SCHOLARLY DEBUT
by Scholarly Review

Fall 2025

Cryptography & Quantum Computing: Why it matters and what comes next?

By Kanav Manoj Mohan

AUTHOR BIO

Kanav Manoj Mohan is a Grade 12 student at Delhi World Public School, Navi Mumbai (India). He has interests in computer science, quantum technologies and physics. His earlier paper, "Decoding Bennu: Understanding the Solar System and Life's Origins," was featured in the Scholarly Review Online Showcase - Equinox 2024 Issue. He hopes to study computer science and quantum computing as well as conduct more projects in these fields in the future.

ABSTRACT

In today's digital world, most of our personal, financial, and health data is stored online. This makes cybersecurity extremely important — but also more challenging. Recent cyberattacks like the one on Australia's MediSecure show how weak security can lead to huge losses. Now, a new risk is emerging: quantum computers. These work very differently from classical computers and can break the encryption methods (like RSA and AES) that we currently use to protect online data. This paper explains how cryptography works, what types exist (symmetric and asymmetric), and why current systems may not survive in a world where quantum computers are common. It introduces powerful quantum algorithms like Shor's and Grover's, which can break RSA and weaken AES much faster using quantum computers than any normal computers. This shows the power of quantum computers. These developments have pushed scientists to create new encryption systems called Post-Quantum Cryptography (PQC), which are built to resist quantum attacks but still run on regular devices. The paper also explores how quantum computing is evolving — from early research in the 1980s to real working processors today — and how countries and companies are investing in this technology. It suggests that in the future, people may access quantum computers over the cloud, rather than owning them. Finally, this research shows that the rise of quantum computing is both a threat and an opportunity. It challenges us to update our security systems, but it also opens the door for new startups and careers in quantum-safe cybersecurity.

Keywords: *Quantum Computing, Cryptography, Post-Quantum Cryptography (PQC), Shor's Algorithm, Grover's Algorithm, RSA Encryption, Quantum Cloud Access, Rose's Law, Cybersecurity Transition, Digital Trust, Quantum-Safe Innovation, Future of Encryption*

SCHOLARLY DEBUT
by Scholarly Review
Fall 2025

INTRODUCTION: WHY WE NEED TO RETHINK CYBERSECURITY

In today's world, most of our information — personal, medical, financial — is stored online. While this has made our lives more connected and efficient, it has also increased the risk of serious data breaches. In 2024, Australia's prescription platform MediSecure was hacked, exposing the private medical records of nearly 13 million people. The breach was so massive that the company had to shut down permanently. Something similar happened to Code Spaces, a code hosting and software development collaboration platform, in 2014. After attackers gained access to its Amazon Web Services control panel, they deleted customer data along with all backups. Unable to recover, the company was forced to close operations entirely (Tozzi, 2025).

These cases show how even a single weak link in cybersecurity can destroy a company. But there's another big concern on the horizon: quantum computers. These powerful machines could eventually break the encryption systems that protect the internet today. Our current encryption methods, like RSA (Rivest-Shamir-Adleman) and AES (Advanced Encryption Standard), are not strong enough against the kind of computing power quantum machines promise to deliver. That's why scientists around the world are now working on Post-Quantum Cryptography (PQC) - new encryption techniques that are designed to stay secure even when quantum computers become common.

This paper explores how quantum computers could change the way we think about cybersecurity, and why post-quantum cryptography could become essential to protect data in the near future.

LITERATURE REVIEW

Cryptography: Keeping Our Data Safe

In today's world, we share and store a lot of personal data online—whether it's sending messages, making payments, or using apps. To keep this data safe from hackers or unauthorized access, we use something called *cryptography*. Simply put, cryptography is a way of hiding information using special mathematical techniques so that only the right person can read it.

Every time you see a lock icon next to a website address or use apps like WhatsApp that say "end-to-end encrypted," you're actually using cryptography, even if you don't realize it. The process of turning normal text into a secret code is called *encryption*, and the process of turning it back into readable text is called *decryption*.

