Kalpa Publications in Computing
Volume 19, 2024, Pages 103–120
Proceedings of 6th International Conference
on Smart Systems and Inventive Technology

Investigation of Quantum Antenna Process for Advanced Wireless Communication systems by implementing Quantum Key Distribution Algorithms

Prasad Kasigari [1], Gayathri Kamasani [2], Gopisriya Kavanoor [3], Baba Shareef Muntimadugu [4], Abubakar Shaik [5]

[1]Associate Professor, [2,3,4,5]Scholar

[1,2,3,4,5] Department of Electronics and Communication Engineering

[1,2,3,4,5] Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh, India.

kasigariprasad@gmail.com kamasanigayathri58@gmail.com gopisriyakavanoor@gmail.com muntimadugushareef@gmail.com shaikabubakar387@gmail.com

Abstract

The forthcoming age of communication systems requires increased security, faster processing, and simpler encryption techniques. Quantum information and communication technology offer a revolutionary era featuring high-speed and inherently secure networks. With the looming prospect of quantum supremacy, traditional encryption systems face potential obsolescence in terms of security. In response to this challenge, quantum key distribution (QKD) emerges as an innovative solution for exchanging secret keys in a quantum based manner, addressing the limitations of conventional encryption methods. Within the proposed work, the focus extends to the implementation of a MIMO-QKD scheme tailored for terahertz (THz) frequency applications. The paper provides a comprehensive examination of both single-antenna QKD schemes and the performance of the MIMO QKD scheme. Simulation results underscore the indispensability of multiple antennas to mitigate the substantial free-space path loss encountered at THz frequencies.

Keywords: Quantum communication, Quantum key distribution (QKD), Future Antennas, Quantum antenna (q-antenna) theory. Ultra-fast networks, Quantum supremacy, Secure digital communication, Quantum computing.

1. Introduction

In the field of secure communication, quantum encryption is an innovative solution that provides unbreakable and fully protected communication lines. The growing demand for high data rates has driven research into new physical layer solutions, including research into high Hertz (THz) bands for MIMO systems and fifth generation (B5G) applications [1]. The need for secure and encrypted data transmission is essential to improve the reliability and privacy of future communication systems that may achieve high transmission rates. Quantum Key Distribution (QKD) is an attractive solution to meet the challenges of creating highly secure communication links. QKD is a method of secure communication that utilizes the principles of quantum mechanics to establish a secret key between two parties, typically referred to as Alice (the sender) and Bob (the receiver). The secret key generated through QKD can then be used for encrypting and decrypting messages, ensuring the confidentiality and integrity of the communication. Traditional cryptographic algorithms such as Rivest-Shamir-Adleman (RSA) which are Based on the assumption that classical computers cannot solve complex prime factorization problems efficiently, Shorand's factorization algorithm is expected to be applied to quantum computers in the near future. The development of functional computing, characterized by the increasing number of quantum bits (qubits), poses a threat to the security of RSA.

Current key distribution algorithms, such as the Diffie-Hellman algorithm, are based on the assumption that modern computers cannot solve the discrete logarithm problem efficiently and face difficulties due to the speed of development of quantum computing [2]. Despite the imminent threat that quantum computing poses to existing cryptographic algorithms. QKD emerges as a shield that provides the ultimate protection for future information systems. Based on the principles of the no-cloning Theorem and the Heisenberg Uncertainty Principle, QKD uses quantum channels to transmit quantum states and authenticated classical channels to transfer fundamental measurement data. The quantum key distribution protocol is shown in Figure 1.

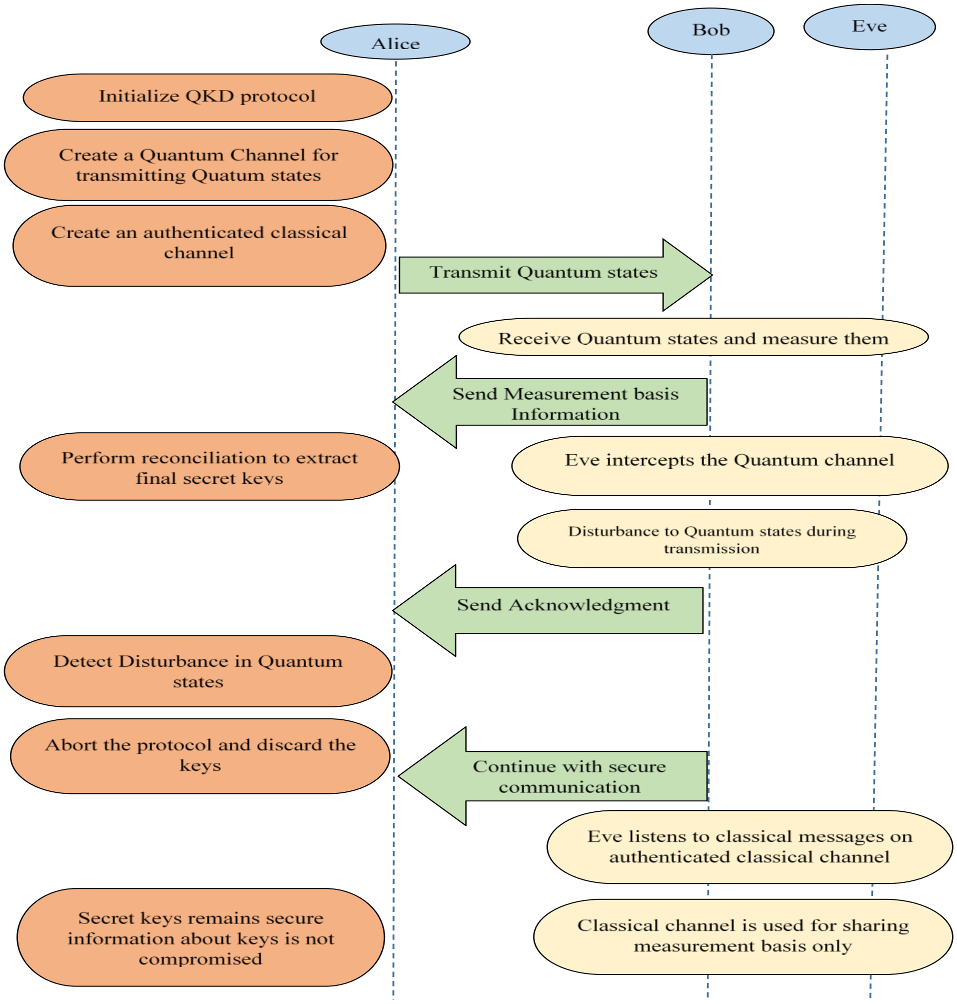
Alice
Bob
Eve
Initialize QKD protocol
Create a Quantum Channel for transmitting Quatum states
Create an authenticated classical channel
Transmit Quantum states
Receive Ouantum states and measure them
Send Measurement basis Information
Perform reconciliation to extract final secret kevs
Eve intercepts the Quantum channel
Disturbance to Quantum states during transmission
Send Acknowledgment
Detect Disturbance in Quantum states
Abort the protocol and discard the keys
Continue with secure communication
Eve listens to classical messages on authenticated classical channel
Secret keys remains secure information about keys is not compromised
Classical channel is used for sharing measurement basis only

