An Exploration of Quantum Cryptography

Alexandra Sklyarova

Math 4480: Spring 2025

Abstract

Recently, Microsoft unveiled Majorana 1, which is the first ever Quantum Processing Unit (QPU). It is a major step towards making a scalable quantum computer, which would make quantum computation more accessible and more powerful. This innovation prompts the question: how will the increased computation speeds impact security and privacy? Most encryption systems are built with trapdoor functions, meaning it is easy to compute in one direction but difficult to invert without a secret piece of information. So, as computation power increases with QPUs, we will need to ensure that our modern encryption systems are resistant to attacks that will inevitably be supercharged with access to quantum computation speeds. Additionally, we need to attempt to harness this power by building quantum based protocols. This paper goes over the history of quantum encryption and emphasize why it is important. It will also discuss several quantum key distributions: BB84 and the E91 protocol, as well as virtually unbreakable cryptography systems: NTRU and quantum one-time pad.

1 Introduction

1.1 Why Quantum?

Have you ever been reading the news and seen a random link to an article excitedly exclaiming that ”a new largest prime number has been found” and wondered, why do we care? The current largest prime has 41,024,320 digits and it was discovered by Luke Durant, a former Nvidia emplyee. He assembled a global super computer made from graphics processing units (GPUs) that excel at parallelized computation. In fact, his computer was 12x faster than any other on the search for the largest prime. So, one answer to the question ”why do we care?” is that people should be marveling at the computation power that humans have achieved.

This prompts another question, how much faster can we get? The answer to this, is we can get unfathomably faster. As previously mentioned, the prime was computed using a supercomputer, and despite its powerful-sounding name, quantum computing makes it seem like an abacus. To illustrate this, we can look at the Frontier supercomputer, which was once the fastest computing technology available. However, Google recently came out with the Sycamore quantum computer, which completed a problem in 6 seconds that would take Frontier over 47 years!

So, how is this related to cryptography? Well, most modern cryptography systems rely on traditional computation power to be effective. For example, RSA is built on the idea that factoring large numbers is difficult. So, as quantum technology, such as Microsoft’s Majorana 1, become more available, we need to figure out way to either harness this power or making our encryption systems stronger.

1.2 Brief Physics Background

Superposition: describes a state where a quantum system can exist in multiple configurations at the same time. Unlike classical bits, which can only be in one of two states, 0 or 1 a qubit can exist in the 0 state, the 1 state, or any superposition $|\psi\rangle$ of both, represented as a linear combination of 0 and 1. This can be expressed as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where $\alpha, \beta \in \mathbb{C}$ represent the probability of measuring the qubit in either state. This allows a quantum computer to process multiple possible states at once, enabling it to perform many computations in parallel.

Quantum entanglement: is a phenomenon where a group of particles becomes interconnected in such a way that the quantum state of each particle cannot be described independently of the others. This also means a change in one instantly affects the others, regardless of the distance between them.

Heisenberg Uncertainty Principle: it is impossible to simultaneously measure the exact position and exact momentum of a particle. This can be represented by the equation

$$\Delta x \Delta p \geq \frac{h}{4\pi}$$

Where Δx is uncertainty of position, Δp is uncertainty in momentum and h is the Plank constant. This is crucial since measuring a quantum system disturbs it, making it impossible for an eavesdropper to intercept information without detection.

Hilbert Space: complex inner product space equipped with a metric induced by the inner product. The inner product is represented by

$$\langle \phi | \psi \rangle = \sum_j \phi_j \overline{\psi_j}$$

where ϕ, ψ are vectors in this space and the bar represents complex conjugation. The state of a quantum system is represented by a vector of unit length within this Hilbert space.

The basis for a Hilbert space is a set of linearly independent vectors that can be used to represent any other vector in the space. There are three main bases. First, the rectilinear basis composed of two orthogonal unit vectors, typically represented as $r_1 = (1, 0)$ for horizontal polarization and $r_2 = (0, 1)$ for vertical polarization. Second, the diagonal basis consists of $d_1 = (0.707, 0.707)$ for 45-degree polarization and $d_2 = (0.707, -0.707)$ for 135-degree polarization. Lastly, the circular basis with $c_1 = (0.707, 0.707i)$ and $c_2 = (0.707i, 0.707)$ corresponding to the polarization. The dimensionality and the choice of basis within this space are crucial for understanding and manipulating quantum information, as seen in the context of quantum cryptography.