This technique works using specific rules called *algorithms*, which mix up the data in such a way that only someone with the right key can understand it. Without the right key or algorithm, the data looks like complete gibberish. This helps ensure that private messages, passwords, and other sensitive data don't fall into the wrong hands (Qadir & Varol, 2019).

Goals of Cryptography

Cryptography helps achieve some important goals in data protection:

1. Authentication - Making sure the person accessing the data is actually who they say they are.
2. Confidentiality - Only people with the correct key can read the message.

3. Data Integrity - Making sure the message hasn't been changed or modified.
4. Non-Repudiation - Proving that both the sender and the receiver were part of the communication.
5. Access Control - Making sure only authorized people can view or decrypt the message (Abood, O. G., & Guirguis, S. K., 2018).

Types of Cryptography

There are two main types of cryptography used to keep digital data safe: symmetric and asymmetric.

Symmetric Cryptography

In symmetric cryptography, the same key is used to both lock and unlock the data. Imagine if Alice and Bob both had the same secret password. Alice uses this password to turn her message into a code (encryption), and Bob uses the same password to decode it (decryption). The most well-known technique that uses this method is AES.

The tricky part is that the password (key) needs to stay secret. If anyone else finds it out, the whole system falls apart. And that's why symmetric cryptography can be hard to use safely on the internet—because we need a secure way to share the secret key (Mavroeidis et al., 2018).

Asymmetric Cryptography

To fix the problem of sharing secret keys, asymmetric cryptography (also called public-key cryptography) was invented. Here, each person has two keys: one public and one private.

Let's say Bob wants to send Alice a secret message. Alice gives Bob her public key. Bob then encrypts the message using Alice's public key (accessible to all but can only encrypt the message) and sends it to her. Once Alice gets the message, she uses her private key (which only she knows) to decrypt it.

The most common asymmetric methods are RSA and Elliptic Curve Cryptography (ECC). These cryptographic systems have worked well until now. But a new kind of computing, quantum computing, is starting to challenge them (Mavroeidis et al., 2018).

Quantum Computing: A Threat to Cryptography

In the early 1980s, physicist Richard Feynman suggested the idea of a quantum computer: a machine that could use the principles of quantum mechanics to perform powerful calculations (Lloyd, 1996). Unlike regular computers that use bits (which are either 0 or 1), quantum computers use qubits, which can be both 0 and 1 at the same time. This is called superposition.

Quantum computers also use a unique principle called entanglement, where two qubits become linked. If you change one, the other changes instantly—no matter how far apart these particles are. This gives quantum computers the power to perform many calculations at once, making them super-fast at solving certain problems.

This power of quantum computers can be used to break cryptographic techniques in use today. If someone wants to break AES encryption using a regular computer - they would have to try every possible combination one by one (called brute force). With long key sizes, this can take thousands of years (Fossen-Helle, 2020).

But quantum computers can use special algorithms (like Shor's and Grover's) to crack certain types of encryption much faster. The classical computers that we have today cannot execute these special algorithms. But quantum computers can. This makes quantum computers very dangerous for breaking encryption, especially asymmetric encryption methods like RSA, used for secure messaging, banking, and software updates.

So, while quantum computers are still developing, their future potential already poses a serious risk to current encryption methods (Mavroeidis et al., 2018).

Quantum Algorithms: A New Threat to Current Encryption

Quantum computers are expected to bring a huge shift in the way we think about encryption. In fact, the U.S. National Institute of Standards and Technology (NIST) has stated that quantum computers could eventually break today's most widely used encryption methods - especially the ones based on public key cryptography (Chen et al., 2016). This isn't just theory. There are already two powerful quantum algorithms that show how this could happen: Shor's Algorithm, which can crack RSA encryption as well as ECC and Grover's Algorithm, which can weaken symmetric encryption like AES. These two algorithms show us why quantum computers could be a major threat to current cryptographic techniques.

Shor's Algorithm: Cracking RSA with Quantum Power

One of the biggest breakthroughs in quantum computing came in 1994, when mathematician Peter Shor showed that a quantum computer could factor large numbers way faster than any classical computer. His algorithm, now known as Shor's Algorithm, changed the way people looked at cryptography forever (Shor, 1994).

