International Journal of Academic Information Systems Research (IJAISR)
ISSN: 2643-9026
Vol. 8 Issue 9 September - 2024, Pages: 65-73

The Quantum Horizon Eexploring Quantum Computing And Quantum Key Distribution

Mangipudi R L Yaswanth,

Bachelor of Technology,Gitam University Visakhapatnam
ramalingeswarayaswanth@gmail.com

Abstract*: Amalgamation of Quantum Sciences with digital computers gave rise to an exceptional technology with significant advancements in computational power and absolute memory utilization compared to the convectional modus operandi. This paper explores the fundamental principles and applications of quantum computing and Quantum key distribution. It explains the uniqueness of QKD from classical public key distribution, examines the need for QKD in the context of advancing quantum computing capabilities, key theories underlying QKD, describes the working mechanisms of QKD protocols, addresses the challenges associated with implementing QKD, and considers the future prospects of this technology*.

Keywords: Quantum Computing, Public Key Cryptography, Qubits, Quantum Key Distribution(referred as QKD hereby in the article).

1. QUANTUM COMPUTING

Max Plank, creator of quantum theory not just hinted revolutionary insight of incompleteness for Newtonian mechanics, but also paved a path of emergence for Quantum Computing.[1]Although Richard Feynman emphasized on potential creation of quantum device to exercise quantum process, David Detausch made the concept of Quantum Turing Machine a reality. Quantum computing represents an advanced method of computation that employs the quantum mechanical principles to handle information in entirely novel manners.[4]In contrast to classical computers, which utilize bits (0 or 1) as their fundamental units of information, quantum computers use quantum bits or qubits, that exist in combination of both 0 state and 1 state, creating a new amalgamated state of 0 and 1 [see Figure(c)], represented by "BRA-KET" notations. Existence of basic units of extrapolation in superimposed states consider Bra-0{<0|} and Bra-1{<1|}, will increase the computational power exponentially as each state can hold possibility of both the states (<0| = [1 0]) and (<1| = [0 1]). Theories of Atomic Physics like Superimposition, Entanglement, Quantum Tunneling, Decoherence spawned quantum computational theories like Shor's Algorithm, Fourier Transformation, Grover Search algorithm and many other enabled quantum computers to solve complex problems at a rate far above the capabilities of classical computers.

1.1 Scope of Quantum Supremacy

Quantum computation could become the pinnacle of computational processes, where a quantum computer is capable of solving problems that classical computers currently find intractable.[1]Achieving quantum supremacy would have profound implications across various fields, including cryptography, materials science, field of medicine-drug discoveries and artificial intelligence. For example, a quantum computer could efficiently factor large numbers, potentially breaking widely used cryptography codes. In materials science, it could simulate molecular structures at an atomic level, leading to breakthroughs in drug discovery and materials engineering. Demonstrating extremes of quantum sciences would mark a significant milestone, showcasing the superior processing power of quantum computers and opening up new possibilities for solving previously unsolvable problems with optimal memory and time complexities.

