International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Decoding the Quantum Code: Cyber Security in A Quantum Driven World

Ankita Paul

Cyber security Expert, Societe Generale

Abstract

Quantum computing represents a paradigm shift in computational power, leveraging the principles of quantum mechanics to solve complex problems that are currently unfeasible for classical computers. While this technology promises breakthroughs in various fields, it also poses significant challenges to the world of cyber security. This whitepaper explores the fundamentals of quantum computing, its potential impacts on cryptographic systems, and the strategies needed to safeguard digital infrastructures in the quantum era.

The Code

The computing that harnesses the principles of quantum mechanics to perform calculations at incredibly high speed is called quantum computing. Unlike classical computers using bits, quantum computing uses qubits. Qubits can represent both 0 and 1 simultaneously, exponentially increasing the potential computing power. Quantum computing has the potential to break encryption methods used today like RSA along with enabling new forms of quantum secure communication such as quantum key distribution.

The Wall

Cyber Security is the practice of protecting systems, networks, and data from digital damage. These damages are effects of attacks that threaten confidentiality, integrity, and availability of digital data.

Spotlight

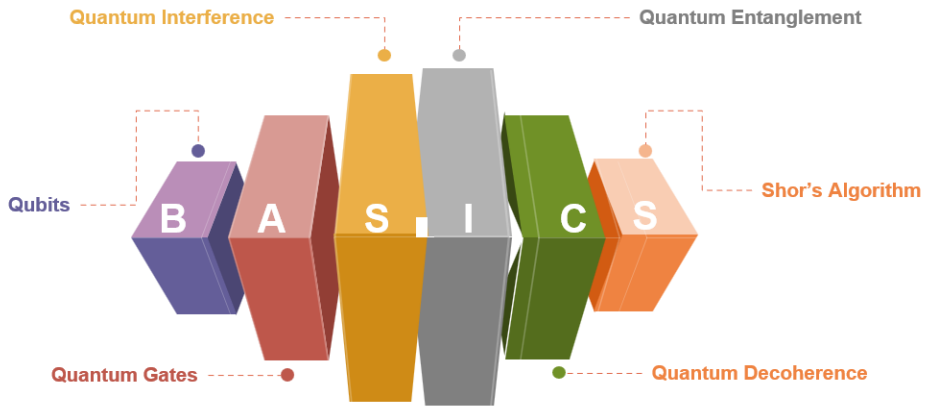
In the wake of Quantum computing, we now see that it poses both as a boon and bane for Cybersecurity. On one hand, it threatens to break existing encryption, but on the other, it provides the tools to build stronger, quantum-resistant security measures. The key for cybersecurity professionals and organizations is to act swift, adopt and leverage quantum advancements to stay ahead of cyber threats.

Getting the Fundamentals Right

The term *quantum* comes from the study of quantum mechanics, which is a field of physics that explores the physical properties of nature on a small atomic and subatomic scale. It is the foundation of quantum physics.

Quantum computers are the devices used to perform quantum computations. Quantum computers are based on **quantum superposition**. Superposition allows quantum objects to simultaneously exist in more than one state or location. This means that an object can be in two states at one time while remaining a single object. Quantum computers use the **entanglement** of qubits and superposition probabilities to

perform operations. These operations can be manipulated so that certain probabilities are increased or decreased, which leads us to the correct and incorrect answers we're looking for.



A quantum bit, or **qubit,** can represent zero, one, or both at the same time. It is the **basic unit of quantum information**, and it is the smallest possible unit of digital information.

Quantum gates are basic quantum circuits that operate on a small number of qubits. Quantum circuits consist of a combination of multiple quantum gates applied on some qubits.

Quantum interference is a byproduct of superposition. It permits us to **bias the measurement** of a qubit toward a desired state or set of states. Hence, quantum interference allows us to affect the state of a qubit to influence the probability of the **desired outcome**.

Quantum entanglement permits two or more quantum particles to become entangled. When these particles get entangled, they become a **single system**. Quantum entanglement provides qubits more computing power as it adds more qubits to a system.