2 History

2.1 Early Days

The beginnings of quantum cryptography can be traced back to the 1970s and 1980s with the publication of *Conjugate Coding* by Stephen Weisner. He was born in the U.S. in 1942 and after receiving his PhD from Columbia University, he developed several important applications of quantum physics. He also was passionate about clean energy and even worked as a construction laborer until his death in 2021 in Israel. His work *Conjugate Coding*, explores a quantum communication technique based on the uncertainty principle and conjugate bases in Hilbert space. Interestingly, his paper was initially rejected by the IEEE and was only published in 1983 in SIGACT News, which suggests many people were skeptical about quantum applications.

In this case two orthonormal bases for an N-dimensional Hilbert space

$$\{\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_N\} \text{ and } \{\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_N\}$$

are conjugate if and only if

$$|\langle a_i | b_j \rangle|^2 = \frac{1}{N}, \quad \forall \ 1 \leq i, j \leq N$$

Physically, this means that if a system is in a state described by a vector from one basis, there is an equal probability of finding it in any of the states of the conjugate basis, and vice versa. He argued that this can be used for something called a conjugate code, which is a communication scheme that encodes information using quantum states that belong to multiple conjugate bases in a Hilbert space. This means that the physical signals (such as photon polarizations) are chosen from bases where measurement in one basis gives no information about states in the other.

Weisner's paper didn't mention cryptography directly, instead he presented other applications such as quantum money. He theorizes that unforgeable currency can be created that would ensure that an unauthorized party cannot accurately measure and replicate the quantum states of the money. The idea here is to rely on the uncertainty principle and the theory behind conjugate bases. The quantum money consists of isolated two-state quantum systems, and if you choose a conjugate basis, you will see that measurement in one basis gives no information about the other. So, when a holder returns the money for verification, they can measure each quantum system in the proper basis to check if the quantum states are unchanged. If any system has transitioned to a different state (due to interference or measurement by a counterfeiter), the verification process detects the alteration. While this might not be the most technologically feasible, it sparked broader conversations about the applications of quantum mechanics.

2.2 Further Developments

Another major contribution happened in 1984, shortly after the publication of *Conjugate Coding.* Two researchers, Charles Bennett and Gilles Brassard developed a cutting edge protocol for distribution of quantum keys. Bennett was born in 1943 and received his PhD from Harvard for molecular dynamics. Brassard was born in 1955 and graduated from Cornell with a PhD in Computer Science. They drew from Weisner's publication and were inspired by other asymmetric key exchanges to create **BB84**. They saw that when information is encoded in non-orthogonal quantum states, such as the polarization of single photons (0, 45, 90, and 135 degrees), any attempt by an eavesdropper to measure these states without knowing the basis in which they were encoded would inevitably disturb the transmission in a random and uncontrollable way, making their presence detectable.

Later on, in 1991 Artur Ekert developed his own protocol called **E91**. Ekert was born in 1961 and graduated from Oxford with a PhD in physics. He used the idea of Bell State to develop this system. First, the Bell states describe entangled 2 quit quantum states. There are 4 such states:

$$|\Phi^+\rangle : \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad |\Phi^-\rangle : \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\Psi^+\rangle : \frac{|01\rangle + |10\rangle}{\sqrt{2}} \qquad |\Psi^-\rangle : \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

In every Bell pair, measuring one of the two qubits instantly determines the state of the other qubit when it is measured. The key idea is that entangled qubits exhibit strong correlations that cannot be explained by classical physics, making it possible to detect eavesdropping attempts.

The implementation of BB84 and E91 will be explained in a later section.

2.3 More Recent Innovation

In 2003 physicists set out to transmit entangled photon through free space. They eventually succeeded and managed to send photons 600 meters across the Danube River. Previously, entanglement had only been observed over a few meters in open air or up to 10 kilometers in optical fibers. Researchers, led by Anton Zeilinger, generated entangled photon pairs by splitting light in a crystal and transmitted them between two telescopes on opposite riverbanks. Their analysis confirmed that the photons' electric fields remained correlated, demonstrating entanglement. This advancement is a step toward using entanglement for secure quantum communication.

In 2004 further progress was made when a bank in Austria has successfully conducted an electronic money transaction using entangled photons to establish an unbreakable communications code. The team, again led by Anton Zeilinger, generated photon pairs by passing a laser through a crystal, splitting single photons into two. One photon from each pair was transmitted from the bank to the city hall via fiber optics. Upon arrival, the polarization of the photons was measured, generating a shared cryptographic key consisting of ones and zeros, which was then used to secure the financial transaction. Fortunately for the researchers, part of the experiment involved the mayor of Vienna transferring a €3000 donation to the University of Vienna team.