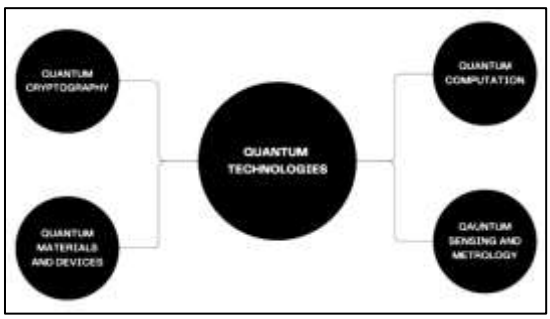


Figure (1) Crucial Fields of Quantum Computing

Quantum Ion Trapping

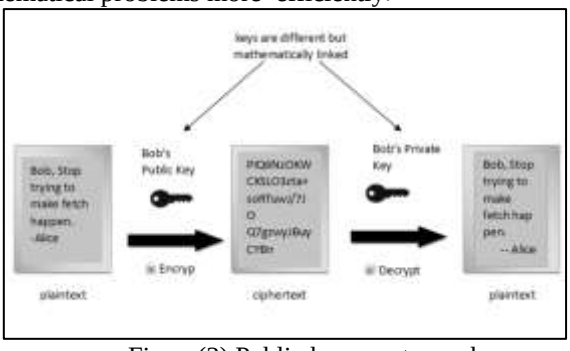
Quantum ion trapping is a sophisticated technique at the forefront of quantum computing, where ions are isolated and controlled to serve as qubits. [19][20] This method involves the use of electromagnetic fields to trap ions(mostly calcium) in a controlled environment, allowing for the precise manipulation of their quantum states, which is crucial for executing quantum operations and developing scalable quantum systems.

At the core of ion trapping is the use of devices like the Paul trap, which utilizes alternating current (AC) and direct current (DC) electric fields to create a dynamic potential that confines ions. The ions are held in place by the balance of these forces, which prevents them from drifting due to thermal motion. This stable confinement is essential for accurate quantum computations. Once trapped, the ions are cooled close to absolute zero using laser cooling techniques. This step is vital as it minimizes the thermal motion of the ions, enabling them to occupy their lowest quantum energy states, which are necessary for reliable qubit initialization. After cooling, laser pulses are employed to manipulate the internal states of the ions. With prescise frequency controlling, intensity, and duration of these pulses, researchers can induce transitions between the quantum states, effectively encoding qubit states (0 and 1) and performing quantum gate operations. A key feature of ion trapping is the ability to entangle ions by manipulating them simultaneously with laser pulses. Entanglement is a fundamental aspect of quantum computing, allowing for operations that are impossible with classical systems. For example, quantum gates like the CNOT gate can be implemented through these entangling interactions between ions. The advantages of quantum ion trapping are significant. It offers high fidelity in qubit operations, essential for error correction and reliable quantum computations. Additionally, ion traps can be scaled to include many qubits, making them suitable for constructing larger quantum systems, and the ions exhibit long coherence times, maintaining their quantum states for extended periods.

However, the technique is not without challenges. The complexity of controlling the laser systems and electromagnetic fields is technically demanding and resource-intensive. Moreover, while ion traps can theoretically be scaled, practical implementation faces issues such as maintaining coherence and avoiding cross-talk between qubits as the number of ions increases. Despite these challenges, ongoing research aims to enhance the control systems, reduce decoherence, and integrate ion traps with other quantum technologies. The future of quantum ion trapping looks promising, with advancements likely to make this technology a cornerstone for development of practical quantum computers.

2. Classical Public Key Distribution

Public key distribution relies on cryptography algorithms such as RSA, DSA, and ECC. These algorithms use pairs of keys: a public key, which can be widely disseminated, and a private key, which remains confidential, Refer [Figure(2)]. Traditional key distribution relies heavily on public key cryptography, which uses complex mathematical algorithms to ensure security. These methods, although robust, face potential vulnerabilities due to increasing computational power and advances in algorithmic attacks. Public Key Cryptography forms the basis of conventional key distribution. Breaking ciphers that employ intricate mathematical calculations demands an impractical amount of processing power. Still, the feasibility of public key ciphers encounters numerous challenges, including the continual development of new attack strategies, weak random number generators, and overall advancements in computing power. The evolution of quantum computing further threatens to undermine the security of public key cryptography by potentially solving these complex mathematical problems more efficiently.



Figure(2) Public key cryptography

3. QUANTUM KEY DISTRIBUTION (QKD)

QKD, or Quantum Key Distribution, is a mechanism to develop secure communication through quantum mechanical principles such as entanglement and classical features of internal reflection, delivering data from the sender to recipients subject to interception.[8] QKD works by producing and transmitting photon particles between sender and receiver, that acts as authentication and threat detection medium.QKD differs from conventional key distribution by employing a quantum system that leverages natural laws to

secure data instead of relying on mathematical principles. For example, the No Cloning Theorem asserts that it is impossible to produce identical clones of an unknown quantum state, thus preventing attackers from merely duplicating the data as they might with current network traffic. This method remains resilient against enhancements in processing power.