When we try to observe or measure quantum particles, it can collapse the superposition state. This is called **decoherence**. Quantum decoherence leads to errors in quantum computational systems.

Shor's Algorithm is an algorithm vastly used in quantum computing to find the prime factor of a large number.

If we have N=pq where p and q are both prime.

Shor's algorithm helps us to find both p and q given N.

This is the backbone of RSA which is a widely used encryption mechanism. It is the backbone that quantum mechanics allows factorization to be performed in polynomial time rather than exponential time which impacts the field of data security as it is a concept based on prime factorization of large numbers.

Potential of Quantum Computing:

Quantum computing offers the possibility of major breakthroughs across sectors & Investors agree to these possibilities. McKinsey mentions that the Quantum computing market could grow by $80 billion by 2035 or 2040. It has the potential to transform many industries which would encourage optimizing investment strategies, encryption and discovering new products. Quantum computers too have marked a milestone which portrays that it can solve complicated problems ten times faster than classical computers.

Quantum computing's cornerstone mark was across the news in the last few years — from Google's 53-qubit quantum computer "Sycamore" achieving what has been coined quantum supremacy to multibillion-dollar initiatives around the world to develop quantum technologies for computing and beyond.

QC can be tailored to address the Optimal route planning for logistics and transportation as it can process

data in real time and adjust routes for an entire fleet of vehicles at once, putting each on the optimal path forward.

In the manufacturing space, Quantum computers can run more accurate and realistic prototyping and testing, reducing the cost of prototyping and resulting in better designs that don't need as much testing.

Organizations today use AI and ML to discover ways to automate and optimize tasks. When used in combination with quantum computing, optimization can happen much faster and at scale, especially when processing and analysing highly complex or even unstructured big data sets.

In the Financial sector, QC has the potential to optimize financial modelling, risk assessment, and fraud detection, thus contributing to the stability and security of financial systems. Additionally, QC can enhance cybersecurity measures to protect financial transactions and data encrypted while in use, providing both in-transit and at-rest protections.

Finally, when it comes to tech, data centres should focus on further digital transformation. Continue building out digital infrastructure and scaling data sets with an eye toward eventually transitioning to or adopting quantum computing workflows in some capacity. When it's feasible to invest in the hardware and expertise needed, organizations can then get quantum computing up and running sooner rather than later.

Code threatening the wall!

Digital data is widely secured by encryption which is a process of converting data into unreadable code using an algorithm and key. Common encryption standards consist of:

- **AES (Advanced Encryption Standard)** - A symmetric encryption standard that comes in key sizes of 128, 192, and 256 bits is commonly used for securing data in transit/at rest.
- **RSA (Rivest-Shamir-Adleman)** - An asymmetric encryption algorithm used primarily for securing data transmission which relies on the mathematical difficulty of factoring large prime numbers.
- **ECC (Elliptic Curve Cryptography)** - Another asymmetric encryption method that offers similar security to RSA but with smaller key sizes, making it more efficient.
- **TLS (Transport Layer Security)** - A protocol that uses various encryption algorithms (including AES and RSA) to secure communications over networks, such as the internet.

All these encryption standards were designed without the consideration of quantum computing and its potential. Quantum computing has the potential to break RSA,AES and ECC encryption within hours or even minutes depending on the size and power of the quantum computer.

Two recent announcements have raised concerns about quantum computing RSA encryption. One is from a team of Chinese researchers, who published a paper on ArXiv in December 2022. They claim to have found a faster way to break RSA encryption with a quantum computer of 372 qubits.

The other announcement is from a researcher named Ed Gerck, who posted on LinkedIn in November 2023. He claims to have decrypted RSA-2048 encryption, the most used public-key algorithm, with a quantum system implementable on a smartphone or a PC running Linux. He mentioned that he developed a quantum algorithm that can calculate prime numbers faster than Shor's algorithm. He published an excerpt of his work however didn't provide any proof or detail of his method. Both announcements are not verified and have been met with scepticism and doubt from the experts as they have neither provided any evidence nor peer-reviewed by other sources.