Jumping two decades forward, in August 2024, the National Institute of Standards and Technology (NIST) finalized and released three encryption standards designed to withstand quantum attacks. These post-quantum encryption standards aim to secure a wide range of electronic information, from confidential emails to e-commerce transactions. Additionally, companies like Cloudflare are proactively integrating post-quantum cryptography into their services. It enhanced its Zero Trust Network Access solution with quantum resistant algorithms and plans to extend support to all IP protocols. This initiative underscores the industry's commitment to safeguarding data against future quantum threats.

Overall, there is still a long way to go until quantum computation is available on a large scale. However, progress has been exponential in recent decades, and the future for this technology is bright.

3 Quantum key Distribution

3.1 BB84

Idea : encode every bit (0 or 1) of the secret key into the polarization state of a photon.

Alice: decides on a binary string as a secret key. She then sends a sequence of pulses that contain a single photon with polarization according to the bits in the secret key. The pulses that are sent can be found in the following table:

	0	1
rectilinear basis	$\uparrow$	$\rightarrow$
diagonal basis	$\swarrow$	$\nwarrow$

Bob: receives the string and measures the polarizations (can use Glan prism or calcite crystal) and determines if he got sent a 0 or 1.

When the transmitter and receiver use the same polarization basis, the receiver correctly detects the transmitted bit based on whether the photon passes through the filter. However, if their bases differ, the received bits become random due to the nature of photon behavior. After transmission, the transmitter and receiver compare their chosen bases and discard mismatched bits, using only correctly received bits to generate the key.

Example: Suppose Alice wants to send the key

$$0\ 1\ 0\ 0\ 1\ 0$$

She chooses a basis for each photon and gets the following polarizations

0	1	0	0	1	0
rectilinear	**diagonal**	**diagonal**	**rectilinear**	**rectilinear**	**diagonal**
$\uparrow$	$\nwarrow$	$\swarrow$	$\uparrow$	$\rightarrow$	$\swarrow$

Bob receives this and chooses bases to analyze the polarizations

rectilinear	**rectilinear**	**diagonal**	**rectilinear**	**rectilinear**	**rectilinear**
$\uparrow$	$\rightarrow$	$\swarrow$	$\uparrow$	$\rightarrow$	$\rightarrow$
0	1	0	0	1	1
yes	no	yes	yes	yes	no

So the key becomes

$$0\ 0\ 0\ 1$$

when only considering matches with the same basis.

3.2 E91

The process begins with some source center choosing some Entangled Bell State (described above). it then sends the first particle to Alice and the second to Bob

Alice: chooses a polarization basis (could be between $\{0, \frac{\pi}{8}, \frac{\pi}{4}\}$) and makes the measurement using this basis.

Bob: also chooses some polarization basis (could be between $\{-\frac{\pi}{8}, 0, \frac{\pi}{8}\}$) and makes his own measurement.

Both record their result and broadcast their measurement basis. Then they divide the measurement into two groups:

$$\begin{align} G_1 &: \text{ decoy qubits where they chose a different basis} \tag{1} \\ G_2 &: \text{ raw qubits where they chose the same basis} \tag{2} \end{align}$$

They use G_1 to detect any eavesdropping. If the quantum channel is determined to be safe, they can use G_2 as the key.

Example: The central source generates an entangled Bell state:

$$|\Phi^+\rangle = \frac{(|00\rangle + |11\rangle)}{\sqrt{2}}$$

It sends the first qubit to Alice and the second qubit to Bob.

Let's assume after several rounds of measurements, they get:

Round	**Alice's Basis**	**Bob's Basis**	**Kept in Key?**
1	$\frac{\pi}{8}$	0	No (G_1)
2	0	0	Yes (G_2)
3	$\frac{\pi}{4}$	$\frac{\pi}{8}$	No (G_1)
4	$\frac{\pi}{8}$	$\frac{\pi}{8}$	Yes (G_2)

Alice and Bob check their G_1 results for correlations using Bell's inequality. If the results satisfy the Bell inequality, the quantum channel is **secure**. Else, an eavesdropper is present, and they discard the session.

Assuming the channel is secure, Alice and Bob use G_2 to generate the final key.