To understand why this is important, think about RSA encryption. It's a popular way of securing data, and its strength comes from the fact that it's really hard to break large numbers that are a product of two big prime numbers. If you can't break those numbers, you can't crack the code. Classical computers take a very long time to do this—sometimes even centuries!

Shor's algorithm changes that. It uses quantum computers to find something called a "period" in a special kind of function. Once that period is found, it becomes much easier to break the large number into its prime factors. The trick is that quantum computers can check many values at the same time using a property called superposition, and then apply something called the Quantum Fourier Transform to find the period very quickly. This means a quantum computer can break RSA encryption in just hours, making it unsafe in a post-quantum world.

To go one level deeper to understand how Shor's algorithm works: we find a number 'a' < N, such that gcd(a,N) =1 or 'a' and N are coprime. Then we find the smallest positive integer r such that $a^r \equiv 1 \pmod{N}$. If r is odd, we must find another number 'a'. If r is even, we can proceed to find the factors given by $\gcd(a^{r/2} - 1,N)$ and $\gcd(a^{r/2} + 1,N)$. These factors may be 1 and N itself if $a^{r/2} \equiv -1 \pmod{N}$, though these cases are rare. In such cases, we try a different number 'a'. Quantum computers come into the picture as classical computers take a lot of time to calculate 'r' if N is sufficiently big. For the periodic function $f(x)=a^x \bmod N$, where x is a whole number and gcd(a,N)=1, we need to find the least positive period 'r' such that f(x) = f(x+r). After evaluating the function over all 'x'

simultaneously using superposition, the Quantum Fourier Transform(QFT) is applied to find 'r'. The time taken by quantum computers to find 'r' increases polynomially with respect to log N, giving it the ability to crack RSA much faster than classical computers, which take exponentially (non-polynomial time) longer. Once we are able to factorise N into two primes, we can use these numbers to easily decipher the private key and break RSA.

Grover's Algorithm: Breaking Symmetric Encryption Faster

While Shor's algorithm helps break asymmetric encryption like RSA, Grover's algorithm, invented by Lov Grover in 1996, focuses on symmetric encryption like AES. Normally, if you're trying to crack a password or encryption key using brute force, a classical computer would have to try every possible combination one by one. If there are P possibilities, on average it would need to go through about P/2 tries to get the right one.

Quantum computers, however, can do this much faster thanks to Grover's algorithm. Instead of checking each option one at a time, quantum computers use superposition to represent all possible answers at once. Then, using quantum interference, they increase the chances of measuring the correct answer. This reduces the number of tries to just about √P. For example, to guess the right key from 100,000 possible options, a classical computer would need around 50,000 tries but a quantum computer using Grover's algorithm might only need around 316 tries (Grover, 1996).

This is why Grover's algorithm matters for symmetric encryption like AES. AES-128, which uses a 128-bit key, is still very secure against classical computers but quantum computers using Grover's algorithm can break it much faster. On the other hand, AES-256, which uses a 256-bit key, is considered safe even in a post-quantum world. It would take a quantum computer trillions of years to crack AES-256 using Grover's method, so it's still a strong choice.

Quantum Computers: Past, Present and the Future

Past (1980 to 2010)

The idea of quantum computing goes back to the 1980s, when physicist Richard Feynman suggested that regular (classical) computers might not be good enough to simulate complex quantum systems. This led to the search for a new kind of computer that used the principles of quantum mechanics. In 1985, David Deutsch introduced the concept of a "universal quantum computer," showing how quantum computers could solve certain problems much faster than classical ones by doing many calculations at once, something called quantum parallelism.

Important breakthroughs followed. As mentioned earlier, in 1994, Peter Shor developed an algorithm that could quickly factor large numbers, threatening the RSA encryption we use today. Two years later, in 1996, Lov Grover came up with another algorithm that could search through unsorted data much faster, challenging the security of symmetric encryption systems like AES.