Let us understand in depth how Quantum computing poses significant challenges & opportunities for secure communications, digital signatures, and authentication mechanisms due to its ability to solve maths

faster than classical computers.

In Secure Communication

Quantum computers can efficiently solve problems like integer factorization (using Shor's algorithm) and discrete logarithms, which form the basis of widely used encryption schemes like RSA, ECC, and Diffie-Hellman.

However, the emergence of quantum computers has driven the development of quantum-resistant algorithms designed to be secure against quantum attacks. These algorithms are such as:

- **Lattice-based cryptography**: This is based on the hardness of finding the shortest vector in a high-dimensional lattice, or the closest vector to a given point. Lattice-based cryptography has the advantage of being fast, versatile, and allowing for advanced features such as homomorphic encryption and digital signatures.
- **Code-based cryptography**: This is based on the hardness of decoding a general linear code or finding the error vector in a noisy transmission. Code-based cryptography has the advantage of being simple, efficient, and having a long history of security analysis.
- **Multivariate cryptography**: This is based on the hardness of solving a system of multivariate polynomial equations over a finite field. Multivariate cryptography has the advantage of being compact, flexible, and allowing for various applications such as encryption, signatures, and identification.
- **Hash-based cryptography**: This is based on the hardness of finding collisions or preimages for a cryptographic hash function. Hash-based cryptography has the advantage of being simple, provably secure, and relying on minimal assumptions.

In Digital Signatures & Authentication Mechanism

Many current digital signature schemes, like RSA and ECDSA, rely on problems vulnerable to quantum attacks. Similarly, authentication mechanisms relying on shared secrets or asymmetric cryptography could be compromised as a sufficiently powerful quantum computer could forge signatures, undermining their integrity and authenticity and can derive private keys from public information.

Research is underway to develop quantum-safe digital signature schemes, such as those based on lattice problems (e.g., Dilithium) or hash-based methods (e.g., SPHINCS+). These provide alternatives to maintain the security of digital signatures in a post-quantum era. Quantum computing also has the potential to enable the creation of highly secure authentication tokens, leveraging the principles of quantum entanglement and superposition to prevent cloning or forgery.

While organizations transition to post-quantum cryptographic systems, which may take years; hybrid systems that combine classical and post-quantum algorithms can be used to mitigate risks.

Efforts like NIST's (National Institute of Standards and Technology) Post-Quantum Cryptography Standardization are key to creating widely accepted and secure cryptographic standards for the future to protect against potential quantum computer cyber-attacks. These standards are the result of an eight-year effort, including algorithms designed to secure digital communications and signatures. NIST urges system administrators to begin transitioning to these new standards immediately to safeguard electronic information as quantum computing technology evolves. Further algorithms are still being evaluated as potential future backups, according to a document published by NIST.

The new algorithms are:

FIPS 203: specifies the module-lattice-based key-encapsulation mechanism standard, derived from crypt-

graphic suite for algebraic lattices (CRYSTALS)-Kyber, for establishing a shared secret key between two parties over a public channel.

FIPS 204: defines the module-lattice-based digital signature standard, derived from CRYSTALS-Dilithium, for detecting unauthorized data modifications and authenticating the signatory's identity.

FIPS 205: specifies the stateless hash-based digital signature standard, derived from SPHINCS+, designed for robust digital signatures without state retention.

The move will also require updates like Java 21+, which is essential for managing quantum-safe encryption keys.

The Ticking Time Bomb:

QC is expected to meet the end of several types of conventional cryptography used widely in billions of devices and over 80% of communications over the global internet.

Criminals and state actors show an understanding of this importance as they have recently demonstrated attack scenarios such as "harvest now, decrypt later." In these attacks, encrypted data is stored after exfiltration, with the expectation of being able to decrypt these stolen secrets, data and other sensitive information in the future when decryption by a quantum computer becomes more approachable.

Y2Q (also sometimes called Q-Day) is the date when quantum computers will defeat public-key cryptography. According to the 2021 Quantum Threat Timeline Report (January 2022), cybersecurity experts appear to be confident that quantum computers will be able to break RSA-2048 within 15 years. The Cloud Security Alliance (CSA) is more pessimistic – they estimate that Y2Q will arrive on April 14, 2030.

