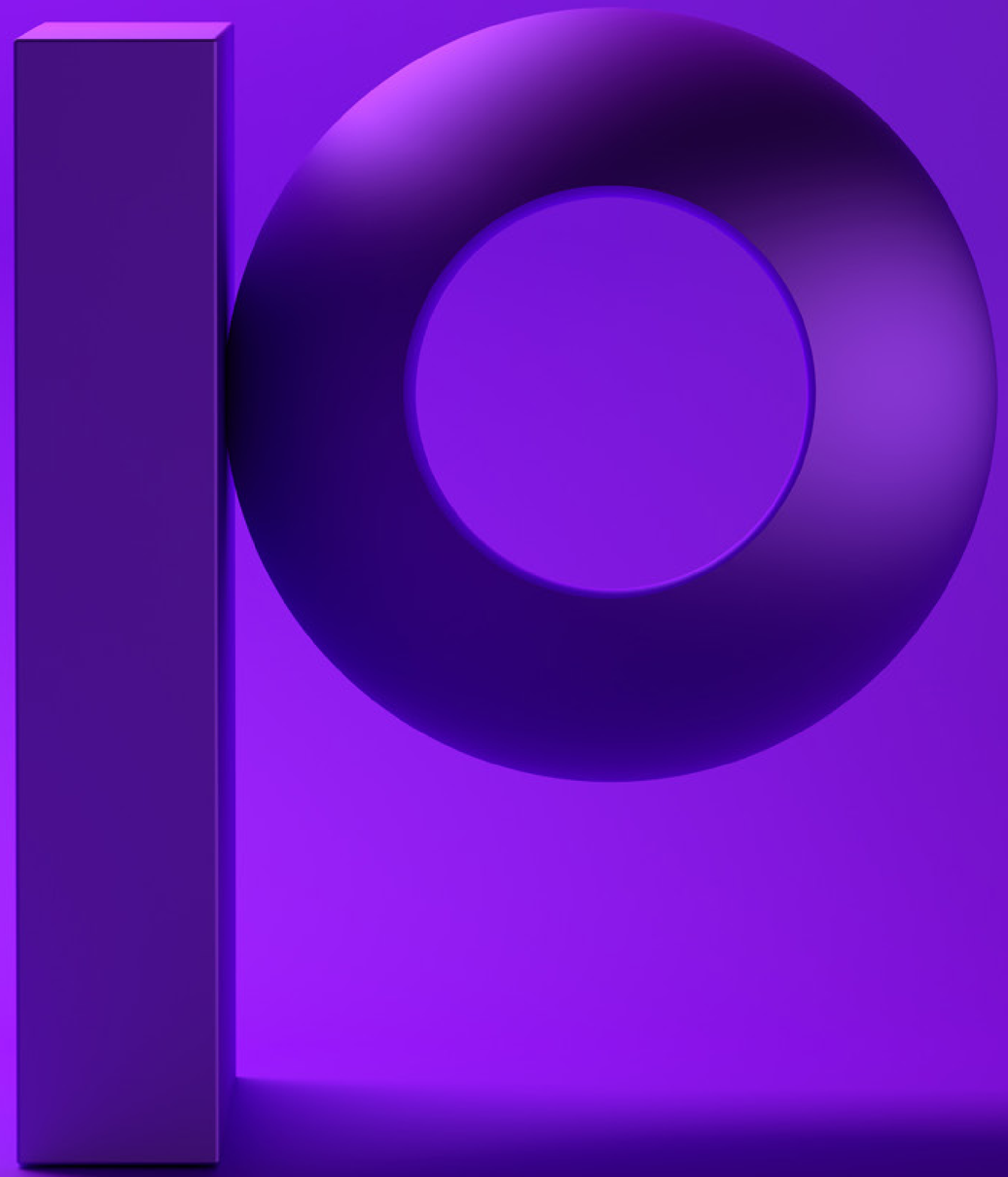
precisely

Quantum Computing and Your Encryption: What Every IT Leader Needs to Know Now



The Quantum Leap

You're about to face one of the most significant shifts in the history of technology. And it's called Quantum Computing. This isn't just another "next-gen" tech update. Quantum computing is an entirely new paradigm. It breaks the mold of how computing works today—replacing the logic we've all built systems around for decades with a radically different framework.

No, your IBM i isn't going anywhere just yet. But quantum computers already exist. And while the machines themselves are still evolving, the impact is coming—fast.

The upside? Mind-blowing breakthroughs in medicine, logistics, materials, and more.

The downside? Quantum computing puts today's encryption at serious risk. That's why this guide exists—to help you understand what's happening, what it means for your security posture, and what steps you should be thinking about today.

Bracing for Impact

Quantum computing will eventually make Moore's Law look quaint. For a while, you'll see its influence arrive slowly. Then, suddenly, it'll be everywhere.

We're talking about serious improvements across industries—from drug discovery to data analysis to logistics optimization. But the shift won't be all smooth sailing. The first wave of real disruption will hit cybersecurity, hard.

Here's the problem: most of the encryption methods in use today weren't designed to stand up to quantum-level brute force. Once quantum machines reach a certain capability, much of what we currently trust to protect sensitive data—will no longer be trustworthy.

And that moment? It's not decades away. Experts say it could happen within five years.

Your Starting Point in the Quantum Era

That's why we created this guide: to give you a clear, useful starting point. Inside, you'll find the core concepts, terminology, and real-world implications of quantum computing—specifically through the lens of IBM i security and encryption.

Whether you're knee-deep in daily operations or mapping out long-term strategy, this guide is designed to help you move forward with confidence.

Toward Quantum Supremacy

Let's define a key milestone: Quantum Supremacy. This is the point where a quantum machine outperforms even the fastest traditional supercomputers.