4. QKD VS CLASSICAL PUBLIC KEY DISTRIBUTION

Security Basis:
Classical Public Key Cryptography: Exists on the computational strength of solving some mathematical problems. Vulnerable to cryptography attacks and highly vulnerable to quantum attacks, that use Shor's algorithm, that is extremely quick with factorizing large numbers
Quantum Key Distribution: Relies on the principles of atomic physics, making it theoretically secure against any computational attack, including those from quantum computers.
Detecting the Man- In-Middle:
Classical Public Key Cryptography: No inherent mechanism for detecting eavesdropping during key exchange. Man in middle attacks are part and parcel of convectional cryptography mechanisms.
Quantum Key Distribution:
Any attempt disturbs the quantum states of photon particles, alerting the communicating parties as change made in the quantum state cannot restored by the attacker. The "No-Cloning theory" [shown in Figure(5)], discussed further in the paper, will states the possibility of recreating the same quantum state as void.

4.1 Need for QKD

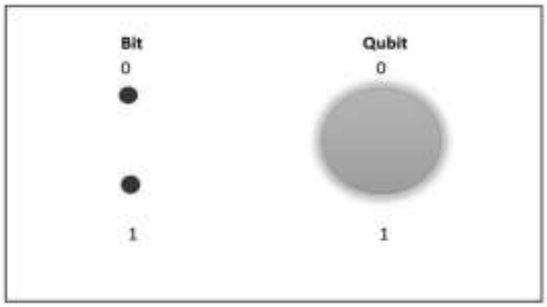
The need for QKD arises from several critical factors:
Quantum Computing Threat: The advancement of quantum computing is a significant threat to present day encryption methods, as quantum computers will be capable of breaking most of the cryptography algorithms that encrypt today's communications. Critical sectors such as finance, healthcare, and national security rely heavily on secure communication channels.
Startups and Enterprises: QKD technology opens up new opportunities for startups and small to medium enterprises in the quantum information sector, fostering innovation and economic growth.[2]Many such agencies can leverage QKD to design robust quantum communication networks with indigenous technologies, ensuring national security and data integrity.
Unbreakable Encryption: QKD leverages the properties of quantum physics to ensure that any attempt to measure the quantum data will disturb it, making eavesdropping detectable. Photons cannot be perfectly copied, and any tampering attempts are traceable. QKD offers a future-proof solution by providing an unbreakable encryption method that can withstand the computational power of quantum computers.

5. ESSENTIAL THEORIES FOR QKD

5.1 Quantum-Based Theories

5.1.1 Superposition

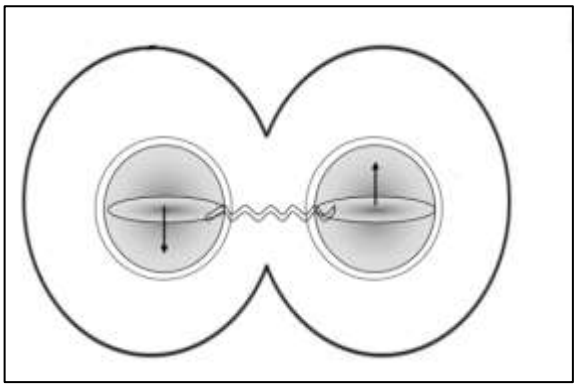
"Schrodinger Cat Problem" that describes the possibility of cat placed in a box being dead and alive at the same instance until a measurement made on its state will be the basis of superimposition.[4]Qubit, the fundamental unit of information in quantum science, exists as fusion state. Unlike classical bits (0/1), a qubit can be both 0 and 1 simultaneously until measured, this phenomenon of existence of the qubit in both 0 and 1 until decoherence is superimposition.Superimposition increase the speed of computation exponentially as the qubits before decoherence exist in multiple states.