Truth be told – no one can tell when Y2Q will come. However, certain factors incline us to believe that the quantum threat will become a reality much sooner than many might be thinking.

One of the difficulties of predicting the date of Y2Q is that technology often doesn't develop linearly – it develops in "fits and starts" including sudden periods of exponential growth. This extends to quantum computing as well. While we can look back at how fast quantum computers have developed so far and extrapolate our observations into the future, we also need to factor in the unexpected (but highly anticipated) leaps in technology and innovative approaches that will exponentially accelerate progress in quantum computing achievements.

At the highest level, the global investment of billions of dollars annually in quantum research is why Y2Q will likely be here sooner than later. This leads us to go a little bit deeper and give more specific reasons as to why Y2Q is getting very close, very fast.

The recent advancements in QC might shorten the time left until Y2Q. However, tech developments aren't the only reason to start thinking about upgrading to quantum-safe protection. Even if we completely disregard research into quantum computing, there are reasons why switching to quantum-secure data protection soon is a very good idea.

Any recent data compromised is likely to be sitting in some hacker group's data center right now, waiting to be cracked. Every piece of data that's been stolen over the years is a ticking time bomb. When that bomb blows up – that is, when hackers get access to quantum computers –business secrets will no longer be secret. Proprietary source code, financial records, client information name it any- hackers will be able to access it all.

Although we don't know for sure if hackers are indeed following the "steal now, crack later" strategy, it would be safe to assume that they do. We should think about the worst-case scenarios to be able to protect ourselves from future threats. So, if we have data that needs to be retained and protected for 10 or 20 years, we should start thinking about quantum-secure protection right now.

The transition to quantum-proof IT infrastructure might take months to years, depending on the scope of the changes. The move to quantum-proof cryptography is a multi-step process. It incorporates understanding current cryptographic tools, identifying most vulnerable and valuable assets, and updating cryptographic policies to include quantum-proof measures. To decide which enterprise quantum-safe solution to use, it may require months of consultations with different vendors.

Post these steps the actual deployment of quantum-secure cryptography would kickstart. Followed by awareness campaigns among staff to update cryptography tools and the new cybersecurity policies. Do we have time to make this enormous transition till we are hit by Y2Q? We aren't sure enough.

Post quantum cryptography provides data protection that is resistant to QC decryption risks. However, switching cryptography methods in existing architectures is not an easy task, as it won't be drop-in replacements for existing asymmetric algorithms.

However, Cryptographic agility (capability to transparently swap out encryption algorithms in an application, replacing them with newer, presumably safer, algorithms) is the way to address cybersecurity challenges in the long run. Cutting-edge technology to protect data today along with a proactive plan on adapting to new cybersecurity policies would be a great start today.

A consistent approach is needed, because, given past and future developments in cryptography, this will not be the last time we have to switch encryption methods. Additionally, new algorithms have different performance characteristics from non-PQC ones. For example, key and ciphertext sizes are larger, and encryption and decryption times are longer, which may impact performance. This means current applications must be retested and, in some cases, rewritten.

For better management of change consider:

- Developing policies that ease the transition to new algorithms. It will reduce confusion and arbitrary choices and increase manageability.
- Build a cryptographic metadata database of all in-use cryptographic algorithms. It would ease identifying the expected end-of-life targets in the short-, mid- and long-term time scales.
- Implement crypto-agile application development and move to production after extensive testing.
- Upgrade or replace hardware where necessary.

An Amulet called QKD.

Quantum Key Distribution (QKD) provides theoretically unbreakable encryption by leveraging the principles of quantum mechanics, specifically the phenomena of superposition and entanglement. In QKD, two parties exchange cryptographic keys using quantum bits (qubits). If an eavesdropper attempts to intercept or measure these qubits, the act of measurement alters the state of the qubits, revealing their presence. The security of QKD arises from the fact that any attempt to observe or interfere with the quantum states will introduce detectable anomalies, allowing the communicating parties to identify and discard compromised keys, ensuring that only a secure key is used for encryption. Thus, the fundamental laws of quantum physics will safeguard the transmission of secure keys against any potential attacks.