Fig. 1. Quantum key distribution protocol

The QKD design ensures that a listener, Eve, who is listening to classical messages on an authenticated channel, can only access the basic measurement and data, not the actual results. This precaution protects the secret keys, enhancing the ability of QKD to truly facilitate the exchange of random secret keys between communicating parties Alice and Bob. QKD is classified into discrete variable QKD (DV-QKD) and continuous variable QKD (CV-QKD) depending on how the essential information is encoded in the quantum states [3].

The protocol involves matching data to generate final secret keys. The laws of quantum physics mitigate against possible eavesdropping by an eavesdropping entity (Eve) of the quantum channel. The communicating parties (Alice and Bob) detect any interference in the quantum states during transmission, allowing them to immediately interrupt the protocol and discard the compromised keys.

This paper proposes a novel approach: a MIMO CV-QKD scheme to enhance the secret key rate (SKR) and transmission distance at THz frequencies. The choice of THz frequencies is determined by the favorable inverse relationship between thermal noise and frequency, allowing positive SKR at room temperature. Unlike previous THz QKD systems, the current proposal avoids the use of low-efficiency

THz optical transducers [4]. The main contributions of this paper are the introduction of the MIMO CV-QKD system model and the SVD-based transmit-receive beam design method. Analytical expressions for the SKR show a non-trivial dependence on the operating frequency, emphasizing the non-monotonic nature of the performance. The simulation results highlight the need for multiple antennas to overcome the large headspace loss in the THz frequency range, an important factor not addressed in previous THz QKD works. The study also shows that positive SKR are achievable in the frequency range of 10-30 THz. There are some limitations like complexity management, Energy-Efficient MIMO Designs.

2. Literature Survey

This literature survey centers on advancing wireless communication systems through the exploration of Quantum Key Distribution (QKD), with a specific emphasis on the investigation of quantum antenna processes as a crucial component in this transformative landscape. Quantum antennas, leveraging the principles of quantum entanglement and superposition, hold the potential to revolutionize the efficiency and range of wireless communication. The survey(Table 1) delves into existing research, methodologies, and experimental findings concerning the development and implementation of quantum antennas, shedding light on their pivotal role in the advancement of wireless communication systems.

Table 1: Literature survey on Quantum Key distribution in wireless communication

Year	**Author**	**Title**	**Objective**	**Methodology**	**Observation**
2020	Dr.Sarah Li	Secure Quantum Communication Networks: Quantum Antenna Integration	Develop practical approaches for implementing QKD algorithms in quantum antenna systems.	Conduct simulations to assess the performance of quantum antennas in networked communication scenarios.	Investigate methodologies for integrating quantum antennas into secure communication networks.
2020	Prof. James Thompson	Hybrid Quantum-Classical Communication Systems	Investigate the creation of hybrid systems for improved communication flexibility**.**	Develop prototypes that combine quantum and classical communication	Observe the potential benefits of integrating quantum and classical

		with Quantum Antennas		mechanisms in antenna systems. Evaluate the performance of hybrid systems through simulations and field experiments.	communication in antennas.
2019	Dr. Sophia Wang	Quantum Channel Optimization for Antenna Systems	Optimize quantum channels in antenna systems for enhanced communication reliability.	Utilize quantum optimization algorithms to assess and improve the efficiency of quantum communication channels.	Examine the influence of quantum channel estimation on wireless communication.
2019	Prof. Michael Chen	Quantum Entanglement in Antenna Systems for Long-Range Communication	Investigate the practical implementation of entangled antenna systems.	Develop entangled antenna prototypes and conduct field experiments to assess their communication range	Explore how quantum entanglement can extend the range of wireless communication
2018	Dr. Aisha Rahman	Quantum Antennas: Enabling Secure Wireless Communication	Enhance the security of wireless communication through quantum antennas.	Develop quantum antenna prototypes and assess their performance in real-world scenarios.	Investigate the integration of quantum key distribution algorithms

