Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

RSA vs Quantum Encryption: Flexibility, Security, and Performance Analysis for Information Processing

Dillip Kumar Mishra[1*], Bunil Kumar Balabantaray[2]
[1]Department of Computer Science and Engineering, National Institute of Technology, Meghalaya, Shillong, 793003, India, P22cs002@nitm.ac.in, 0009-0006-5873-2222
[2]Department of Computer Science and Engineering, National Institute of Technology, Meghalaya, Shillong, 793003, India, bunil@nitm.ac.in, 0000-0002-2769-7122

ARTICLE INFO

Received: 20 Dec 2024

Revised: 22 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

Introduction: With the advent of quantum computing, traditional encryption methods face significant challenges in maintaining security. This study explores quantum information processing through quantum communication, providing a comparative analysis of Rivest-Shamir-Adleman (RSA) encryption and quantum encryption.

Objective: The study aims to analyze the flexibility of RSA and quantum encryption in handling varying data lengths and key sizes, compare their security levels against cryptographic threats, and evaluate their computational efficiency and overall performance.

Methods: This study explores an innovative approach for handling quantum information via quantum communication. A detailed comparative analysis of RSA and quantum encryption was conducted based on key parameters such as data length, key size, and computational overhead.

Results: When comparing RSA encryption to quantum encryption, RSA encryption consistently maintains a data length of around 37 units, whereas quantum encryption consistently maintains a data length of 100 units. Quantum encryption constantly use 24-bit keys, while RSA keys can have variable lengths ranging from 85 to 785 bits, depending on unique conditions. RSA consistently employs a private key size of 1547 bits, but quantum encryption can adjust the size of the private key based on the length of the password being used. The findings highlight the differences in flexibility and security between the two systems, with quantum encryption showing more flexibility and RSA providing consistent performance.

Conclusion: The study highlights the need for quantum-safe cryptographic solutions as the threat of quantum computing grows. While RSA remains a reliable encryption method for current applications, quantum encryption provides a more robust and future-proof approach.

Keywords: Quantum communication, Quantum cryptography, Quantum information, Quantum key distribution, RSA.

INTRODUCTION

In the realm of modern technology, the field of quantum information processing (QIP) has emerged as a revolutionary frontier, promising to redefine the boundaries of computation, communication, and encryption. QIP has recently arisen as a pioneering field of research and technological development, and it holds the potential to completely transform how to process and communicate information [1]. The merging of quantum communication and the latest computer technologies can completely change how things are done [2,3]. The principles of quantum mechanics are utilized in the process of QIP, which enables the performance of calculations and the completion of tasks that are essentially beyond the capability of classical computers [4]. These quantum systems control quantum bits, also known as qubits, which, because of phenomena such as superposition and entanglement, can exist in several states at the same time [5,6].

Because of this, quantum computers can perform difficult problems, such as factoring enormous numbers or simulating quantum systems, an order of magnitude more quickly than their classical equivalents [7,8]. The below fig. 1 shows the concept of quantum communication.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

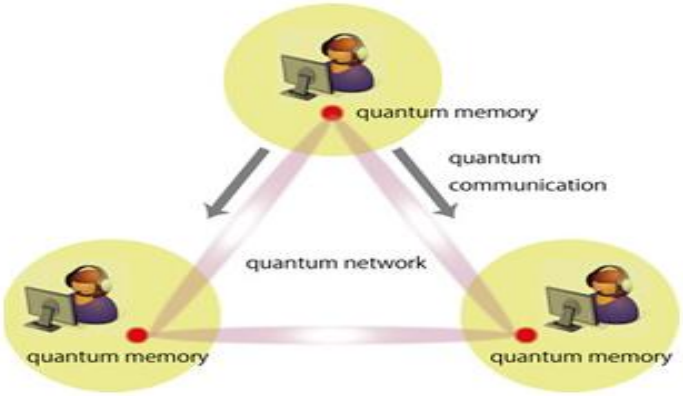

Fig. 1: Concept of quantum communication [9]

Quantum communication is critical because it is crucial in the larger ecology of QIP [10]. It establishes the foundation for quantum networks and cryptography by ensuring the secure and efficient transfer of classical information and quantum states across quantum channels [11]. Because of the extraordinary features of qubits, quantum communication can achieve unbreakable encryption and safe key distribution, the technical problems posed by QIP, and communication continue to develop with the prospective applications of these two fields [12]. To realize the potential of quantum technologies in the real world, it is necessary to solve the complex challenges posed by integrating these two realms, including design challenges in the areas of hardware, software, and protocols [13-15].