Also in 1996, physicist Seth Lloyd proved that quantum computers could accurately simulate quantum systems, a key moment that confirmed Feynman's early idea (Lloyd, 1996). By 2000, researchers Edward Farhi and his team at MIT introduced a new type of quantum computing called adiabatic quantum computing. This approach solved optimization problems by slowly evolving a quantum system into its lowest-energy state (Farhi et al., 2000). In 2001,

IBM and Stanford demonstrated the first working version of Shor's algorithm by factoring the number 15 using a 7-qubit quantum processor.

Present (2010 to 2025)

Since 2010, progress in quantum computing has moved from labs to commercial systems. D-Wave Systems launched the first commercial quantum computer based on adiabatic methods, using 128 qubits. In 2016, IBM introduced "IBM Quantum Experience," the world's first cloud-based quantum computer. This allowed users from anywhere to run quantum experiments on a 5-qubit processor, sparking global interest in quantum computing.

A major milestone came in 2019 when Google's Sycamore processor (with 54 qubits) claimed quantum supremacy, completing a task in 200 seconds that would take a classical supercomputer thousands of years. Recent advances show that companies are getting better at dealing with errors and building more stable quantum systems. For instance, Google's Willow (2024) reached 105 qubits and demonstrated better error correction, while Microsoft's Majorana 1 (2025) used a special kind of qubit called a topological qubit, designed to resist errors.

Future: What Lies Ahead?

Although quantum computing is making big strides, many challenges remain. One major issue is errors and stability. Qubits are sensitive and can be easily disturbed by heat or noise, leading to calculation errors. Another limitation is coherence time, since qubits can only hold their quantum state for a short time (milliseconds or less). Finally, there is the challenge of scalability; cracking strong encryption may require thousands of error-free qubits, something we haven't achieved yet.

Despite these hurdles, companies like IBM, Google, and Quantinuum are investing billions to build better systems. A prediction known as Rose's Law (like Moore's Law for classical chips) suggests the number of qubits doubles roughly every 18 months. If this trend holds, quantum computers could soon reach the scale needed for real-world impact. Some recent forecasts highlight the pace of this progress. IBM expects to develop over 1,000 logical qubits (error-corrected and reliable qubits) by 2029, while Quantinuum aims to build a 100-logical-qubit system by 2027. Governments are also joining in. For example, the UK government recently pledged over £500 million to advance quantum technologies.

A REVIEW OF POST-QUANTUM CRYPTOGRAPHY

Most modern encryption works on a two-part model: asymmetric encryption (like RSA) is used at the start of communication to securely exchange keys, and symmetric encryption (like AES) handles the actual data transfer. This setup works well in a classical computing world, but quantum computers threaten to break it.

For example, RSA (the most widely used public key cryptosystem today) can be fully cracked using Shor's algorithm, which factors large numbers in polynomial time. This makes RSA unsafe once quantum computers scale up. Similarly, AES-128, a symmetric encryption method, becomes vulnerable to Grover's algorithm, which effectively cuts its security in half. That's why AES-256 (which has a much larger key size) is still considered quantum-safe, though it's slower and harder to implement.

The key vulnerability lies not in how we encrypt data, but in how we start the conversation. If the initial handshake, usually

done using RSA or ECC, is broken by a quantum computer, then even the strongest symmetric encryption offers no protection. The encrypted data could be recorded now and decrypted later.

To address this, researchers have developed PQC. These algorithms are designed to be secure even against quantum attacks, but importantly, they run on classical computers. NIST (National Institute of Standards and Technology) is leading the charge in selecting and standardizing these new techniques (NIST, 2017).

Some key categories of PQC include:

- Lattice-Based Cryptography: These algorithms rely on extremely hard math problems based on multi-dimensional grids called lattices. Examples include Kyber (for secure key exchange) and Dilithium (for digital signatures). These two have been selected by NIST as part of its new cryptographic standards.
- Code-Based Cryptography: This technique uses ideas from error-correcting codes. The best-known example is Classic McEliece, which has been around for decades and is still considered highly secure, though it uses very long keys.
- Hash-Based Cryptography: Built around cryptographic hash functions, this type is especially good for digital signatures. A prominent example is SPHINCS+, which is useful in situations where keys are reused frequently.