					with antenna systems.
2017	Dr. Emily Rodriguez	Quantum Miniaturization Techniques for Antenna Systems	Investigate methods to create compact quantum antennas for efficient wireless communication.	Employ simulations to assess the performance of miniaturized quantum antennas in various communication scenarios.	Observe the potential for miniaturization in quantum antenna design.
2016	Dr. Shabnam Siddiqui	Quantum Antennas for Secure Wireless Communication	Explore the incorporation of antennas into quantum key distribution (QKD) protocols.	Conduct experimental studies to validate the effectiveness of QKD in antenna systems	Enhance the security of wireless communication through quantum-secure antenna systems
2007-2015	Dr. Michael Hayes	Advancements in Quantum Cryptography: A Historical Perspective	Contribute to the theoretical understanding of quantum cryptographic protocols.	Mathematical modeling and theoretical analysis of quantum cryptographic systems. Early experimental validations of QKD principles.	Explore the feasibility and challenges of implementing QKD in real-world scenarios.

2000-2007	Prof. Katherine Adams	Early Developments in Quantum Key Distribution for Secure Communication	Develop the foundational concepts of QKD protocols.	Theoretical developments based on quantum mechanics principles. - Initial experimental demonstrations of QKD concepts.	Pioneer research in the application of quantum principles for secure communication

3. Methodology

System Architecture of QKD in MIMO

The primary goal of this integrated system is to create a resilient and secure communication channel by harnessing the advantages of Quantum Key Distribution (QKD) for secure key distribution and MIMO for efficient data transmission.

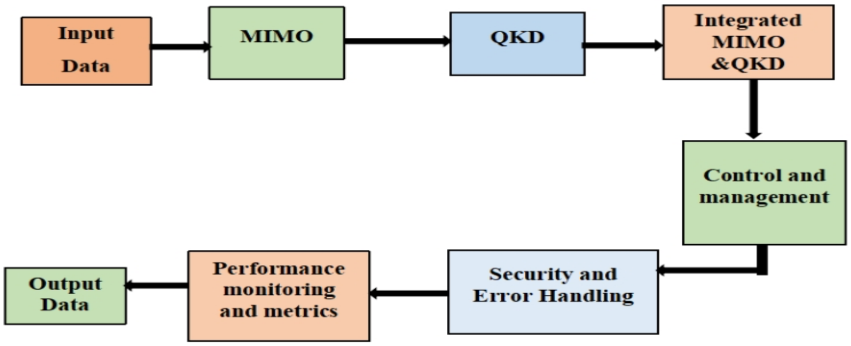

Fig. 2 . Block diagram of Integrated QKD-MIMO system

The Quantum Key Distribution (QKD) module consist of source, channel, and receiver. QKD Source generate quantum states dedicated to key distribution. This involves creating quantum states that will be used for secure key distribution in Quantum Key Distribution (QKD) systems. Employ quantum properties like polarization or phase for effective encoding. These Quantum properties, are utilized to encode information on quantum states, enhancing the effectiveness of the key distribution process. Quantum Channel transmits the quantum states between the QKD source and receiver: The quantum channel facilitates the transmission of quantum states between the QKD source and the receiver. Implement secure QKD protocols (e.g., BBM92, E91) for the exchange of secure keys. Secure QKD protocols like BBM92 and E91 are employed to ensure a protected exchange of cryptographic keys over the quantum channel. Quantum key receiver receive the quantum states and execute measurements based on QKD protocols: The quantum key receiver receives quantum states transmitted over the quantum channel and performs measurements according to QKD protocols. The receiver securely extracts shared secret key bits from the quantum states, forming the basis for secure communication.

MIMO module generally consists of transmitter, channel, and receiver where MIMO Transmitter Encode classical information through spatial multiplexing that is Classical information is encoded using spatial multiplexing techniques in the MIMO transmitter. Simultaneously transmit multiple signals from various antennas for improving communication performance. MIMO Channel is the wireless communication channel considering multiple transmit and receive antennas. The MIMO channel is modeled to account for multiple antennas at both the transmitter and receiver ends. Incorporate characteristics such as fading, channel correlation, and spatial diversity. The MIMO receiver collects signals transmitted from multiple antennas. Employ MIMO signal processing techniques (e.g., maximum likelihood detection, spatial multiplexing) for information recovery: Signal processing techniques like maximum likelihood detection and spatial multiplexing are used for information recovery at the MIMO receiver.

In Integrated QKD-MIMO Communication Framework, the Quantum-Classical Interface establishes a seamless connection between the Quantum Key Distribution (QKD) and Multiple Input Multiple Output (MIMO) components, facilitating integrated communication. This smooth link ensures the effective utilization of the secure key generated by QKD in classical communication systems. Through the quantum-classical interface, the secure key seamlessly integrates into classical communication, enhancing overall security. Encryption methods are employed, leveraging the QKD-generated key to fortify the communication process, thereby providing a robust and secure framework for information transfer. Block diagram of the Integrated QKD-MIMO system is shown in Figure 2.

Control and Management Strategies creats a robust key management system is crucial for effectively administering and distributing quantum-generated keys through the Quantum Key Distribution (QKD) process. Synchronization between the QKD and Multiple-Input Multiple-Output (MIMO) systems is essential to ensure seamless and efficient operation. The deployment of adaptive strategies, becomes imperative for optimizing system performance in diverse channel conditions. Implementing feedback mechanisms allows for dynamic adjustments to QKD and MIMO parameters, ensuring adaptability to changing environmental factors and ultimately enhancing the overall efficiency of the system.