Call for action.

This year, the United Nations proclaimed 2025 as the International Year of Quantum Science and Technology, and the U.S. Department of Commerce's National Institute of Standards and Technology announced its post-quantum cryptographic standards designed to withstand quantum computing cyberattacks, indicating the threat may be around the corner. Tom Patterson, quantum security lead at Accenture, predicts that boards will become increasingly vocal about their desire for quantum preparedness. Organizations should begin by assessing their current cryptographic protocols to identify vulnerabilities to quantum threats. They should then prioritize the adoption of post-quantum cryptography (PQC) standards, which involves selecting algorithms that are resistant to quantum attacks, and gradually integrating them into their systems. Regular training and awareness programs must be implemented to educate staff on secure communication practices. Additionally, organizations should invest in testing and validating their new cryptographic systems to ensure compatibility with existing infrastructure. Finally, maintaining agility in updating security measures as PQC standards evolve will be essential to staying ahead of emerging quantum threats.

Regulatory bodies play a crucial role in ensuring the adoption of quantum-resistant standards by establishing guidelines and frameworks that advocate for the integration of post-quantum cryptography (PQC) into existing security protocols. They can facilitate collaboration among stakeholders, including governments, industry leaders, and academic researchers, to identify best practices and promote research and development in quantum-resistant technologies. By setting compliance requirements and industry benchmarks, regulatory entities can motivate organizations to transition to PQC, thereby mitigating the risks posed by quantum computing threats. Moreover, they can also provide resources and incentives for organizations to upgrade their systems, and periodically review and update the standards to keep pace with advancements in quantum technology. Ultimately, regulatory bodies serve as critical architects in the evolution of a secure digital landscape capable of resisting future quantum-based attacks.

The Path Ahead

The timeline for quantum computers becoming mainstream is a subject of considerable debate among experts, with projections varying widely. In the near term, within the next decade, we can expect significant advancements in quantum technology, including the development of more reliable and powerful quantum processors. According to a survey by Gartner, 60% of companies will adopt quantum-resistant algorithms by 2030. Companies like IBM, Google, and startups in the quantum computing space are making strides toward achieving quantum advantage for specific applications, such as optimization challenges and materials science. However, achieving a threshold where quantum computers are widely adopted for general-purpose use could take an additional 10 years. This longer timeline accounts for the need for robust error correction, scalable architectures, and the establishment of practical applications that outperform classical computers in fields like cryptography and complex system modelling. As research progresses and investment continues to grow, a clearer picture of quantum computing's role in the technology landscape will emerge, likely leading to a more integrated use of quantum systems alongside traditional computing in the coming decades.

To future-proof cyber systems against the evolving threat landscape posed by quantum computing, organizations need to consider a dual investment strategy that accentuates both quantum computing and post-quantum cryptography (PQC).

Big players industry wide should take on the path of leaders like IBM, Google, Rigetti Computing, and

D-Wave, which are pioneering developments in quantum processors and quantum algorithms. Startups can consider innovating in specific applications, like pharmaceuticals and materials science, as well as partnerships with academic institutions that are conducting cutting-edge research in quantum technologies.

Additionally, it gets crucial to prioritize investments in firms specializing in encryption solutions designed to be robust against quantum attacks. Already a few of the companies are actively working on implementing NIST's PQC standards, which are expected to lead the way in securing data. Organizations such as Thales and Micro Focus already offer solutions in this space. Furthermore, organizations can consider investing in cybersecurity firms that are proactively adapting their offerings to include PQC solutions.

By diversifying investments across these critical areas, businesses can enhance their resilience against both current cybersecurity threats and future risks associated with quantum computing advancements.