Together, these new approaches are the foundation of future-proof security. They will eventually replace older systems like RSA and ECC to ensure that the digital world stays safe, even in the quantum era (NIST, 2017).

DISCUSSION & FORECASTING: CRYPTOGRAPHY AT A CROSSROADS

When Will Quantum Computing Go Mainstream?

A key question after learning about all these breakthroughs is: When will quantum computers actually become useful, and how powerful will they be?

One way to estimate is by using something called Rose's Law. While Moore's Law says that classical chips double in power every 18 months, Rose's Law suggests that the number of qubits in quantum computers is also doubling roughly every two years. However, unlike Moore's Law, which held up for several decades, Rose's Law is based on a much shorter historical trend. Given the technical and physical challenges involved in scaling quantum systems, it's uncertain whether this doubling pattern will continue. So while it offers a rough estimate of progress, it should be viewed as more of an optimistic projection than a guaranteed trajectory. Looking at the progress so far, Google's Sycamore reached 54 qubits in 2019 (Arute et al. 2019), and IBM announced a 1,121-qubit processor called Condor for 2024 (Gambetta, 2023). If this growth continues, we might see systems with between 1,000 and 10,000 qubits by the early 2030s, and possibly 100,000 or more by 2040.

But having a lot of qubits isn't enough. What really matters is how many of them are logical qubits, meaning they are stable, error-corrected, and can actually be used for real applications. That's much harder to achieve, and current systems are still far from this. Still, if progress continues, it's possible that by the

2030s or 2040s, quantum computers could break encryption systems like RSA using Shor's Algorithm, solve complex problems in chemistry and physics, and even be used by companies, scientists, and maybe even students through the cloud.

How Will We Use Quantum Computers?

Classical computers became smaller and cheaper over time, from giant mainframes to laptops and now phones. But quantum computers need special conditions: ultra-cold temperatures, zero noise, and complete isolation. So it's very unlikely we'll have quantum computers at home.

So, instead of shrinking into everyday devices, quantum computers will likely stay in labs or data centers. Based on how cloud services are already being used for quantum access today, it seems likely (in the author's view) that a "mainframe-plus-cloud" model could become the standard. In such a setup, quantum systems remain in specialized facilities, while users, from students to companies, can access them remotely via the internet.

This is already starting to happen. For example, IBM has the IBM Quantum Experience, which lets users try quantum experiments online, and Microsoft offers Azure Quantum, which also allows remote access. So while we won't be carrying quantum computers in our pockets, we might still get to use them, just not locally.

The Impact on Cryptography

Quantum computing isn't just about faster science or better simulations, it directly affects cybersecurity.

Today, encryption relies on problems that classical computers can't solve easily, like factoring large numbers (RSA) or searching through all possible keys (AES). But quantum computers can do these much faster using Shor's and Grover's algorithms. If these quantum machines are available on the cloud, and someone uses them to break RSA or AES-128, even encrypted messages could become unsafe, especially during transmission.

That's why researchers are now working on PQC, new types of encryption that even quantum computers can't break. These new methods don't need quantum hardware. They run on regular devices but are designed to resist quantum attacks. But, shifting to PQC, while important, is not easy. It involves updating certificates and secure websites, changing how digital signatures and key exchanges work, and training people in IT and cybersecurity. One report by the U.S. government said that switching just their federal systems could cost over $7 billion between 2025 and 2035. For smaller companies, the cost and effort could be even harder.

An Opportunity for Startups

But this big challenge also opens up a big opportunity. Many startups are now offering PQC-as-a-Service, cloud tools that provide quantum-safe encryption for email, VPNs, and secure websites. These tools are easier to use and don't require expert knowledge. This moment feels a bit like the early days of cloud computing, companies that build trusted tools early might become the giants of the post-quantum security world.