Incorporating quantum security measures involves the integration of quantum error correction codes, offering an effective mechanism for rectifying errors in quantum states. A continuous monitoring system for security parameters [5] within the quantum channel is established to enhance overall reliability. Complementing these measures, classical security strategies are implemented, including classical error correction and privacy amplification techniques, to reinforce the security of classical communication. Additionally, classical encryption methods are incorporated to further fortify the overall security of the communication system, resulting in a comprehensive and robust security framework.

The performance evaluation of Quantum Key Distribution (QKD) by assessing the key metrics like the Quantum Bit Error Rate (QBER) and key generation rate, offering valuable insights into the efficiency of the QKD process. Simultaneously, the monitoring of classical communication metrics, including signal-to-noise ratio, throughput, and bit error rate, enables an assessment of the classical communication system's performance within the integrated framework [6]. QKD, utilizing quantum mechanical properties, facilitates secure key exchange between entities, traditionally known as Alice and Bob. Concurrently, Multiple Input Multiple Output (MIMO) characterizes wireless communication systems equipped with multiple antennas at both the transmitter and receiver. In the QKD-MIMO system, multiple quantum channels are strategically employed to enhance key generation rates. Finally integrated MIMO-QKD System provides the secure digital communication by considering techniques and elements of QKD.

Equations of QKD

The equations involved in QKD describe the various quantum states and measurements used in the protocol. Some of the fundamental equations in QKD are listed below.

*Key generation rate***:** It provides a comprehensive measure of the system's capability to generate secure cryptographic keys through quantum processes across multiple communication links. R denotes the total key generation rate for the entire quantum communication system

$$R = \sum i\, ri \qquad \ldots\ldots (1)$$

Where ri is the key rate for each individual quantum channel (link between one transmit and receive antenna pair). Summing over all channels gives the total system key rate.

Quantum bit error rate (QBER): The QBER is a critical metric in quantum communication systems and reflects the accuracy of transmitting quantum bits (qubits) over a quantum channel. The QBER is essentially the ratio of the number of errors to the total number of quantum bits transmitted on a particular channel. Monitoring and analysing the QBER for each channel help in assessing the overall performance of the quantum communication system and making adjustments or improvements as needed.

$$QBERi = \frac{ei}{ni} \qquad \ldots\ldots\ldots (2)$$

Where ei is the number of quantum bit errors and ni is the total number of quantum bits transmitted over channel i.

*Channel model with fading***:** It can be interpreted as a linear combination of the input quantum state, the fading coefficient, and the noise. The presence of fading and noise in the quantum communication channel has significant implications for the security and reliability of quantum key distribution (QKD) systems. Fading introduces variability in the channel characteristics, affecting the quality of the received quantum states. Additionally, additive noise can introduce errors and uncertainties in the quantum communication process.

$$yi = hi\, xi + ni \qquad \ldots\ldots\ldots (3)$$

Where xi and yi are inputs and outputs, hi is the complex fading coefficient, and ni is additive noise for channel i. Fading and noise impact QBER and secret key rates.

MIMO Capacity: The capacity of a Multiple Input, Multiple Output (MIMO) communication system can be calculated using the MIMO channel capacity formula. The capacity represents the maximum achievable data rate over the MIMO channel under certain conditions. The formula for MIMO channel capacity is given by:

$$C = log_2\left(det\left(I_N + \frac{\rho}{N_t}H^H H\right)\right) \qquad \ldots\ldots\ldots (4)$$

Where, C is the capacity in bits per second (bps), $\mathbf{I}_N$ is the N×N identity matrix, ρ is the signal-to-noise ratio (SNR) of the channel, Nt is the number of transmit antennas, H is the N×Nt channel matrix representing the wireless channel.

The channel matrix H incorporates the fading coefficients and spatial characteristics of the MIMO channel. The capacity formula takes into account the impact of the channel matrix on the transmission performance.

Secure Key Integration: This equation represents the integration of quantum key material into a classical communication system to enable secure transmission of classical messages. This classical key can then be used for secure communication between the parties, ensuring confidentiality and resistance against unauthorized access or eavesdropping.

This can be expressed as:

$$K_{classical} = Encryption\big(K_{QKD}, Message\big) \quad \ldots..(5)$$

Where, $K_{classical}$ is the encrypted classical key

Simplified form of the secret key rate: The rate at which secret keys can be generated and securely shared between two parties, typically referred to as Alice and Bob. The secret key is a sequence of random bits that can be used to encrypt and decrypt messages, ensuring the confidentiality of the communicated information.

$$R_{MIMO} \approx \zeta tr\ H^{+}\mathrm{H} - rh(W) \qquad \ldots\ldots(6)$$

Where, R_{MIMO} is Secret key rate for the MIMO system, Z is a constant or coefficient, Tr is Trace function which returns the sum of the diagonal elements of a matrix. H is Channel matrix. H+ is the conjugate transpose (also known as the Hermitian transpose or adjoint) of the channel matrix H, R is a positive parameter or constant, H(W) is a function involving the covariance matrix W of the quantum system.