- Measurement outcome 0 $\Rightarrow$ bit 0
- Measurement outcome 1 $\Rightarrow$ bit 1

So using the above results we get

Round	**Alice's Result**	**Bob's Result**	**Final Key Bit**
2	0	0	0
4	1	1	1

The shared secret key becomes

$$0\ 1$$

4 Cryptography Systems

Besides harnessing the power of quantum mechanics, it is important to consider which classical encryption systems are resistant to the speeds of a quantum computer, i.e. which ones are complicated and convoluted enough to resist.

4.1 NTRU

NTRU was developed in 1996 by Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. All three mathematicians have a background in Number Theory, and especially in cryptography. The system relies on the nuances of polynomial rings as well as the capabilities of reducing modulo a prime to develop a quantum resistant protocol.

Convolution Ring : Let $R[x]$ be a polynomial ring over a commutative ring R. In a convolution polynomial ring, we define a new multiplication operation of $c(x) = a(x) * b(x)$ via :

$$\left(\sum_i a_i x^i\right) * \left(\sum_j b_j x^j\right) = \sum_k \left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k$$

For NTRU, first take the ring of polynomials with integer coefficients, denoted by $\mathbb{Z}[x]$. Then reduce all of the coefficients by some prime q, i.e. all coefficients are in $\mathbb{Z}/q\mathbb{Z}$. After, take the ideal generated by $x^N - 1$, for $N \in \mathbb{N}$, and mod by it. The result is

$$R_q = {}^{\mathbb{Z}_q[x]}\!/_{(x^N - 1)}$$

Here, if we take two polynomials $a(x), b(x) \in R_q$, the convolution is defined as

$$a(x) * b(x) = c(x) \quad \text{with} \quad c_k = \sum_{i+j \equiv k \, (\mathrm{mod} N)} a_i b_{k-i}$$

Center Lift : if $a(x) \in R_q$, then we can lift it to a unique polynomial in R that reduces to $a(x)$ mod p with coefficients in the range $-\frac{q}{2} < a_i < \frac{q}{2}$

Ternary Polynomial : a polynomial $f(x)$ is ternary if

$$f \in T(d_1, d_2) = \{\text{coefficient } d_1 = 1, \text{coefficient } d_2 = -1, \text{all other coefficients } d_{i \neq 1,2} = 0\}$$

NTRU Process:

Choose $N, d, p, q \in \mathbb{Z}$ with p, q prime. Also, $\gcd(p, N) = 1$, $\gcd(q, N) = 1$, $q > (6d + 1)p$

Alice : chooses a private invertible $f \in T(d + 1, d)$ and $f \in T(d, d)$. She computes

$$f^{-1} = F_p \text{ modulo p} \quad \text{and} \quad f^{-1} = F_q \text{ modulo p}$$

and publishes

$$h = F_q * g$$

Bob : chooses plaintext $m \mod p$ and ephemeral key $r \in T(d,d)$. He computes ciphertext

$$e = p \cdot r * h + m \mod q$$

Alice : computes

$$f * e \mod q$$

and center lifts to $a \in R$. The gets

$$F_p * a \equiv m \mod p$$

Quantum computers have not been shown to be able to efficiently solve the NTRU problem. In fact, the best known attacks on NTRU, such as lattice based attacks, are still inefficient compared to classical brute force methods, and quantum computers don't seem to have a clear advantage over classical methods for these specific problems. This is because of the difficulty of the shortest vector problem (SVP) and learning with errors (LWE), which are believed to be hard even for quantum computers.

4.2 One Time Pad

The one-time pad was originally described by Frank Miller in 1882, but in 1919, Gilbert Vernam developed the XOR operation used in the modern encryption process of one-time pad. The term pad originates from early implementations where the key was distributed on a pad of paper, with each sheet being used once and destroyed. This cipher was used throughout the 20th century, with KGB agents being known for carrying minuscule pads.

One Time Pad Process :

A person or organization generates a string of letters or values

$$k = k_1 k_2 ...$$

(at least as long as the secret message). This gets written on a "pad" and is distributed to all the necessary parties.

Alice : converts the message

$$m = m_1 m_2 ...$$

into its binary form and uses the XOR operation with the corresponding bits of the message and the secret key

$$c_i = m_i \oplus k_i$$

She then sends out c.

Bob : undoes the operation directly by reversing the XOR process to get

$$m_i = c_i \oplus k_i$$

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Table 1: XOR Truth Table

While seemingly simple and eerily close to Vigenere, this cipher is virtually unbreakable. This is due to the fact that the key is as long as the message so it is impossible to find a statistical relation within the encrypted text. The key must be truly random and can only be used once because of this.