Figure(3) Superimposed quantum state

5.1.2 Entanglement

A phenomenon where qubits on getting entangled with each other, even on separating to a distance, tend to stay connected with each other behaving like one linked state. Measurement of one entangled particle instantly affects the state of its partner, irrespective of the distance between them. This property is utilized in QKD to detect eavesdropping, as any interference changes the entangled states, signaling an intrusion.[4]

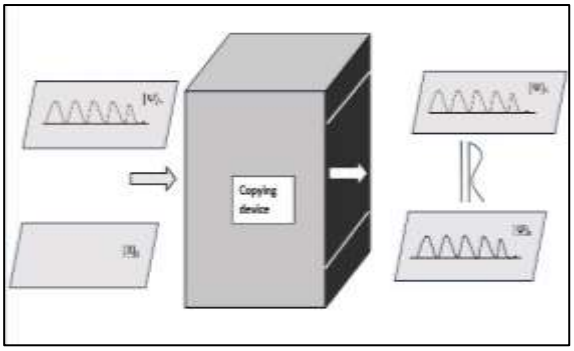


Figure(4) Entangled Qubits

5.1.3 No-Cloning Theorem

The No-Cloning Theorem asserts that it is impossible to create an identical copy of an arbitrary unknown quantum state and cloning of such state is possible based on their orthogonality. Unlike convectional case, replicating the message without loss of information not possible due to quantum inherit properties. This ensures that any attempt to intercept and copy the quantum key will fail and alert the legitimate parties

.



Figure(5) No-Cloning Theorem

5.1.4 Decoherence

Quantum nature is highly benign to external environment. Any possible disturbance or noise from beyond bubble will cause in loss of quantum properties. This loss of vanishing of coherent state is termed as Decoherence. This property of quantum matter is important as it detects the event of interference with external environment.

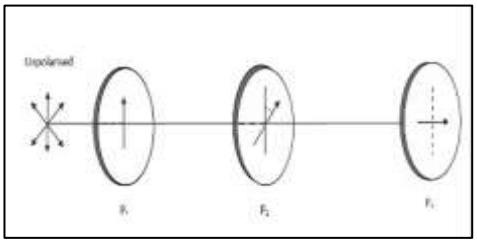
5.1.5 Heisenberg Uncertainty Principle

[5][4]This principle states that certain pairs of properties, like position and momentum, energy and time, spin moments, cannot both be precisely measured simultaneously with absolute accuracy.

5.2 Classical Theories

5.2.1 Electromagnetism

QKD uses photons to transmit information. The polarization states of these photons (horizontal, vertical, diagonal) are crucial for encoding and decoding the keys. Photons, as carriers of electromagnetic waves, exhibit properties such as wave-particle duality and polarization, which are essential for the encoding process in QKD.



Figure(6) Inclinations of Polarized light

5.2.2 Probability and Statistics

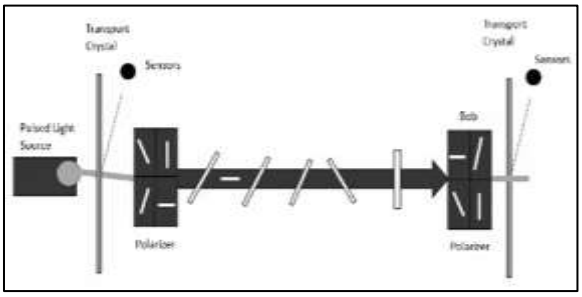
Probability theory is essential in analyzing the error rates and ensuring the security of the transmitted key. QKD protocols, such as BB84, involve statistical analysis of shared bits to detect eavesdropping. By publicly sharing and comparing a subset of their qubits, communicating parties can identify discrepancies that indicate tampering.