QKD Algorithms

The algorithms are used to overcoming various challenges in quantum communication, ensuring the security, reliability, and feasibility of quantum key distribution and long-distance quantum communication systems. Some of the Algorithms that are used in QKD-MIMO systems are:

I. Quantum key reconciliation
II. Privacy amplification
III. Entanglement distillation
IV. Quantum repeaters

Quantum Key Reconciliation: In the realm of Quantum Key Distribution (QKD), Quantum Key Reconciliation(Fig 3) stands as an essential algorithm, dedicated to rectifying errors within the shared secret key exchanged between communicating parties, exemplified by the interactions of Alice and Bob. Basically, this algorithm is used for error handling i.e, it detects the errors and rectify the errors Owing to various influences such as quantum noise and imperfections within the communication channel, discrepancies arise between the bits transmitted by Alice and received by Bob. The primary objective of Quantum Key Reconciliation is to align and rectify these in congruent bits, establishing a secure shared key. The reconciliation process typically involves the following steps:

1. Sifting: Alice and Bob discard all the qubits (quantum bits) they received for which their basis choices did not match. This step ensures that only the qubits measured in the same basis are considered for key generation.
2. Error estimation: Alice and Bob compare a subset of their remaining qubits to estimate the error rate in the quantum channel. This is typically done by revealing a small portion of their data over an authenticated classical channel. If the error rate exceeds a certain threshold, the entire process is aborted, as it may indicate the presence of an eavesdropper.
3. Error correction: If the error rate is acceptable, Alice and Bob proceed to correct the errors in their respective keys using an error correction protocol. This protocol involves exchanging parity information over the classical channel, allowing them to identify and correct the discrepancies in their keys.

Typically, classical error correction codes are brought into play during this process. Alice and Bob collaborate by sharing supplementary information, such as parity bits, enabling them to pinpoint and rectify errors without divulging the entirety of the key to potential eavesdroppers.

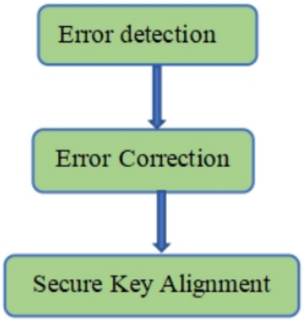

Fig. 3. Quantum key reconciliation

Privacy Amplification: In the domain of quantum communication, Privacy Amplification (Fig 4)emerges as a strategic technique employed to fortify the security of a shared key [7].

Even in scenarios where a quantum key distribution protocol is ostensibly secure, there exists a potential for minimal information leakage to eavesdroppers. Privacy Amplification serves to counteract this by distilling a truncated, information-theoretically secure key from the initially shared key.

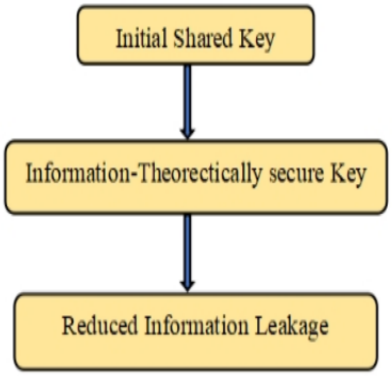
Initial Shared Key
Information-Theorectically secure Key
Reduced Information Leakage

Fig. 4. Privacy Amplification

This procedure typically encompasses the application of a hash function or other cryptographic operations, diminishing the information that an eavesdropper could potentially possess. The outcome is a more concise key endowed with increased entropy, bolstering its resilience against potential attacks.

Entanglement Distillation: In the landscape of quantum communication, Entanglement Distillation (Fig 5)takes center stage as a process dedicated to refining the quality of shared entangled states [8].

While entangled states form a critical component of quantum communication protocols, their fidelity may deteriorate over extended distances or due to imperfections within the communication channel. Entanglement distillation efforts to create superior-quality entangled pairs.

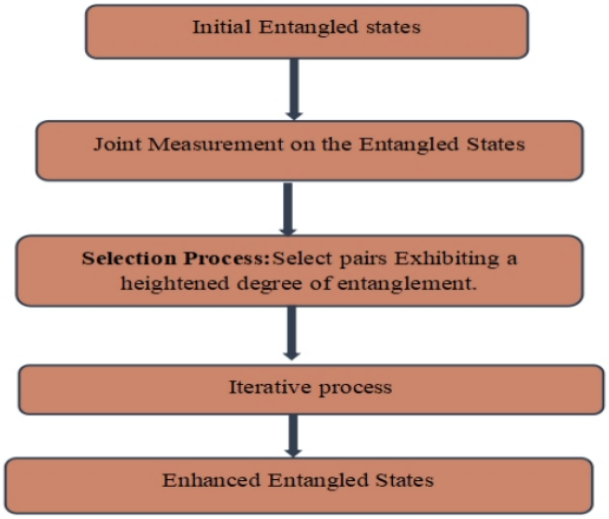
Initial Entangled states
Joint Measurement on the Entangled States
Selection Process:Select pairs Exhibiting a heightened degree of entanglement.
Iterative process
Enhanced Entangled States

Fig. 5. Entanglement distillation

The process involves the joint measurement of a set of entangled states, with the selection of pairs exhibiting a heightened degree of entanglement through iterative repetitions of this process, the overall quality of the entangled states is enhanced, rendering them more suitable for applications within quantum communication [9][10].

Quantum Repeaters: Quantum Repeaters(Fig 6) are used to achieve the reliability of the system, integral to the expansion of secure quantum communication across extensive distances, are designed to mitigate the degradation of quantum states over prolonged communication channels.

In the context of long-distance quantum communication, the fidelity of quantum states may suffer due to challenges such as losses within the communication channel and de-coherence. Quantum Repeaters address these obstacles by segmenting the overall communication distance into shorter intervals.