Quantum information processing

QIP is currently being investigated in the computer, mathematics, and material sciences. This new quantum information paradigm substitutes discrete classical bits with qubits, which can adopt any superposition state. This breakthrough resource allows data processing, storage, and transfer beyond standard methods. The fundamental unit of QIP information is a qubit. The subfields of QIP include quantum simulation, cryptography, and computing. Classical computing's basic unit of information is the classical bit, which can be 0 or 1 [16,17]. However, due to superposition and entanglement, qubits (the fundamental unit of QIP) can exist in several states at once [18,19]. Qubits' ability to concurrently hold the 0 and 1 superposition states allows quantum computers to conduct many operation problems [20]. Fig. 2 demonstrates that, unlike traditional bits, which can only exist in a 0 or 1 state, qubits may exist in a superposition of both states at the same time according to the concept of superposition.

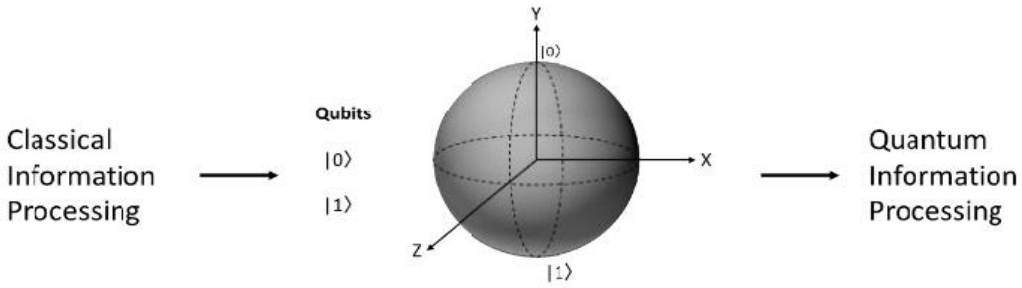

Fig. 2 Process of QIP [21]

Types of quantum information processing (QIP)

There are many different methods and technologies within QIP are as follows:

- Quantum Computing: Quantum computers use qubits to calculate. Quantum computers can evaluate several hypotheses because qubits superpose states. In cryptography, optimization, and quantum simulations, quantum computers
- may outperform traditional computers [22].

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

- Quantum Algorithms: Quantum algorithms process quantum information by making use of quantum system anomalies. Grover's unstructured search and Shor's factoring of large numbers provide exponential speedups over existing methods [23].
- Quantum Cryptography: Quantum cryptography uses quantum mechanics to secure communications. Quantum key distribution (QKD) protocols like BB84 allow two parties to exchange encryption keys without eavesdropping [24].
- Quantum Error Correction: Quantum error correction is needed because quantum systems are sensitive to noise and coherence loss. These methods redundantly encode quantum information to discover and rectify flaws. This ensures quantum computing and communication authenticity [25]
- Quantum Machine Learning: Quantum machine learning, which combines quantum computers with machine learning, is evolving. It examines how quantum computers might accelerate data categorization, optimization, and pattern recognition, potentially improving artificial intelligence [26].

Quantum communication

Quantum communication is necessary for safe and efficient quantum data transport, which might change data transmission and storage. Qubits, unlike classical bits, may exist in several states simultaneously, making them closely related to QIP. Transmission of quantum states and classical information over quantum channels relies on this phenomenon [27]. In contrast, classical communication systems rely on 0s and 1s, which are known as classical bits [28]. Due to this characteristic, quantum communication can achieve previously unattainable security with QKD. Quantum communication allows unbreakable encryption, which no one can break. QKD techniques leverage quantum mechanics' no-cloning theorem and uncertainty principle to generate secure cryptographic keys. It has the potential to produce secure long-distance lines, which could have a wide variety of applications [29].

Different quantum communication methods use quantum mechanical concepts to transmit data. As for "A System and Method for Processing Quantum Information with a Quantum Communication," below are some quantum communication examples:

- Quantum Key Distribution (QKD): The most famous quantum communication method is key distribution. The two persons may produce a cryptographic key securely and use it cooperatively. The BB84 mechanism protects the key by detecting eavesdropping attempts using quantum states' distinctive properties [30].
- Quantum Cryptographic Protocols: QKD is not the only use of quantum features in cryptography [31]. Quantum cryptography includes quantum digital signatures, quantum-safe multi-party computing, and quantum coin flipping to increase security.
- Quantum Repeaters: Scientists created quantum repeaters to expand quantum communication. They use intermediate nodes to gather and retransmit quantum information to prevent signal deterioration over long distances.