5.2.3 Classical Cryptography Principles

Classical physics principles are integrated with quantum theories to create a hybrid system that enhances overall security. While QKD is fundamentally based on quantum mechanics, it also incorporates classical cryptography principles, such as error correction and privacy amplification, to ensure the robustness and security of the key distribution process.

6. WORKING OF QKD

Quantum Key Distribution operates by transmitting photon sequence over fiber optic cables. Each photon encodes a bit of information and passes through a beam splitter, which directs the photon along one of several possible paths to a photon detector. The receiver then communicates with the sender about the sequence of received photons. By comparing a subset of these photons, they can detect any eavesdropping attempts and establish a secure key.

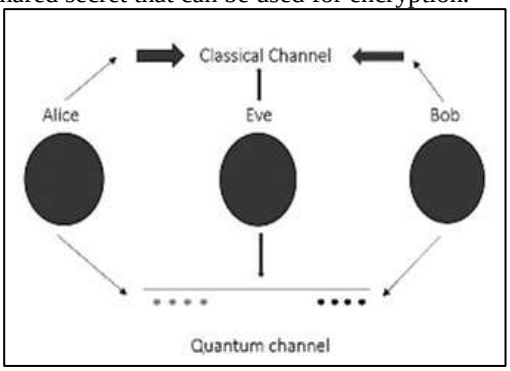


Figure(7) Photon sequence transmission

Consider data transmission between two parties Alice and Bob. Key distribution takes place in following steps:

1. **Quantum State Preparation**: Alice prepares photon states in a specific polarization sequence for transmission. Sequence may contain combination of horizontal, vertical, diagonal polarization.
2. **Transmission**: Alice sends these photons to Bob over a quantum channel (e.g., optical fiber).
3. **Measurement**: Bob randomly selects bases to measure the incoming photon sequence.

4. **Public Discussion**: Alice and Bob publicly compare the bases they used and discard any measurements where the bases do not match.
5. **Key Sifting**: The remaining bits, where Alice and Bob used the same bases, form the sifted key.
6. **Error Correction**: They correct any discrepancies in their sequences using classical communication.
7. **Privacy Amplification**: Alice and Bob reduce the key length to eliminate any partial information an eavesdropper might have.
8. **Final Key**: The resulting key is a shared secret that can be used for encryption.



Figure(8) Information exchange in QKD

TABLE 1. PROTOCOLS OF QUANTUM KEY DISTRIBUTION

PROTOCOL	ABSTRACT	LIMITATION
BB84 Protocol	Developed by Charles Bennett and Gilles Brassard in 1984, this protocol uses the polarization states of photons to encode key bits. [6]It is the first and most widely used QKD protocol, ensuring secure key exchange by utilizing quantum superposition and the no-cloning theorem.	Susceptible to photon number splitting (PNS) attacks and implementation flaws such as detector inefficiencies. Requires ideal single-photon sources for optimal security.
E91 Protocol	Proposed by Artur Ekert in 1991, the E91 protocol relies on quantum entanglement rather than polarization states. Two entangled particles are generated, with each party receiving one. Measurements on these particles lead to correlated outcomes, allowing for the establishment of a secure key.[7]	The protocol requires a reliable source of entangled particles, which can be challenging to produce and maintain over long distances. Entanglement distribution can be affected by environmental factors, reducing the fidelity of the entangled states.
Decoy State Protocol	An extension of the BB84 protocol, the Decoy State protocol addresses the vulnerability of multi-photon pulse attacks by varying the intensity of the pulses used in key generation. This variation helps in detecting potential eavesdropping by comparing the	The security of the Decoy State protocol depends on accurately controlling the intensity of the decoy pulses, which can be difficult in practical implementations. The protocol also assumes an idealized environment, which may not always be

