



Future-Proof Your Organization with Quantum-Safe Cryptography



Index

Introduction.....3

What is Quantum Computing?.....4

Keep Going!5

What’s Driving Quantum Computing?.....6

The Impact of Quantum Computing on Cryptography.....7

What is QSC?.....7

Why Does QSC Matter?.....8

QSC Isn’t a Luxury; It’s a Necessity8

Gradual Migration From Classical Cryptography.....9

Implement QSC Now.....9

NQX: Quantum-Proof and Future-Proof.....9

NQX Benefits Begin Now.....10

Contact.....11

Introduction

Words like “quantum computing” and “quantum-safe cryptography” may seem quite advanced for the average enterprise. But quantum computing is here, and it is of critical importance to every enterprise today. It’s also on the rise: the Global Quantum Computing Market is projected to **reach 949 million USD by 2025**, boasting a CAGR growth of 30% from 2017. By 2030, there could be between 2,000 and 5,000 **quantum computers** worldwide.

Many organizations are now actively involved in the world of quantum computing, including Google, IBM, Microsoft, and Amazon. Government-backed financial investments for quantum computing are also manifesting today, with countries across Europe as well as China, the US, and Russia hoping to apply quantum computing to communications infrastructure known as the “quantum internet.” NASA has even claimed to reach “quantum supremacy,” in which quantum computers have solved problems deemed unsolvable by classical computers.

This quantum computing guide will explore the rising importance, implications, and potential impacts of quantum computing, particularly within the cybersecurity sphere.

Quantum computing is an extremely advanced subject, one **SSH has explored in depth before**. For this reason, this guide won’t attempt to provide an in-depth understanding of quantum computing. Instead, we hope to help raise awareness of quantum computing’s significance for businesses and explain why organizations should introduce quantum-safe cryptography to combat the rising cybersecurity threats associated with quantum computing.

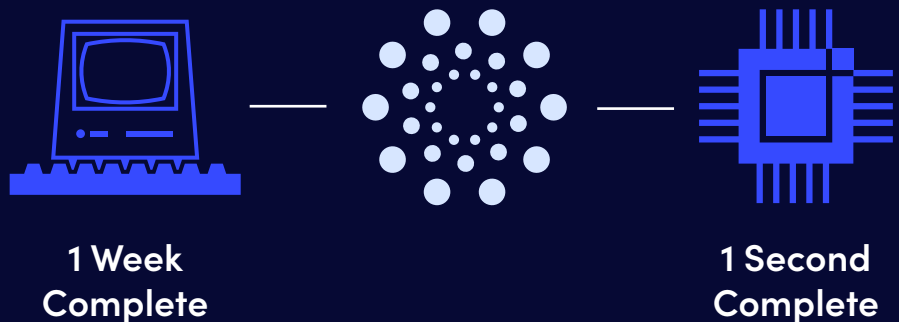
What is Quantum Computing?

In very simple terms, quantum computing applies the phenomena of quantum mechanics to computation in order to more rapidly, accurately, and efficiently solve particular problems — especially problems that could have potentially thousands of answers. For example, if you want to find the ideal seating arrangement for a 150-guest dinner party and take a multitude of factors into account, you could use quantum computing for a fast and first-rate answer.

In the very recent past, people had to rely on “supercomputers” to solve these kinds of problems. Supercomputers are essentially very large, powerful classical computers — but these aren’t great at solving problems that could have multiple answers. They don’t have the working memory to hold a wide variety of combinations; instead, they have to analyze each combination individually and one at a time. Unlike classic supercomputers, quantum computers can represent massive and elaborate problems all at once. This provides us with new opportunities for problem-solving.

Quantum computers use quantum bits called qubits (pronounced “Q” bits) to run multi-dimensional quantum algorithms, known as quantum wave interference algorithms. These algorithms connect many qubits, creating vast multidimensional computational spaces that can represent complex problems in new ways. Then, the solutions are translated from the quantum space into understandable insights.