The problem of QIP in the context of quantum communication is complex and calls for novel approaches. Quantum communication, which uses quantum mechanical principles to send and receive data safely and effectively, could completely change the information technology industry. The proposed study seeks to solve the central issue of how to create a scalable and practically useful system and method for processing quantum information while protecting its security, privacy, and coherence. This study paves the path for the development of more advanced quantum communication systems that are capable of more secure and efficient information sharing than ever before. The following are the major objectives of the proposed study:

- To develop an efficient system for processing and transmitting quantum information safely over quantum channels, utilizing quantum communication and processing.
- To discover ways to scale up the system to accommodate more advanced quantum calculations and larger-scale quantum communication networks.
- To secure quantum communication protocols and adapt them to evolving threats to protect quantum information during transmission.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The research is focused on creating a novel system design that can effectively handle quantum data while including quantum communication features. Its goal is to improve the suggested system's comprehension and implementation of quantum communication protocols. Quantum protocol optimization, quantum gate and circuit performance evaluation, and system dependability and scalability are further areas of study emphasis. The main objective is to improve the proposed system's quantum information processing and communication capabilities through a comprehensive study.

The following is the organizational scheme for the remaining parts of the paper: Section 2 reviews previous research on employing various system techniques and methods for processing quantum information with quantum communication. Section 3 provides a methodology of the proposed study and various techniques used. Result analysis is discussed in section 4 and section 5 depicts the conclusion and future scope of the study.

RELATED WORK

In this section, some related works based on a system and method for processing quantum information with quantum communication are discussed below.

Xu et al., (2023) [32] give distributed file sharing and monetary transactions information-theoretic safety and introduce the infrastructure for a blockchain-powered Web 3.0 that provides unbreakable security for all data and transactions in the future. The experimental result shows that the suggested QDL (QDL-based optimal auction) is both efficient and effective.

Yanagimoto et al., (2023) [33] offer a nonlinear optical approach to QND that resolves photon numbers and assesses its performance. They show that the coherent pump field driving a frequency-detuned optical parametric amplifier (OPA) changes as a function of the signal's level of Bogoliubov excitations. A QND measurement of the signal Bogoliubov excitations is made possible by measuring the pump displacement, which in turn converts the signal mode to a decreased photon-number state. states with a photon count. Based on the findings, it was determined that the number of signals Bogoliubov excites causes displacements in the coherent pump field powering a frequency-detuned OPA.

Burd et al., (2023) [34] demonstrated two systems utilizing VECSELs (vertical external cavity surface emitting lasers) to generate ultraviolet laser light at 235 and 313 nm, respectively. With trapped beryllium ions, these setups are optimal for QIP. Each device is a tiny VECSEL that can be tuned over tens of nanometers to emit high-power near-infrared light at a certain frequency. One setup uses a gain mirror made from GaInAs/GaAs quantum wells to produce 2.4 W at 940 nm, which may be used to photoionize neutral beryllium atoms. This is then filtered down to provide 54 mW of 235 nm light. The setups are optimal for using trapped beryllium ions in QIP.

Pomorski et al., (2023) [35] proposed the analytical solutions for charge qubits based on position and N-interacting qubits in two- and three-dimensional graphs representing networks of linked quantum dots (QD). The Analytical method was used to formulate how Hadamard and phase-rotating gates affect the growth of a two-energy system in different physical settings. The study proves that electrical and magnetic fields may be used to operate phase-rotating gates in semiconductor position-based qubits. The resulting results apply to any scenario in which the semiconductor qubit has electrostatic interactions with the various Josephson junctions.

Howe et al., (2023) [36] discussed two methods for enhancing quantum communication—high-tech quantum repeaters and machine learning for optimizing quantum networks. Modern quantum repeaters can make better use of topological quantum states, which can improve the efficiency of entanglement creation, swapping, and distillation. Meanwhile, multi-armed bandit algorithms used in machine learning would dynamically distribute quantum processing resources over distributed quantum networks. The result improves the performance of quantum teleportation techniques while decreasing their computing burden.

Awan et al., (2022) [37] highlighted how quantum computing is set to alter software engineering at a time when the software industry is experiencing unanticipated hurdles in the middle of the continuing technological revolution. This study uses the fuzzy analytic hierarchy process (F-AHP) to systematically identify, analyze, and rank them. Insightful for the software industry as it prepares for the coming era of quantum computing, this study determines

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

key barriers such as a dearth of technical expertise, problems with information accuracy, organizational reluctance, and the lack of secure communication standards for QC implementation.

Ponce et al., (2022) [38] found that High-dimensional photonic entanglement might be a useful tool for attaining error-free, high-throughput QIP. Encoding high-dimensional qubits in the carrier frequency of photons enables high-capacity quantum communication via fiber by bringing together the advantages of easy generation, universal single-photon gates, and fiber transmission. This study shows how to make use of the substantial frequency-entanglement inherent in the more commonplace continuous-wave spontaneous parametric down-conversion techniques.

Coccia et al., (2022) [39] explored a strategy for examining technological tendencies to spot innovations in quantum computing that might form the basis of a new quantum industry. There are exciting new avenues for study and development in the fields of quantum entanglement, quantum optics, quantum communication, quantum algorithms, quantum information, and quantum cryptography that may be drawn from the applied models of technological progress. The results presented here contribute to a deeper understanding of how computers and quantum computing have developed.