	transmission rates of decoy and signal states.[14]	achievable in real-world applications.
Silberhorn Protocol	This protocol, also known as the Continuous-Variable QKD (CV-QKD) protocol, was introduced by Christine Silberhorn and her collaborators. It uses continuous variables, such as electromagnetic field quadrature components, instead of discrete variables like polarization, to encode information.[12]	CV-QKD is highly sensitive to losses and noise in the communication channel, limiting its effective range and making it less robust compared to discrete-variable QKD protocols. It also requires advanced detection techniques, such as homodyne or heterodyne detection, which may complicate implementation.
KMB09 Protocol	Proposed by Kiyoshi Tamaki, Marcos Curty, and Norbert Lütkenhaus in 2009, the KMB09 protocol combines the decoy state method with phase-randomized weak coherent pulses. This hybrid approach aims to enhance security against practical attacks, including PNS attacks, by better detecting and mitigating eavesdropping attempts.	The protocol's complexity increases due to the combination of multiple techniques, which may lead to challenges in implementation and increased computational overhead. Additionally, the effectiveness of the protocol depends on the accurate randomization of phases and precise control of pulse intensity.[13]

7.1 CHALLENGES WITH QKD

Integration with Existing Infrastructure: Incorporating Quantum Key Distribution (QKD) into curent communication networks requires significant modifications to existing hardware and protocols. This process involves updating or replacing conventional components with quantum-compatible ones, such as quantum repeaters and single-photon sources, which can be technically challenging and resource-intensive. Moreover, ensuring seamless interoperability between classical and quantum systems necessitates extensive testing and standardization efforts[16].

Practical Imperfections: Real-world QKD systems are not immune to practical imperfections that can affect their performance and security. For instance, single-photon detectors used in QKD may have non-ideal efficiency and dark counts, which can introduce errors and potentially open up security vulnerabilities. These imperfections require careful calibration and error correction techniques to ensure the reliability and robustness of the QKD system.

Distance Limitations: The effective range of QKD is constrained by photon loss over long distances in fiber optic cables. As photons travels through the optical fibers, they can absorb and scatter, leading to a decrease in the signal strength. This limits the maximum distance over which QKD can be implemented effectively. Although solutions such as quantum repeaters and satellite-based QKD are being explored to extend the range, they are still in the experimental stage and are not yet widely deployed.

Cost and Complexity: The implementation of QKD systems is currently expensive and complex, posing a significant barrier to widespread adoption. The specialized technologies required for QKD, such as single-photon sources, detectors, and quantum repeaters, is costly and often requires highly skilled personnel for installation and maintenance. Additionally, the complexity of integrating QKD with existing infrastructure adds to the overall expense, making it less accessible for many organizations and industries. Reducing these costs and simplifying the technology is crucial for broader adoption in the future.

7.2 Future

The full potential of Quantum Key Distribution (QKD) will soon be existent with efforts focusing on several following areas:
Research and Development: Ongoing investment in research and development (R&D) is crucial to overcome the existing limitations of QKD systems. By advancing quantum repeaters, improving single-photon detectors, and developing robust error correction methods, R&D can significantly enhance the efficiency, range, and security of QKD. These innovations are crucial for making QKD more practical for widespread adoption.

Developing a Comprehensive Strategy: A well-structured strategy is necessary to ensure effective resource allocation. [9]This strategy should prioritize areas with substantial economic and strategic value, such as protecting critical infrastructure, financial services, and national security. It should also provide a clear road map for the development, testing, and deployment of QKD systems, ensuring that efforts are coordinated to achieve long-term objectives.

Harnessing the Power of Startups and Big Tech: Development of Collaboration and innovation that drive productivity between startups and large technology companies is vital for advancing quantum technology applications. Startups bring innovative approaches and agility, while big tech companies contribute significant resources, advanced research facilities, and market reach. By working together, these entities can accelerate the development and commercialization of QKD technologies, making them more accessible and practical for various sectors.