It too gets extremely crucial to collaborate between government, industry, and academia to effectively combat the quantum cyber threat, as each sector fetches unique strengths and resources to the table. Governments can provide regulatory frameworks, funding, and strategic guidance to prioritize national security and foster innovation. Industry players, including tech companies and cybersecurity firms, can drive the development and deployment of quantum-resistant technologies and practices, leveraging their expertise in practical applications. Academia plays a critical role in advancing research and education in quantum computing and cryptography, producing the next generation of experts, and fostering a collaborative environment for knowledge sharing. By joining forces, these sectors can create an all-inclusive approach to understand and mitigate the risks posed by quantum technologies, ensuring that robust, scalable solutions are developed and implemented effectively across society. This tripartite partnership is vital for keeping ahead of adversaries and protecting critical infrastructure, sensitive data, and overall cybersecurity.

The Bottom Line

Quantum Computing is set to grow quickly in 2025 and beyond, changing fields such as healthcare, finance, and security. While there are still challenges, like ensuring the technology is stable and scalable, quantum computing has the potential to change the way of tackling complex problems. With ongoing research and innovation, the quantum computing future scope looks promising. The Impact of Quantum computing on CyberSecurity has its both pros and cons. As it threatens to break existing encryption it too provides the tools to build stronger, quantum-resistant security measures. Even Q-Day looks to be a tentative entry in the calendar, we just don’t know when the clock will strike midnight. Acknowledging that potential is the first step to securing the future & the key for cybersecurity professionals and organizations is to act quickly, adopting post-quantum cryptography and leveraging quantum advancements to stay ahead of cyber threats.

References

1. Erin Schaffer. August 19, 2021. Intro to quantum computing: Qubits, superposition, & more. https://www.educative.io/
2. Erica Vartanian. April 29, 2022. Approaching quantum computing basics, bit by qubit. https://www.educative.io/
3. Margaret Rouse. March 14, 2017. Quantum key Distribution. https://www.technopedia.com/

4. Maria Webb. June 27, 2024. Quantum Computing Investment Boom: Funding Driving Breakthroughs. https://www.technopedia.com/
5. Ray Fernandez. June 12, 2024.The Era of Commercial Quantum Computing Has Begun. https://www.technopedia.com/
6. Sam Cooling. August 7, 2023. Quantum Resistance. https://www.technopedia.com/
7. Margaret Rouse. September 25, 2019. Quantum Decoherence. https://www.technopedia.com/
8. Claudio Buttice. February 18, 2020. Quantum Cryptography Vs. Quantum Hacking: A Cat and Mouse Game. https://www.technopedia.com/
9. Linda Rosencrance. November 19, 2024. Future of Quantum Computing: Predictions for 2025 & beyond. https://www.technopedia.com/
10. July 19, 2022. Quantum Cryptography - Shor's Algorithm Explained. https://www.classiq.io/
11. Quantum Key Distribution (QKD) and Quantum Cryptography (QC). https://www.nsa.gov/Cybersecurity/
12. June 25, 2022. How quantum computing could change the world. https://www.mckinsey.com/featured-insights/themes
13. Bernice Chan. March 12, 2024. What Are the Opportunities Presented by Quantum Computing. https://viterbischool.usc.edu/news/2024/03/
14. October 18, 2024. Quantum Computing - How it Changes Encryption as We Know It. https://it.umd.edu/news/
15. Mullamuri B 2021 ProQuest Dissertations Publishing Enabling Quantum Cryptography Using Quantum Computer Programming p 28864879.
16. Chuang DG 2001 Quantum digital signatures.
17. Delpech De Saint Guilhem and Cyprien P. R. 2021 University of Bristol (United Kingdom) ProQuest Dissertations Publishing On the Theory and Design of Post-Quantum Authenticated Key-Exchange, Encryption, and Signatures.
18. TangLi X, Hu X, Wang R and Zeng XY 2021 IEEE Access A New Post-Quantum Digital Signature Scheme Based on Binary Goppa Codes pp 164530-164543.
19. Yu Y 2021 National Science Review Preface to special topic on lattice-based cryptography vol 8.
20. Li B, Xie Y, Cao X, Li C, Fu Y, Yin H and Chen Z 2023 Quantum Physics (quant-ph.) Cryptography and Security One-Time Universal Hashing Quantum Digital Signatures without Perfect Keys.