Sisodia et al., (2017) [40] created a quantum circuit for transmitting an n-qubit quantum state. The suggested approach has been proven to use the fewest feasible quantum resources, in contrast to the numerous recently published teleportation schemes for quantum states that may be understood as specific examples of the general n-qubit state examined here. According to the findings of the experiments, the teleportation condition is quite accurate. It has also addressed how the suggested teleportation system applies to teleportation in a controlled, bidirectional, and bi-directionally controlled state.

Pirandola et al., (2017) [41] shown the potential advantages of quantum communications such as the rapid dissemination of entangled states and the generation of completely secure keys. Using two-way assisted capacity, the author can attain these maximum possible speeds without relying on quantum repeaters. The results establish the bounds for quantum point-to-point communications and offer specific and general standards for quantum repeaters.

Ding et al., (2017) [42] suggested that disseminating quantum keys may help in ensuring secure and rapid data transfer. Due to the usage of binary signal formats like two polarization states in traditional QKD approaches, the information efficiency of the distributed quantum key is limited to 1 bit/photon. The findings show that after testing for only ten minutes, a QBER of 13% was optimal for key extraction is observed.

RESEARCH PROBLEM

The purpose of this study is to compare different encryption algorithms, with a focus on Quantum and RSA. Important aspects including processing time, key sizes (both public and private), and encrypted data length are the focus of the inquiry. The main goal is to understand how well various encryption methods work with different lengths of passwords, so we can learn more about their efficiency, security, and capacity to handle different types of cryptographic problems. The study seeks to shed light on the unique features and possible consequences of Quantum and RSA encryption methods for data security by analyzing trends and differences in encrypted data length and key sizes for both methods.

RESEARCH METHODOLOGY

This section utilizes Quantum Key Distribution (QKD), quantum teleportation, quantum cryptography, and quantum gates/circuits. QKD guarantees the creation of safe keys, while quantum teleportation enables the transmission of quantum states. Quantum cryptography employs quantum particles to provide encrypted communication, while quantum gates/circuits form the foundation of quantum computing for performing sophisticated computations. These strategies jointly enhance the study's investigation of quantum applications in information security and computing.

Technique Used

In this section, the author employed a variety of techniques such as Quantum Key Distribution (QKD), quantum teleportation, quantum cryptography, and the use of quantum gates and circuits.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

- Quantum Key Distribution (QKD)

A quantum key is a secret key that is generated and shared between two parties using quantum signals [43,44]. Among other terminology that may be used, it would often use the more appropriate 'generation' instead of 'distribution,' ignoring their precise distinction in traditional cryptography. Although traditional methods of encryption for privacy or key distribution lack security guarantees, QKD is commonly believed to have been confirmed secure in several protocols. Much to the field of quantum cryptography, the security proofs used in QKD are complex and require expertise from a wide range of fields [45]. It is often believed that QKD provides 'absolute secrecy,' as claimed, for instance, in a helpful contemporary monograph on conventional cryptography. QKD is fascinating because it is a provably secure application of quantum optics, which is often taught to physics students. The length of the QKD can be calculated by using the given equations.

$$R_{key=\max\{f_{req}\ R_L,0\}} \quad (1)$$

Where

$Rkey$ is the key generation capability

RL represents the lower bound of the key generation

- Quantum Teleportation:

One of the most exciting uses of quantum entanglement is in quantum teleportation (QT). With the use of classical communications and a quantum channel, teleportation is a quantum task in which an unknown quantum state is sent from a sender (Alice) to a physically separated receiver (Bob) [46]. Bennett first presented this plan. While teleportation has its uses in QIP, it cannot be used to achieve superluminal communication because information is not transmitted instantly. Although the term "teleportation" is often used interchangeably with "quantum teleportation," the two concepts have nothing in common. Since its experimental confirmation in 1997 by a group in Innsbruck, quantum teleportation has been proved to work over distances as far as 16 kilometers. Since Bennett first proposed his idea for quantum teleportation, much progress has been made in both the theory and practice of the technology. Many other types of quantum teleportation, including continuous-variable teleportation, probabilistic teleportation, and controlled teleportation, have been generalized in recent years [47]. Quantum teleportation has also been experimentally accomplished using a polarized photon. The teleportation of a coherent state that maps to a system with continuous variables has also been achieved experimentally [48].