Standardization and Regulation: Establishing standards and regulatory frameworks is crucial for the secure and interoperable deployment of QKD technologies. Standardization ensures that different QKD systems can operate together seamlessly, facilitating broader adoption. [9][3]Regulatory frameworks provide guidelines for the safe implementation and operation of QKD, protecting against potential security risks and ensuring adherence to industry best practices internationally.

TABLE 2. QUANTUK KEY DISTRIBUTION CHALLENGES

CHALLENGE	DESCRIPTION	WAYS TO RESOLVE	SUPPORTING RESEARCHES
Integration with Existing Infrastructure	QKD systems often struggle to integrate with existing classical communication networks, which are not inherently designed for quantum-based technologies. This challenge includes compatibility with existing protocols and the need for specialized hardware.	Hybrid systems combining classical cryptography with QKD can be developed to ease the integration. Standardization efforts, such as those by ETSI and ITU-T, are also key to fostering interoperability.	Roman Wolf's "Quantum Key Distribution" discusses the importance of hybrid systems for gradual integration, while Sergiy O. Gnatyuk's work highlights the role of international standards in this process.
Practical Imperfections	Real-world QKD implementations suffer from imperfections such as detector inefficiencies, faulty single-photon sources, and environmental noise. These imperfections can lead to security vulnerabilities and reduced performance.	Implement error correction and privacy amplification techniques to mitigate the effects of imperfections. Advances in photonic technology, such as improved single-photon sources, can also address these issues.	Research by Marand and Townsend (1995) focuses on error correction in QKD, while later studies by Gisin et al. (2002) examine advances in photonic technology for enhancing QKD systems.
Distance Limitations	The secure transmission distance of QKD is limited by photon loss and decoherence over long distances. Currently, QKD is feasible over distances up to about 100-200 km without repeaters.	Quantum repeaters and satellite-based QKD are promising solutions to extend the range. Quantum repeaters work by using entanglement swapping, while satellite QKD can overcome terrestrial limitations.	Sergei Kulik's work on quantum repeaters explores their potential for extending QKD distances. Additionally, the Micius satellite project demonstrates the feasibility of space-based QKD over long distances.
Cost and Complexity	QKD systems are expensive and complex, requiring specialized hardware such as single-photon detectors and secure quantum channels. This makes widespread adoption challenging.	Economies of scale and advancements in quantum photonics can reduce costs. Research into simpler and more cost-effective QKD setups, such as continuous-variable QKD (CV-QKD), can also alleviate this issue.	The work of Silberhorn et al. on CV-QKD explores how continuous-variable systems can offer a more cost-effective alternative to traditional discrete-variable QKD systems.

CONCLUSION

Quantum Key Distribution offers a groundbreaking method for ensuring secure communication. By harnessing the principles of quantum mechanics, offering a theoretically unbreakable method of establishing a secret key between two parties. Unlike traditional cryptography based on complex mathematical problems, this key distribution leverages the unique properties of quantum bits to ensure security. The future of Quantum key distribution looks promising, but several challenges must be addressed for its widespread adoption. Integration with existing infrastructure, overcoming practical imperfections, addressing distance limitations, and reducing costs are critical areas that require focused research and development.To realize the full potential of this technique, it is essential to harness uniqueness of Quantum Sphere. Research and development in quantum technology continues to focus on overcoming the current limitations of QKD systems and improving their efficiency and range. Additionally, standardization and regulation will be crucial in ensuring the secure and interoperable deployment of QKD technologies.

Digital Computation has emerged as a response to how developed Analog Logic could be.How enhanced can digital computation go? Quantum Computation should be the paramount.

APA REFERENCES

Books

[1] Kaku, M. (2019). *Quantum Supremacy: How Quantum Computers Will Unlock the Mysteries of Science—and Usher in a New Quantum Age*. Dutton.

[2] Sanders, B. (2020). *Quantum Computing for Everyone*. The MIT Press.