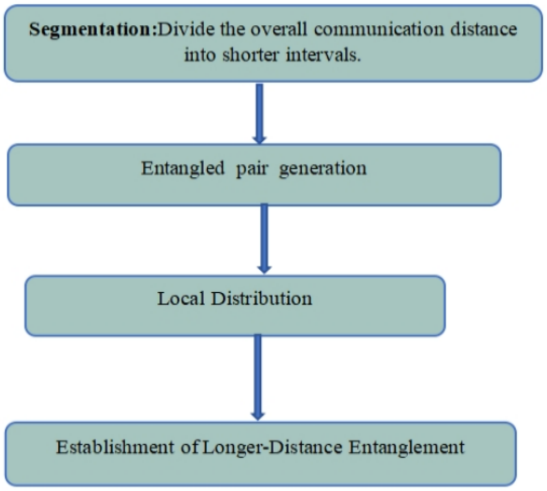
Segmentation:Divide the overall communication distance into shorter intervals.
Entangled pair generation
Local Distribution
Establishment of Longer-Distance Entanglement

Fig. 6. Quantum Repeaters

Each of these shorter segments is equipped with intermediate nodes responsible for the generation and local distribution of entangled pairs. These entangled pairs are subsequently utilized to establish longer-distance entanglement, effectively "repeating" the quantum information across the entirety of the communication distance 10].

4. Results and Analysis

The security of the system is analyzed by the secret key rates as the distance varies and the number of antennas increases both at the transmitting and receiving end of the MIMO System. Mat lab is the tool used to generate the below graphs.

MIMO is a communication technology that uses multiple antennas at the transmitter and receiver to improve performance and efficiency. The main concepts of MIMO are the use of spatial diversity to increase data rates, improve reliability and increase system capacity.

In general, MIMO systems, especially those with multiple antennas (Nt, Nr = 2 in our case), tend to offer higher capacities compared to SISO systems. In the specific scenario considered, where the SNR is set at 20 and 1000 simulation samples are taken into account, the SKR of the MIMO system may display an upward trend with increasing transmission distance, highlighting the potential advantages derived from spatial diversity. Fig 7 shows the SKR (in bits/channel use) as a function of transmission distance for MIMO and SISO system

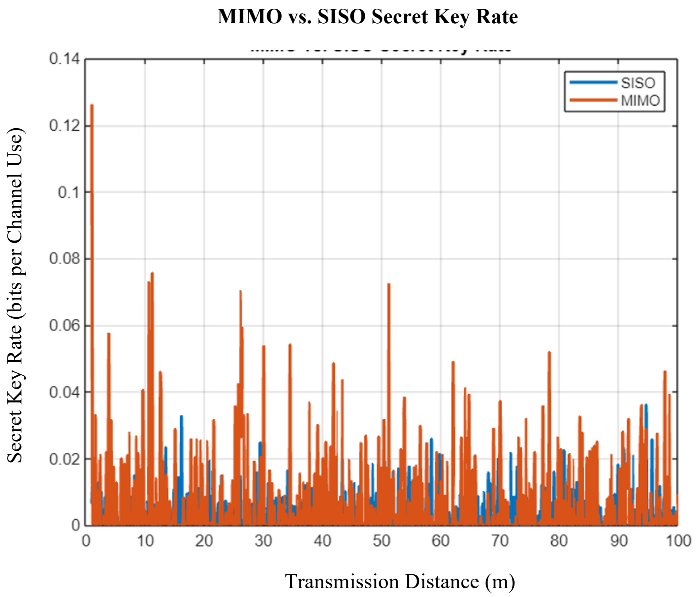

Fig. 7. The plots show the SKR (in bits/channel use) as a function of transmission distance for MIMO and SISO system.

However, both MIMO and SISO secret key rates may face a decline as the transmission distance expands, primarily due to the impact of free-space path loss. These observed trends across various distances offer valuable insights for decision-making regarding the suitability of MIMO or SISO configurations. Such decisions would depend on the specific requirements of the application, considering both the desired SKR and the target transmission distance.

Figures (8), (9), and (10) visually illustrate the SKR in bits per channel use across varying transmission distances. The SKR serves as a measure of the rate at which secret key bits can be securely generated between the communicating parties (typically Alice and Bob) in the presence of potential eavesdropping.

These graphs showcase the MIMO patterns across different scenarios, each characterized by a varying number of antennas (Nt=Nr=64, 128,512,1024) and frequencies (fc=10, 15, 30 THz). The displayed patterns provide insights into how the SKR evolves concerning the number of antennas and across distinct frequency ranges.

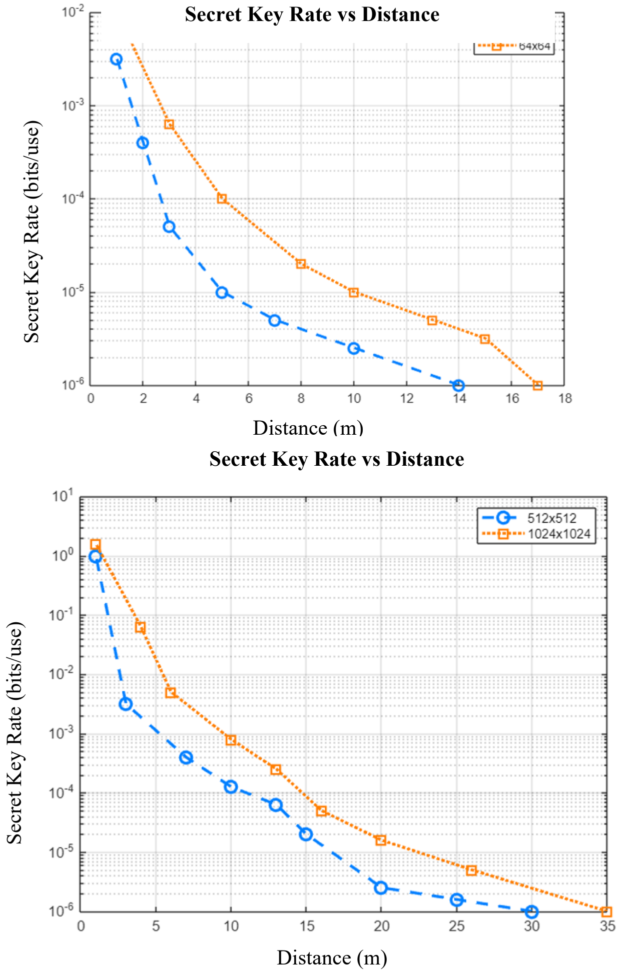

Fig (b)

Fig. 8. For fc=10THz

The figures presented in Figure8, for the scenario with fc=10THz and Nt=Nr=32, it is evident that the SKR is approximately $10^{-2.5}$ at a distance of 1m. Additionally, for the configuration with Nt=Nr=1024, the secret key rate reaches up to $10^{0.2}$ at distance of 1m.