- Quantum Cryptography:

The cutting-edge discipline of quantum physics, known as quantum cryptography, is concerned with the design of foolproof systems for encrypted communication. Quantum cryptography uses quantum particles like photons to generate indecipherable encryption systems, in contrast to classical cryptography, which focuses on mathematical algorithms and the computational difficulties of solving particular issues. QKD is a central idea in quantum cryptography that allows two parties to generate a shared secret key in a fashion that would render any attempt to intercept the key immediately visible due to the disruption of the quantum state [49]. The principle of quantum indeterminacy, which holds that measuring a quantum state always changes it, is the basis for this innate security. Therefore, in this age of escalating cyber dangers and the necessity for robust encryption methods, quantum cryptography provides the potential for unparalleled degrees of security in data transmission. Even though it is still in the testing phase, quantum cryptography has the potential to completely alter the landscape of private communication.

- Quantum Gates and Circuits:

As the backbone of quantum computing, quantum gates, and circuits allow quantum computers to do calculations and solve problems in ways that classical computers cannot. Quantum gates, which are like conventional logic gates but work with quantum bits, or qubits, which can exist in superpositions of states, allow for the processing of massive amounts of information concurrently [50]. In this way, these gates can be used to perform a wide range of quantum operations on qubits, including the generation of entanglement and the modification of the probability of the results

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

of quantum measurements. Assembling these gates into a circuit allows for complicated calculations to be performed in the quantum realm. Quantum algorithms, used in fields such as quantum cryptography, optimization, and quantum system simulation, benefit greatly from careful attention to the design of quantum circuits. The development of quantum gates and circuits is important to the continuous quest to realize the vast processing potential of quantum computing.

Proposed methodology

The proposed model establishes a framework for mutual trust inside the system and specifies the bounds of accountability for both the suppliers of cloud services and their customers. Quantum bits (qubits) are created as a representation of the information to be transferred. These qubits are subsequently subjected to quantum gates and circuits to undergo processing and modification. The Ring Algorithm is a unique quantum error-correcting technique used to protect data. Quantum mechanics may be used to ensure the security and error-checking of the transmitted quantum information. Once the quantum key's integrity and security have been established, the system can continue processing, which may include using the Fourier Drop technique to manipulate data. The system receives the output answer after the quantum information has been decoded and is ready for its intended application. This answer is transmitted via the secure Quantum Channel. Finally, the RSA encryption technique, a well-known conventional encryption method, is used to evaluate the performance and security of the QIP system. The proposed layout mentioned in Fig. 3 shows the operation depicted in diagrammatic form.