[3] Bernhardt, C. (2020). *Quantum Computing: The Future of Computing*. Sterling.

[4] Susskind, L., & Friedman, A. (2014). *Quantum Mechanics: The Theoretical Minimum*. Basic Books.

[5] Planck, M., & Bohr, N. (1922). *Quantum Theory*. Class CS Publisher.

Research Papers

[6] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., … & Wehner, S. (2020). Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012-1236. doi:10.1364/AOP.361502.

[7] Xu, F., Ma, X., Zhang, Q., Lo, H. K., & Pan, J. W. (2020). Secure quantum key distribution with realistic devices. Reviews of Modern Physics, 92(2), 025002. doi:10.1103/RevModPhys.92.025002.

[8] Pirandola, S., Braunstein, S. L., & Lloyd, S. (2015). Advances in quantum teleportation. Nature Photonics, 9(10), 641-652. doi:10.1038/nphoton.2015.154.

[9] Diamanti, E., Lo, H. K., Qi, B., & Yuan, Z. (2016). Practical challenges in quantum key distribution. npj Quantum Information, 2(1), 1-12. doi:10.1038/npjqi.2016.25.

[10] Yin, H. L., Chen, T. Y., Yu, Z. W., Liu, H., You, L. X., Zhou, Y. H., … & Pan, J. W. (2016). Measurement-device-independent quantum key distribution over a 404 km optical fiber. Physical Review Letters, 117(19), 190501. doi:10.1103/PhysRevLett.117.190501

[11] Bruzewicz, C. D., Chiaverini, J., McConnell, R., & Sage, J. M. (2019). Trapped-ion quantum computing: Progress and challenges. Applied Physics Reviews, 6(2), 021314. doi:10.1063/1.5088164.

[12] Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N. J., Ralph, T. C., Shapiro, J. H., & Lloyd, S. (2012). Gaussian quantum information. Reviews of Modern Physics, 84(2), 621-669. doi:10.1103/RevModPhys.84.621.

[13] Yin, Z. Q., Fu, Y., & Chen, W. (2019). Practical quantum key distribution with polarization encoding. Physical Review A, 99(4), 042326. doi:10.1103/PhysRevA.99.042326.

[14] Lucamarini, M., Yuan, Z. L., Dynes, J. F., & Shields, A. J. (2018). Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature, 557(7705), 400-403. doi:10.1038/s41586-018-0066-6.

[15] Zhang, J., Pagano, G., Hess, P. W., Kaplan, H. B., Kyprianidis, A., Becker, P., … & Monroe, C. (2020). Observation of a many-body dynamical phase transition with a 53-qubit quantum simulator. Nature, 551(7682), 601-604. doi:10.1038/nature24654.

[16] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., … & Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505-510. doi:10.1038/s41586-019-1666-5.

[17] Zhang, J., Pagano, G., Hess, P. W., Kaplan, H. B., Kyprianidis, A., Becker, P., … & Monroe, C. (2020). Observation of a many-body dynamical phase transition with a 53-qubit quantum simulator. Nature, 551(7682), 601-604. doi:10.1038/nature24654.

[18] Bharti, K., Haug, T., Vedral, V., & Kwek, L. C. (2021). Noisy intermediate-scale quantum algorithms. Reviews of Modern Physics, 94(1), 015004. doi:10.1103/RevModPhys.94.015004.

[19] Bruzewicz, C. D., Chiaverini, J., McConnell, R., & Sage, J. M. (2019). Trapped-ion quantum computing: Progress and challenges. Applied Physics Reviews, 6(2), 021314. doi:10.1063/1.5088164.

[20] Wright, K., Beck, K. M., Debnath, S., Amini, J. M., Nam, Y., Grzesiak, N., … & Monroe, C. (2019). Benchmarking an 11-qubit quantum computer. Nature Communications, 10(1), 5464. doi:10.1038/s41467-019-13534-2.