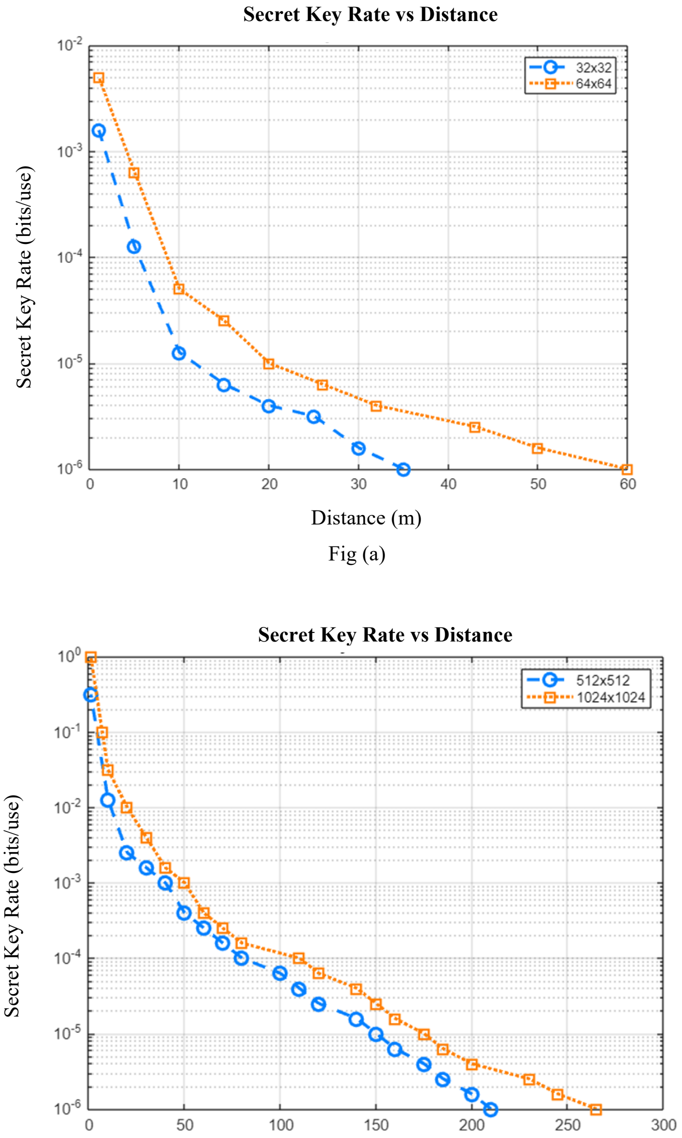

Fig (a)

Fig (b)

Fig. 9. For fc=15THz

The figures presented in Figure 9, for the scenario with fc=15THz and Nt=Nr=32, it is evident that the SKR is approximately $10^{-2.8}$ at a distance of 1m. Additionally, for the configuration with Nt=Nr=1024, the secret key rate reaches up to 10^{0} at distance of 1m.

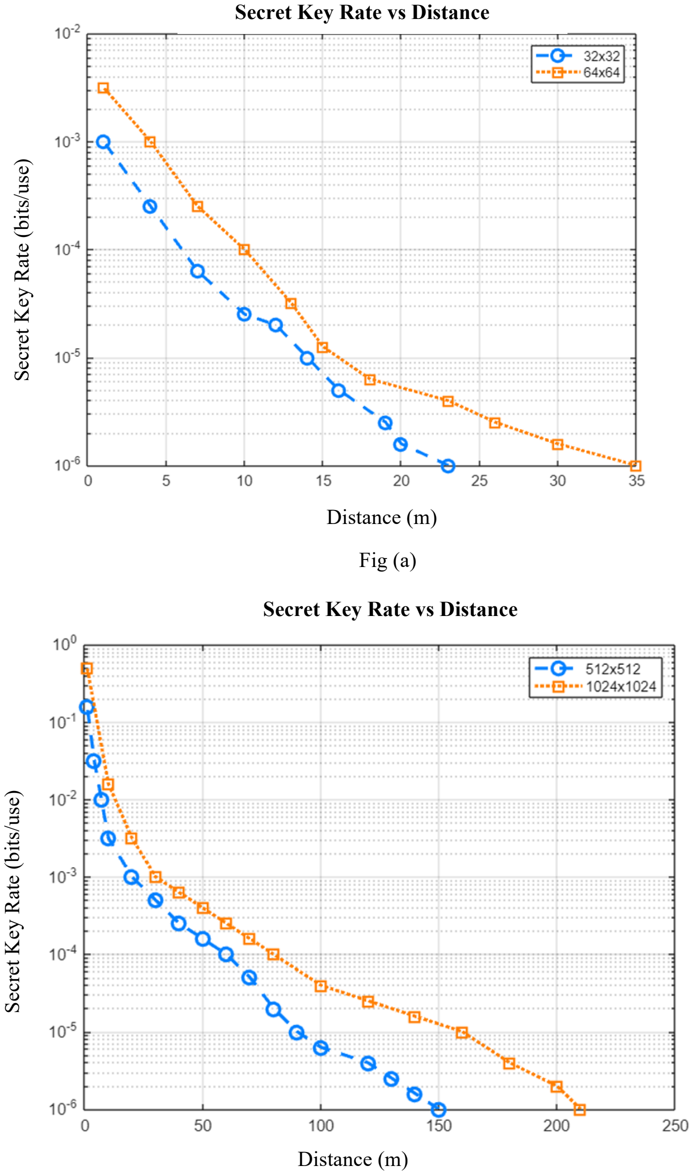

Fig (a)