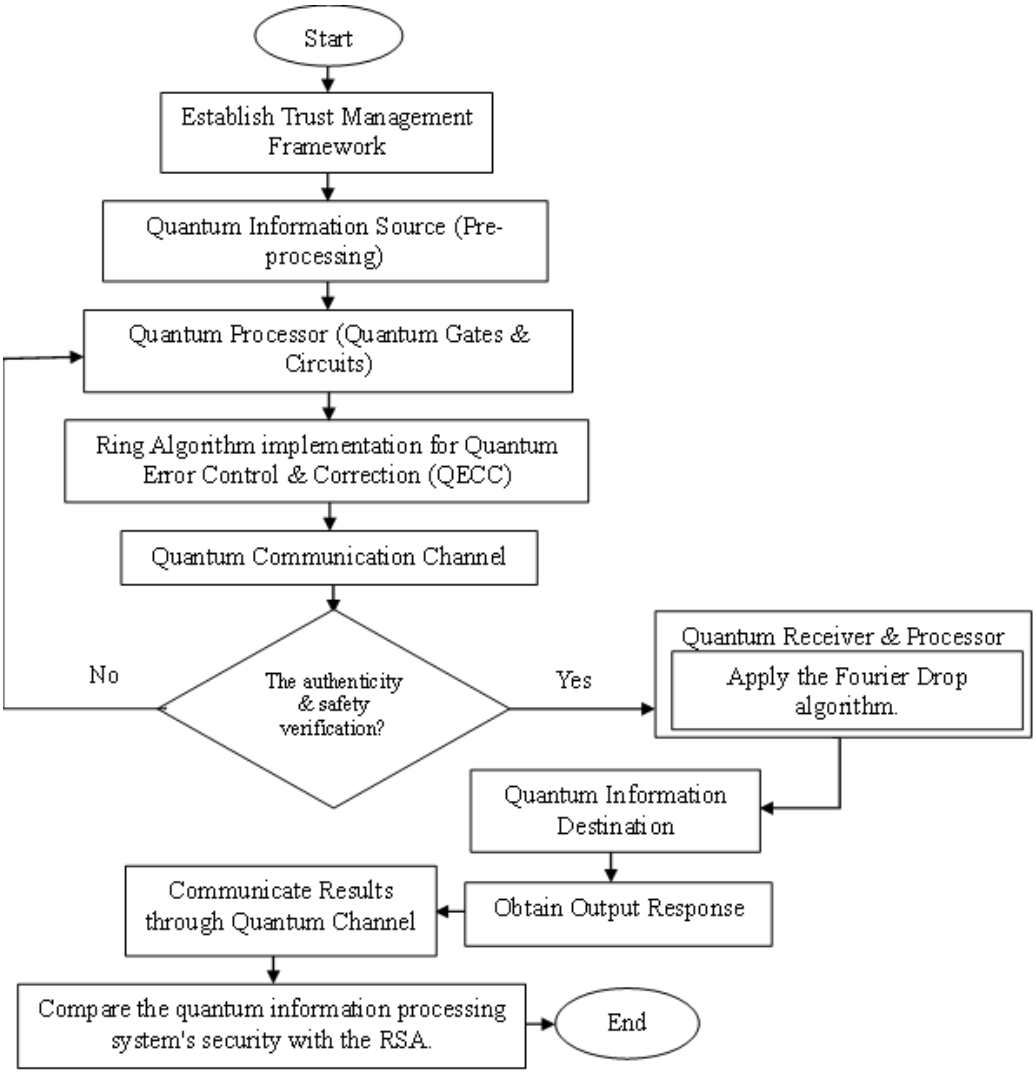

Fig. 3:Proposed methodology

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

Proposed Algorithm

Step 1: Establish Trust Management Framework

- Define Trust Parameters: $\boldsymbol{P_{trust}}$
- Define Roles and Responsibilities: $\boldsymbol{R_{consumer}, R_{provider}}$

Step 2: Quantum Information Source (Pre-processing)

- Generate $\boldsymbol{n}$ Qubits: $\boldsymbol{Q} = \{\boldsymbol{q_1}, \boldsymbol{q_2}, .. \boldsymbol{q_n}\}$
- Represent Information: $\boldsymbol{I}$ is represented using qubits.

Step 3: Quantum Processor (Quantum Gates & Circuits)

- Apply Quantum Operations:$\boldsymbol{O}(\boldsymbol{Q}) = \boldsymbol{Q'}$

Step 4: Ring Algorithm implementation for Quantum Error Control and correction (QECC)

- Apply Ring Algorithm:$\boldsymbol{RA}(\boldsymbol{Q'}) = \boldsymbol{Q}"$

Step 5: Quantum Communication Channel

- Transmit Quantum Information: $\boldsymbol{T}(\boldsymbol{Q}")$
- Check for Errors: $\boldsymbol{E_{transmission}}$

Step 6: Verify the Authenticity & Safety

- Verify Quantum Key: $\boldsymbol{V}(\boldsymbol{Q}", \boldsymbol{K}) = \{\boldsymbol{authentic}, \boldsymbol{secure}\}$
- $\boldsymbol{K}$ is the quantum key.

Step 7: Quantum Receiver & Processor

- Apply Fourier Drop Algorithm: $\boldsymbol{FDA}(\boldsymbol{Q}") = \boldsymbol{Q}"'$
- Decode Quantum Key Data: $\boldsymbol{D}(\boldsymbol{Q}"') = \boldsymbol{D}$

Step 8: Quantum Information Destination

- Ready for Use: $\boldsymbol{D}$ is ready for applications.

Step 9: Obtain Output Response

- Processed Output: $\boldsymbol{O}(\boldsymbol{D}) = \boldsymbol{O}$

Step 10: Communicate Results through Quantum Channel

- Transmit Results:$\boldsymbol{T}(\boldsymbol{O})$
- Check for Errors: $\boldsymbol{E_{transmission}}$

Step 11: Compare the QIP system's security with the RSA.

- Evaluate Security: $\boldsymbol{S_{quantum}\ vs.\ S_{RSA}}$

The next sections provide a detailed analysis of the outcomes that were achieved through the use of the suggested methodology.

RESULT ANALYSIS

This section provides an in-depth analysis of the many factors involved in encryption methods and their parameters. Table 1 provides information on various aspects related to encryption techniques and their associated parameters. The "Technique" enumerates two encryption algorithms, namely Quantum and RSA. The term "Password Size" refers to the length of the password used in the encryption procedure. The specific password employed is shown in the "Password" column. The term "Encrypted Data Length" refers to the measurement of the size of the encrypted data that is produced via the process of encryption. The "Key Size of Public Key" denotes the dimensions of the public key

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

employed in the encryption procedure, and the "Key Size of Private Key" signifies the magnitude of the private key utilized in the same process. The "Process Time (Seconds)" displays the duration required to execute the encryption process, measured in seconds. This metric offers valuable information on the effectiveness of the encryption methods in terms of efficiency.