In addition to being able to solve multidimensional problems, quantum computers present solutions faster than humans could have imagined in the not so distant past. For example, if it took one millisecond to check each item on a list, it would take a classic computer about a week to check a list of one trillion items. Meanwhile, a quantum computer could check this list in a single second.



How are quantum computers so efficient? Essentially, through a process called entanglement — in which qubits are correlated with one another through the use of exploitative quantum algorithms. The best answers are magnified, and the least likely answers are shrunk within the quantum computational space. This makes it easier to discover the right answers almost immediately.

Keep Going!

Don't be discouraged if you don't understand quantum computing. In fact, nobody in the world understands it — quantum computing, quantum mechanics, and quantum physics are all physiological ideas applied to math phenomena to explain nearly undocumentable states.

As Richard Feynman put it, "If you think you understand quantum mechanics, then you don't."

Quantum computing is complex, but it's also growing — and its effect is becoming more pervasive. It is important for businesses to understand quantum computing, even at a very basic level. In this next section, we'll explore why businesses shouldn't ignore the rise of quantum computing.

"If you think you understand quantum mechanics, then you don't."

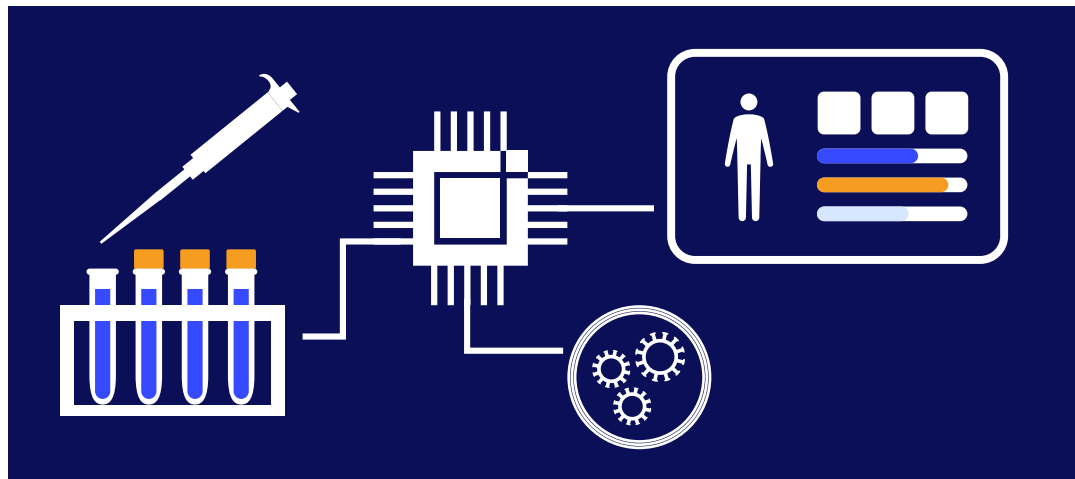
What's Driving Quantum Computing?

Despite its complex nature, the relevance and importance of quantum computing to businesses increasing. Here are the industries driving the quantum computing revolution:

- Technology
- Finance
- Healthcare
- Science
- Security
- Cybersecurity
- Artificial intelligence (AI)
- Business
- Cryptocurrency

Quantum computing has many applications, and represents an opportunity for huge advancements across a wide range of industries.

Quantum computing opens global doors for almost every company. For example: if a healthcare company is making a pill for COVID-19, they must analyze the medicine's impact on all relevant body cells. With quantum computers, scientists can analyze all the cells in the human body all at once, so they know what happens throughout your body when you take the Covid pill.



Quantum computing will also become a critical element in the business world, thanks to its ability to deliver real-time discoveries. By enabling problem-solvers to understand millions of situations simultaneously, quantum computers can uncover accurate findings at a rapid pace — meeting the modern-day demands for real-time business insights.

Because of hefty investment in quantum computing from governments and major organizations around the world, it is evolving with unprecedented speed.