The Bigger Picture

Finally, this isn't just about businesses or researchers. It's also part of a global cybersecurity race. Countries like the U.S., China, the European Union, and India are all investing heavily in quantum tech, not just to

build new things, but also to protect or crack encrypted communications. The first real-world use of quantum computers in cybersecurity might not come from hackers, but from governments. Cryptography has always been about trust. In the quantum era, that trust will depend on how quickly we adapt and how seriously we take this transition.

CONCLUSION: PREPARING FOR A QUANTUM FUTURE

Quantum computing is no longer just science fiction. It is steadily progressing and beginning to impact fields like cryptography. From Shor's and Grover's algorithms to the development of new post-quantum encryption methods, we are entering a phase where the rules of secure communication are being rewritten.

This paper explored how current encryption systems, like RSA and AES-128, are at risk due to the power of quantum algorithms. It also reviewed how governments, researchers, and companies are responding by designing PQC, algorithms that can resist quantum attacks but still work on classical devices.

We also looked at how the field of quantum computing is evolving. While personal quantum devices are unlikely, the "mainframe plus cloud" model means that many users could soon access powerful quantum systems remotely. Companies are already offering quantum-secure services over the cloud, and global investments in quantum research are growing rapidly.

As this new era unfolds, both risks and opportunities will emerge. For young students, researchers, and future engineers, understanding these shifts is not only important, it is exciting. We are part of a generation that will see quantum technology move from theory to real-world use. Learning about it now helps us prepare to build, protect, and shape the digital world of tomorrow.

ACKNOWLEDGEMENTS

The author would like to acknowledge the use of OpenAI's ChatGPT (2025) for support during the ideation, copyediting, and structuring stages of this paper. The tool was used to brainstorm outline options, organize the flow of technical content, and refine the abstract. All critical analysis and final conclusions are the original work of the student researcher.

REFERENCES

Abood, O. G., & Guirguis, S. K. (2018). A Survey on Cryptography Algorithms. *International Journal of Scientific and Research Publications (IJSRP)*, *8*(7). https://doi.org/10.29322/ijsrp.8.7.2018.p7978

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G. S. L., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., & Fowler, A. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, *574*(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. In *National Institute of Standards and Technology*. https://doi.org/10.6028/nist.ir.8105

Farhi, E., Goldstone, J., Gutmann, S., & Sipser, M. (2000). Quantum Computation by Adiabatic Evolution. In *arXiv*. https://arxiv.org/abs/quant-ph/0001106

Fossen-Helle, A. (2020). *Quantum Computing, how it is jeopardizing RSA, and Post-Quantum*

Cryptography. https://bora.uib.no/bora-xmlui/bitstream/handle/11250/2720429/master_thesis_Anna_Fossen-Helle.pdf?sequence=1&isAllowed=y

Gambetta, J. (2023, December 4). *IBM Quantum Computing Blog | The hardware and software for the era of quantum utility is here*. Www.ibm.com. https://www.ibm.com/quantum/blog/quantum-roadmap-2033

Grover, L. K. (1996, November 19). *A fast quantum mechanical algorithm for database search*. ArXiv. https://arxiv.org/abs/quant-ph/9605043

Lloyd, S. (1996, August 23). *Universal Quantum Simulators*. Science. https://fab.cba.mit.edu/classes/862.22/notes/computation/Lloyd-1996.pdf

Mavroeidis, V., Vishi, K., D., M., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications*, *9*(3). https://doi.org/10.14569/ijacsa.2018.090354

NIST. (2017, January 3). *Post-Quantum Cryptography | CSRC | CSRC*. CSRC | NIST. https://csrc.nist.gov/projects/post-quantum-cryptography

Qadir, A. M., & Varol, N. (2019, June). (PDF) A Review Paper on Cryptography. *ResearchGate*. 2019 7th International Symposium on Digital Forensics and Security (ISDFS). https://www.researchgate.net/publication/334418542_A_Review_Paper_on_Cryptography

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134. https://doi.org/10.1109/sfcs.1994.365700

Tozzi, C. (2025, February 24). *5 Companies That Were Forced to Shut Down Due to Data Breaches*. N2WS; N2W. https://n2ws.com/blog/5-companies-shut-down-data-breaches