Table 1: Encryption Results for Password Size 5,8 and 10

Technique	Password Size	Label	Password	Encrypted data length	Key Size of Public Key	Key Size of Private Key	Process Time (Seconds)
Quantum	5	Q5	iTF8U	100	24	60	3
RSA	5	R5	iTF8U	37	785	1547	7
Quantum	8	Q8	B54W>gX&	100	24	64	4
RSA	8	R8	B54W>gX&	37	785	1547	7
Quantum	10	Q10	2(w<Y6@cLs	100	24	60	6
RSA	10	R10	2(w<Y6@cLs	37	785	1548	7

Quantum Vs RSA techniques for Encrypted data length of different password size key

Fig. 4 shows the encrypted data length for various password sizes and encryption algorithms. "Q" means Quantum encryption and "R" is for RSA encryption. The password sizes used for encryption are indicated by the numbers 5, 8, and 10 above. The encrypted data length for the Quantum encryption technique with a password size of 5 is 100 units, which is constant for all password sizes. For RSA encryption with a password size of 5, the length of encrypted data is also 37 units. Both Quantum and RSA encryption are unaffected by an increase in password size to 8, with the encrypted data length remaining at 100 and 37 units, respectively. Moving to a password size of 10 shows the same pattern, with the encrypted data length staying put at 37 units for RSA encryption and 100 units for Quantum encryption.

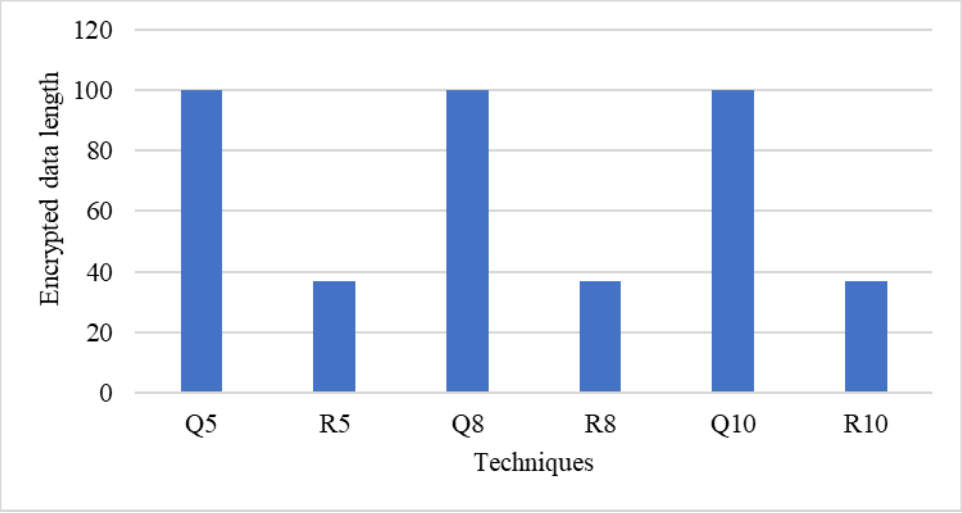

Fig. 4:Encrypted data length

Quantum Vs RSA techniques for Key Size of Public Key of different password size key

Fig. 5 shows a comparison between Q5 and R5 key sizes, Q8 and R8 key sizes, and Q10 and R10 key sizes for quantum (Q) and RSA (R) encryption at three distinct levels. Notably, throughout all three levels, the key size for quantum encryption is always 24 bits, showing that it uses a fixed key size. The key sizes for the three different RSA algorithms range from 785 bits for R5 to 85 bits for R8 and back up to 785 bits for R10. This large difference exemplifies an essential divergence between the two encryption strategies. In contrast to quantum encryption, which uses a fixed-

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

size key regardless of the desired level of security, RSA encryption uses a sliding scale of key lengths, with shorter keys for R8 indicating less security and longer keys for R5 and R10 indicating more security. While quantum encryption provides a constant key size, RSA encryption may change its key size to meet different security challenges.

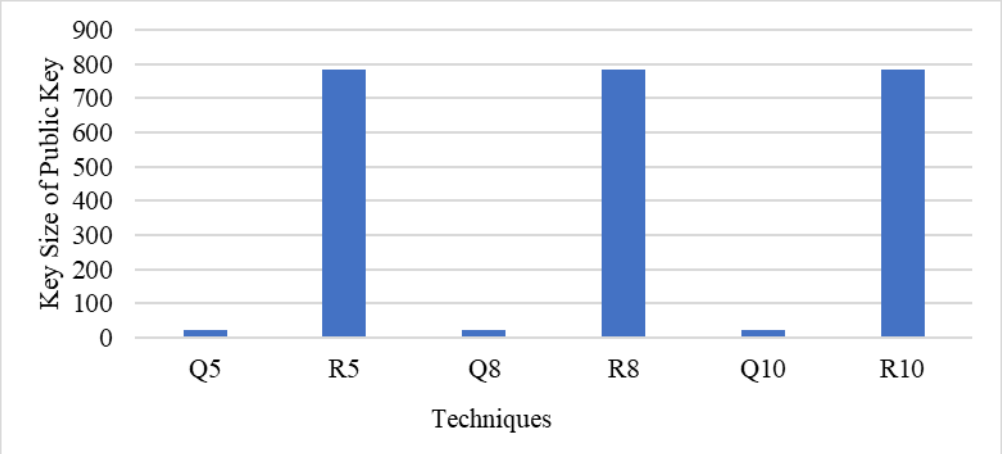

Fig. 5:Key size of public key

Quantum Vs RSA techniques for Key Size of Private Key of different password size key