But before we get there, another important phase will arrive: the launch of commercially available Quantum-Capable computers. These won't just be science projects—they'll be tools bad actors can use.

When that happens, binary-based systems will begin their slow retreat—from critical systems to desktops, and eventually to historical footnotes.

Why Qubits Matter

To understand why quantum computing is so powerful, let's start with the qubit.

Traditional computers use binary bits: 1s and 0s. Quantum bits—or qubits—can be 1, 0, or both at once (thanks to a property called superposition). They can also be entangled with one another, creating a kind of instant coordination that defies classical physics.

We won't go deep into the quantum mechanics here. What matters to you is this: qubits unlock new dimensions of processing power. And that power scales fast.

Why It's Different: The Power Curve

With traditional computers, every doubling of bits gives you a modest increase in power.

With qubits? Doubling the number of qubits doesn't just double the power. It grows exponentially faster—what's known as a doubly exponential increase. That's why quantum computers are likely to surpass classical machines much sooner than most people expect.

The bottom line: quantum computing isn't just more power. It's a different kind of power. And it's coming.

A Quick Vocabulary Check

Before we dive further, here are a few terms you'll run into as quantum tech evolves:

- Qubits / Logical Qubits: Physical qubits are unstable and error-prone. To get reliable results, quantum computers bundle and correct thousands of them to produce a single logical qubit.
- Quantum Encryption: Uses quantum physics directly—like encoding data into photons or entangled particles—to protect information.
- Post-Quantum Encryption: Built with traditional computing methods but designed to resist attacks from quantum machines.

Why Encryption Is On the Clock

Quantum-capable machines don't need to be perfect to cause problems. Even early models will have enough raw power to challenge the encryption methods you rely on today.

Especially if AI gets involved.

Imagine AI-enhanced quantum computers built for one purpose: to break encryption. Now imagine what happens if bad actors get their hands on one.

To describe this risk, experts use the term Cryptographically Relevant Quantum Computers (CRQCs)—machines powerful enough to break today's encryption protocols.

If you think "well, we can upgrade our encryption later," here's why that thinking doesn't hold up.

Why Timing Matters

Let's say you're storing financial records, pension details, or health data. That information needs to stay protected for decades.

Now picture this: a hacker steals that data today, stores it, and waits. As soon as they get access to a CRQC—even years from now—they can decrypt it.

That's called a Harvest Now, Decrypt Later attack. And it's a real, growing threat.

This is why experts are urging IT leaders to act now—especially in environments like IBM i where long-term data retention is common.

Quantum Safe vs. Quantum Resistant

These terms get thrown around a lot. Here's what they really mean:

- Quantum Safe: Proven to be secure against both today's threats and tomorrow's quantum ones.
- Quantum Resistant: Likely secure, but still carries some theoretical risk under future quantum conditions.

That might seem like splitting hairs. But for long-term planning? It matters.

Looking at Your Encryption Stack

Most encryption protocols in use today weren't designed with quantum threats in mind. They're deeply embedded in systems, apps, and communication layers.

Replacing them takes time, effort, and planning. You don't want to wait until it's urgent.

For example:

- RSA, a widely used asymmetric encryption protocol, starts to buckle under quantum pressure. Increasing key lengths doesn't scale—it makes encryption slow and inefficient.
- AES, a symmetric key protocol, holds up better. You can double key sizes without killing performance, which is why AES-256 and beyond are considered Quantum Safe.

But even if you use AES, updating your broader system architecture still takes real planning.

Precisely Blog on RSA v. AES

The Post-Quantum Future Starts Now

In August 2024, after years of research, NIST officially approved three new encryption standards designed to stand up to quantum attacks. These are now the benchmark for Post-Quantum Cryptography.

One standard is designed for general encryption. The other two are for digital signatures and identity authentication.

If your work touches data protection in any way, now is the time to:

- Get familiar with these standards.
- Start mapping where current encryption is used in your systems.
- Identify where and how you'll phase in post-quantum options.

Federal Information Processing Standard (FIPS) 203 is intended as the primary standard for General Encryption. Among its advantages are comparatively small encryption keys that two parties can exchange easily, as well as its speed of operation.

This standard is based on the CRYSTALS-Kyber algorithm, which has been renamed ML-KEM, short for 'Module-Lattice-Based Key-Encapsulation Mechanism.'

FIPS 204 is intended as the primary standard for protecting digital signatures. This standard uses the CRYSTALS-Dilithium algorithm, which has been renamed ML-DSA, short for 'Module-Lattice-Based Digital Signature Algorithm.'

FIPS 205 is also designed for digital signatures. The standard employs the Sphincs+ algorithm, which has been renamed SLH-DSA, short for 'Stateless Hash-Based Digital Signature Algorithm.'

This standard is based on a different math approach than the ML-DSA used in FIPS 204, and it is intended as a backup method in case ML-DSA proves vulnerable.

You're Not Alone

While this may feel like uncharted territory, the reality is that this work has been quietly underway for years. The good news? You don't have to start from scratch. There's a growing ecosystem of resources, tools, and communities to help guide you forward.

Quantum computing is coming fast—but so are the solutions.

The best thing you can do right now is get informed, get strategic, and start preparing.

Your future systems—and the people who rely on them—will thank you.

precisely

About Precisely

As a global leader in data integrity, Precisely ensures that your data is accurate, consistent, and contextual. Our portfolio, including the Precisely Data Integrity Suite, helps integrate your data, improve data quality, govern data usage, geocode and analyze location data, and enrich it with complementary datasets for confident business decisions. Over 12,000 organizations in more than 100 countries, including 93 of the Fortune 100, trust Precisely software, data, and strategy services to power AI, automation, and analytics initiatives. Learn more at www.precisely.com

www.precisely.com