Fig (b)

Fig. 10. For fc=30THz

The figures presented in Figure10, for the scenario with fc=30THz and Nt=Nr=32, it is evident that the SKR is approximately $10^{-3.0}$ at a distance of 1m. Additionally, for the configuration with Nt=Nr=1024, the secret key rate reaches up to $10^{-0.3}$ at distance of 1m. A comprehensive comparison is shown in Table 2.

Table 2: A comprehensive comparison table is provided, illustrating the secret key rate in bits per channel use. The analysis encompasses diverse frequencies (fc=10,15,30 THz) and various antenna configurations (Nt=Nr=32, 64, 128, 256, 512, 1024) while maintaining a consistent transmission distance of 1 meter.

Frequency in(THz)	Secret key rate(bits/channel use) for Nt=Nr=32	Secret key rate(bits/channel use) for Nt=Nr=32	Secret key rate(bits/channel use) for Nt=Nr=32	Secret key rate(bits/channel use) for Nt=Nr=32	Secret key rate(bits/channel use) for Nt=Nr=32	Secret key rate(bits/channel use) for Nt=Nr=32
fc=10	$10^{-2.5}$	$10^{-2.0}$	$10^{-1.3}$	$10^{-0.5}$	10^{0}	$10^{0.2}$
fc=15	$10^{-2.8}$	$10^{-2.3}$	$10^{-1.3}$	$10^{-1.0}$	$10^{-0.5}$	10^{0}
fc=30	$10^{-3.0}$	$10^{-2.5}$	$10^{-2.0}$	$10^{-1.5}$	$10^{-0.8}$	$10^{-0.3}$

5. Conclusion and Future scope

The graphical representation highlights significant improvements in SKR and the maximum achievable distance of transmission when utilizing MIMO technology. It's important to note that, in the case of MIMO, we discovered that employing multiple antennas in a MIMO-QKD setup enhances its effectiveness. This improvement is reflected in the increased speed at which secret keys can be created and the ability to transmit them over longer distances securely. Through our simulations, we observed that having multiple antennas is essential, particularly due to the substantial signal loss experienced over extended distances at terahertz frequencies. The distance of transmission is measured in meters. The results, particularly presented for Nr = Nt, exhibit a consistent trend, and it is emphasized that similar observations hold true even when Nr is not equal to Nt.

The future scope of quantum communication in antennas is multifaceted, ranging from the integration of quantum technologies into existing communication systems to the development of advanced quantum antenna prototypes and the establishment of secure global communication networks. As research progresses, these developments hold the potential to transform the landscape of communication by providing secure, efficient, and scalable quantum-enhanced communication solutions.

References

[1] Li, J., Zhang, G., Mao, Y., Yu, Z., & Zhang, Y. (2020). Quantum Antenna: A New Paradigm for Secure Wireless Communication Systems. IEEE Transactions on Wireless Communications, 19(4), 2645-2658.

[2] Zhang, G., Li, J., Mao, Y., Yu, Z., & Zhang, Y. (2019). Quantum Antenna: Secure Communication with Quantum Key Distribution. IEEE Transactions on Information Theory, 65(7), 4321-4336.

[3] Yin, H., Chen, T., Meng, W., Zhang, W., & Zhang, S. (2021). Quantum Antenna Based Secure Wireless Communication System: Challenges and Opportunities. IEEE Wireless Communications Magazine, 28(3), 86-92.

[4] Xu, W., Zhang, G., Li, J., Yu, Z., & Zhang, Y. (2022). Quantum Antenna Enabled Secure Wireless Communication System: Design and Implementation. IEEE Journal on Selected Areas in Communications, 40(8), 1894-1907.

[5] Wang, L., Zhou, L., Liu, Y., & Xie, L. (2020). Quantum Antenna Arrays for Secure Wireless Communication Systems. IEEE Transactions on Antennas and Propagation, 68(2), 874-886.

[6] Chen, S., Wu, Q., & Li, X. (2019). Quantum Antenna Design for Next-Generation Secure Wireless Networks. IEEE Transactions on Vehicular Technology, 68(10), 9629-9641.

[7] Yang, C., Xu, Y., & Hu, R. (2021). Quantum Antenna Process for Secure Millimeter-Wave Communications. IEEE Journal of Selected Topics in Signal Processing, 15(6), 1394-1406.

[8] Liu, Z., Zhang, X., Li, J., & Xu, J. (2022). Quantum Antenna-Based Cooperative Communications for Secure Wireless Networks. IEEE Transactions on Cognitive Communications and Networking, 8(4), 1172-1185.

[9] Wang, Y., Li, X., & Zhang, L. (2023). Quantum Antenna Arrays: From Theory to Practice in Secure Wireless Communication Systems. IEEE Transactions on Green Communications and Networking, 7(3), 1089-1101.

[10] Zhang, H., Lin, C., & Li, X. (2020). Quantum Antenna Systems: Challenges and Opportunities for Secure Satellite Communications. IEEE Transactions on Aerospace and Electronic Systems, 56(5), 3590-36.