The Impact of Quantum Computing on Cryptography

When commercial quantum computers hit the markets, they will have a transformative effect on digital activities across all sectors. However, for the disciplines that rely on intricate calculations and large volumes of data — including but not limited to finance and economic analysis, scientific and medical research, big data and AI — quantum computing will have a particularly massive impact by wildly improving upon current problem-solving capabilities.

But it's not all sunshine and rainbows in the quantum computing landscape. Unfortunately, many cybersecurity experts — including SSH — are concerned about the potential harm quantum computing could wreak on modern-day data security.

Thanks to its super-efficient algorithm processing power, quantum computing could be maliciously used to undermine modern cybersecurity practices and solutions. In 1994, MIT professor Peter Shor identified a quantum algorithm used for factoring integers. This algorithm is leveraged in public-key cryptography (also called prime factorization) for key generation.

The implication here is that a quantum computer running Shor's algorithm could potentially decrypt currently used asymmetric algorithms like RSA in a matter of days, if not mere hours. This will result in the encryption techniques that support most of the world's cryptography today becoming largely obsolete.

The most concerning element of this reality is not simply the cybersecurity implications, but also how rapidly the problem could potentially escalate. As soon as a quantum computer that is capable of hacking our current cryptography comes along, it will be able to break into everything — emails, credit cards, identification data, online banking information, and even other algorithms used in cybersecurity.

So, if you have a secret you want to remain a secret in 20 years, you need quantum resilience — and you need it today.

What is QSC?

QSC, which stands for quantum-safe cryptography, reflects the efforts currently underway to identify algorithms that can resist attacks by quantum computers.

Many modern popular cryptographic schemes — including RSA and Elliptic Curve Cryptology — rely on public-key cryptography. The mathematical algorithms used in public-key cryptography use entropy, which fosters randomness and a lack of predictability. Since classical computers are only effective at ascertaining patterns, public-key cryptography has been sufficient to secure important information.

However, in the quantum computing era, this entropy is unlikely to be sufficient. Because quantum computers can rapidly and efficiently understand patterns, they could easily break through the complex algorithms currently securing our critical data. This will render public-key cryptography obsolete. Not only does this have massive implications within the cybersecurity world, but for all organizations that hold sensitive and secured information.

Why Does QSC Matter?

However, in the quantum computing era, this entropy is unlikely to be sufficient. Because quantum computers can rapidly and efficiently understand patterns, they could easily break through the complex algorithms currently securing our critical data. This will render public-key cryptography obsolete. Not only does this have massive implications within the cybersecurity world, but for all organizations that hold sensitive and secured information.

In order to proactively combat quantum hacking, many organizations are currently developing QSC. One example of QSC is the Quantum Random Number Generators (QRNGs) that leverage “true randomness” by using quantum physics principles. Another example of QSC is Quantum Key Distribution (QKD), which uses a quantum principle called the “observer effect” to distribute keys in a way that guarantees forward secrecy.

The need for quantum-safe cryptography cannot be ignored. Current estimates point to a quantum computer capable of breaking our current cryptography coming along in the next few years. If correct, QSC will become a necessity in the near future — meaning we must take action now.

Quantum computers are not yet widely available, but it's only a matter of time until these powerful machines get into the wrong hands. The moment a quantum computer unlocks the algorithms behind our current cryptography, it will simply be too late to implement QSC.

Another reason why QSC is so urgent is due to the scale of change required for implementation. It has taken about 20 years for the public-key infrastructure (PKI) to exist at its present scale, and QSC implementation will likely be just as lengthy. Although it may only take 10 years to transition to QSC, it will likely take longer to reach a global scale.

Organizations simply don't have the time (nor the resources) to play QSC catch-up. That's why it's critical to take action now, as recommended by NIST.

QSC Isn't a Luxury; It's a Necessity

Without quantum-safe cryptography, every bit of information transmitted through PKI is vulnerable to malicious attacks — even data encrypted against today's most pertinent cybersecurity threats.

Once a quantum computer arrives on the scene that can unlock our current encryption algorithms, any compromised data will go undetected. Not only will this violate all current regulatory requirements for data security and privacy, but it will also make it impossible to guarantee the authenticity and integrity of shared information.