Back To QKD : Since QKD is a technique for generating and securely distributing random cryptographic keys between two parties, it can be leveraged for OTP. The main weakness of OTP is related to the distribution of the key, so QKD will completely eliminate all vulnerabilities of this cipher.

5 Connections to Other Fields

Quantum cryptography (including QKD and quantum proof schemes) have the potential to revolutionize the safety and security in countless fields. As quantum computing and related processes become more available, it offers a solution to potential attacks on regular encryption systems and increases privacy for all parties that use it.

Banking and Finance

- **Quantum Secure Transactions**: Banks rely on cryptographic protocols to secure online transactions. QKD can ensure that financial transactions remain secure even against future quantum computers.
- **Fraud Prevention**: Quantum cryptography makes man-in-the-middle (MITM) attacks nearly impossible, reducing fraud risks.
- **High-Security Communication**: Secure connections between financial institutions, preventing cybercriminals from intercepting sensitive financial data.

Government and Military

- **Secure Communication**: Quantum encryption can protect classified military and diplomatic communications from cyber espionage.
- **Cybersecurity in Defense Systems**: Prevents adversaries from hacking into military networks, command centers, and intelligence databases.
- **Secure E-Voting**: Ensures that digital votes cannot be altered or intercepted.
- **Tamper-Proof Digital IDs**: Governments can issue quantum-secured national IDs, passports, and biometric authentication systems.

Healthcare and Medical Data

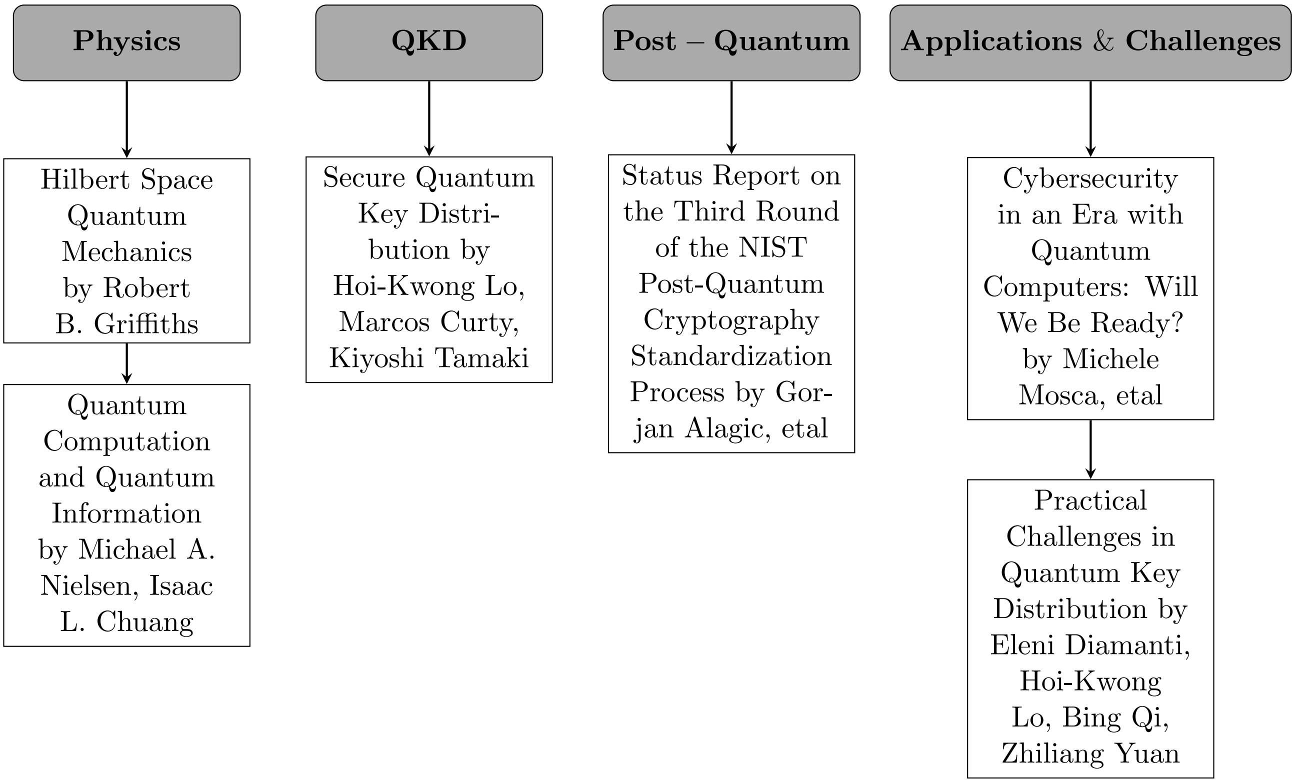
- **Protected Patient Records**: Ensures that medical records stored in hospitals and insurance companies remain confidential and tamper-proof.
- **Secure Telemedicine**: Quantum encryption can protect telehealth consultations from cyber threats.
- **Biomedical Research Security**: Pharmaceutical companies can safeguard drug research and prevent corporate espionage.