Organizations must be prepared for the age of quantum-safe cryptography. Enacting QSC immediately is the only way to ensure the continued protection of valuable, sensitive enterprise data.

Implement QSC Now

Gradual Migration From Classical Cryptography

In a way, upgrading encrypted connections with the latest algorithms is nothing new, since organizations should be doing it at regular intervals anyway. However, when a paradigm shift of this magnitude is looming on the horizon, it's a good idea to review your current state of cryptography and identify which sets of data have long-term value. You can then start protecting this data with quantum-safe algorithms first, while you are planning your next step. Gradual migration makes this big task more approachable and manageable.

This is also the perfect opportunity to upgrade any potentially obsolete classical encrypted connections of encryption keys in your environment, since classical and quantum-safe algorithms co-exist side by side through the transition period.

Although NIST is still standardizing the certified quantum-safe algorithms, software solutions like [SSH NQX™](#) are already prepared for the world of quantum computing.

NQX leverages quantum-safe cryptography by using key exchange support hardening, new authentication algorithms, and quantum-resilient encryption. This protects your critical data from quantum threats, even those that have not yet emerged. Along with using new encryption and algorithms, the Utility data plane on NQX uses non-scalable technologies to protect the platform from quantum threats.

NQX: Quantum-Proof and Future-Proof

NQX safeguards sensitive data from quantum threats using the most up-to-date key exchange and encryption techniques. In fact, Traficom — the National Cyber Security Authority (NCSA) at the Finnish Transport and Communications Agency — has certified NQX as a cryptographic product for protecting classified information, according to the Finnish national (FI) TL III (Confidential) security requirements.

In addition to its present protection capabilities, NQX is also a future-proof hybrid quantum threat solution. This is because the NQX software can quickly and efficiently be upgraded with the NIST standards once they have been finalized. NQX already has a commercially available PQC Edition with post-quantum cryptography (PQC) algorithms in place, enabling you to begin transitioning to PQC algorithms now — a feature not offered by many quantum cryptographic infrastructures.


As well as allowing for updates of quantum-safe protocols, NQX also leverages secure data routing and a variety of appliance portfolio models. This lets you meet strict security policies, regulatory mandates, and specific industry requirements.

NQX Benefits Begin Now

The time to implement QSC is here. Those who invest early will reap rewards down the line, as well as in the immediate future.

When you leverage a quantum-safe tool like NQX, you can prepare for the quantum threats of the future and improve your current security. Key length is longer, algorithms are more complex, and encryption is more powerful when using NQX – protecting data from the quantum threats of tomorrow and the most vicious cyberattacks of today.

Would you be prepared to leave your business-critical data unencrypted? Without quantum-safe cryptography, this may become your reality in the near future. So if you are skeptical about investing in quantum resilience, think of it as business insurance. Quantum-safe cryptography is vital protection against an inevitable future.



Learn more about SSH
NQX Quantum Encryptor
for data-in-transit.

We'd love to hear from you

Get in touch
with our experts
around the world.

GLOBAL HEADQUARTERS

Helsinki

SSH COMMUNICATIONS
SECURITY CORPORATION

Karvaamokuja 2b, Suite 600
FI-00380 Helsinki
Finland
+358 20 500 7000
info.fi@ssh.com

US HEADQUARTERS

New York City

SSH COMMUNICATIONS
SECURITY, INC.

434 W 33rd Street, Suite 842
New York, NY, 10001
USA
Tel: +1 212 319 3191
info.us@ssh.com

APAC HEADQUARTERS

Hong Kong

SSH COMMUNICATIONS
SECURITY LTD.

35/F Central Plaza
18 Harbour Road
Wan Chai
Hong Kong
+852 2593 1182
info.hk@ssh.com

Let's get to know each other

Want to find out more about how we safeguard mission-critical data in transit, in use, and at rest for leading organizations around the world?

We'd love to hear from you.

[Request a Demo](#)