Internet Security

- **Hacker-Proof Communication**: providers can use QKD to offer truly secure messaging and video calls.
- **Quantum-Secure VPNs**: protects businesses and individuals from cyber attacks by providing a quantum safe encrypted communication channel.
- **Quantum-Secure Cloud Storage**: companies like Google, Amazon, and Microsoft can use quantum cryptography to protect user data in cloud servers.

6 Further Research

Here are some more papers if you are interested in these topics (citations in Bibliography, [10]-[15]).


Physics
QKD
Post – Quantum
Applications & Challenges
Hilbert Space Quantum Mechanics by Robert B. Griffiths
Quantum Computation and Quantum Information by Michael A. Nielsen, Isaac L. Chuang
Secure Quantum Key Distribution by Hoi-Kwong Lo, Marcos Curty, Kiyoshi Tamaki
Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process by Gorjan Alagic, etal
Cybersecurity in an Era with Quantum Computers: Will We Be Ready? by Michele Mosca, etal
Practical Challenges in Quantum Key Distribution by Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, Zhiliang Yuan

References

[1] Bennett, C. H., Brassard, G. (2014). Quantum cryptography: public key distribution and coin tossing. Theoretical Computer Science, 560, 7–11. https://arxiv.org/pdf/2003.06557.

[2] Microsoft Quantum Team. (2025). Microsoft unveils Majorana-1: The world's first quantum processor powered by topological qubits. Azure Blog. https://azure.microsoft.com/en-us/blog/quantum/2025/02/19/microsoft-unveils-majorana-1-the-worlds-first-quantum-processor-powered-by-topological-qubits/.

[3] Ortiz, J., Sadovsky, A., Russakovsky, O. (n.d.). Modern Cryptography: Theory and Applications - Quantum Cryptography.

[4] Microsoft Quantum Team. (n.d.). Superposition - Quantum Concepts. Retrieved from https://quantum.microsoft.com/en-us/insights/education/concepts/superposition.

[5] Wiesner, S. (1983). Conjugate Coding. SIGACT News, 15(1), 78–88. Columbia University, New York, N.Y., Department of Physics.

[6] Veridify Security. (2025). Quantum Computing is Decades Faster Than the Best Supercomputers. Veridify. https://www.veridify.com/quantum-computing-is-decades-faster-than-the-best-supercomputers/

[7] Baker, S. (2025). New Prime Number 41 Million Digits Long Breaks Math Records. Scientific American. https://www.scientificamerican.com/article/new-prime-number-41-million-digits-long-breaks-math-records/

[8] Garg, A. (2025). Fundamentals of Quantum Key Distribution: BB84, B92, E91 Protocols. Medium. https://medium.com/@qcgiitr/fundamentals-of-quantum-key-distribution-bb84-b92-e91-protocols-e1373b683ead

[9] Hoffstein, J., Pipher, J., Silverman, J. (1998). NTRU: A Ring-Based Public Key Cryptosystem. https://www.ntru.org/f/hps98.pdf

Citations for further research :

[10] Griffiths, R. B. (2014). Hilbert Space Quantum Mechanics. Version of 16 January 2014. Retrieved from https://www.cambridge.org

[11] Nielsen, M. A., Chuang, I. L. (2010). Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge: Cambridge University Press

[12] Lo, HK., Curty, M. Tamaki, K. Secure quantum key distribution. Nature Photon 8, 595–604 (2014). https://doi.org/10.1038/nphoton.2014.149

[13] National Institute of Standards and Technology (NIST). (2025). Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. Retrieved from https://www.nist.gov/publications/status-report-third-round-nist-post-quantum-cryptography-standardization-process

[14] M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?," in IEEE Security & Privacy, vol. 16, no. 5, pp. 38-41, September/October 2018

[15] Diamanti, E., Lo, HK., Qi, B. et al. Practical challenges in quantum key distribution. npj Quantum Inf 2, 16025 (2016). https://doi.org/10.1038/npjqi.2016.25