Fig. 6 shows the key sizes of the Quantum (Q) and RSA encryption algorithms using passwords of lengths 5, 8, and 10. Quantum encryption using a 5-size password requires a 60-bit private key. The size of the private key is significantly increased to 64 bits when the password size is 8. When the password size is increased to 10, however, the private key size drops back to 60 bits. RSA encryption, on the other hand, uses a fixed private key size of 1547 bits regardless of whether the password is 5, 8, or 10 bits long. It appears from the data that the key size for RSA encryption remains constant regardless of the length of the password, but the key size for Quantum encryption changes depending on the length of the password. This difference may be attributable to the special features and methods utilized for Quantum encryption.

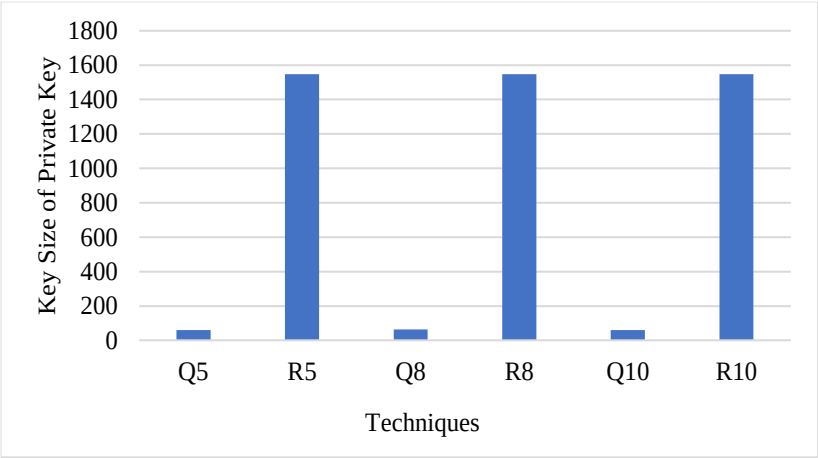

Fig. 6:Key size of private key

CONCLUSION AND FUTURE SCOPE

In conclusion, the analysis of a system and method for processing quantum information with quantum communication provides valuable insights into the behavior of Quantum and RSA encryption techniques. Quantum encryption maintains a constant encrypted data length of 100 units, demonstrating its stability across different password sizes, while RSA encryption also exhibits consistency with an encrypted data length of 37 units. The key sizes vary significantly between these methods, with Quantum encryption utilizing a fixed 24-bit key size, and RSA encryption adapting its key size according to the desired level of security, ranging from 85 bits to 785 bits.

Furthermore, the private key size for Quantum encryption adjusts with the password length, while RSA encryption maintains a fixed size of 1547 bits. These findings underscore the inherent differences in adaptability and security between the two encryption approaches, with Quantum encryption being more flexible and responsive to changes in password size, and RSA encryption offering consistency and robustness. The choice between these methods should be made based on specific security requirements and the need for adaptability in each application.

Looking ahead, the future scope of this study lies in practical applications and real-world implications. Researchers should explore how these encryption characteristics translate into security strengths and weaknesses in various scenarios. Moreover, the interplay between encryption techniques and evolving cybersecurity threats should be examined, offering insights into adapting these methods to the challenges of a dynamic digital landscape. There is also an opportunity to investigate hybrid approaches that combine the advantages of Quantum and RSA encryption, potentially paving the way for more robust and adaptable security solutions.

Acknowledgments

I would like to thank my supervisor for his guidance. The Manuscript communication number issued by the Research & Development cell of Integral University; Lucknow is IU/R&D/2023-MCN0002120

Author contributions

Author contribution the 1st author of the manuscript wrote the complete manuscript. The 2nd author helped in designing the research work. The 3rd author helped in arranging the Ethical committee meeting proving the idea to the committee and getting approval. The 4th author was responsible for reviewing the complete manuscript. The 5th author helped the 1st author in writing and adding references to the manuscript.

REFRENCES

[1] Möller, Matthias, and Cornelis Vuik. 2017. “On the Impact of Quantum Computing Technology on Future Developments in High-Performance Scientific Computing.” Ethics & Information Technology 19, no. 4: 253–69. https://doi.org/10.1007/s10676-017-9438-0.

[2] Lau, Jonathan Wei Zhong, Kian Hwee Lim, Harshank Shrotriya, and Leong Chuan Kwek. 2022. “NISQ Computing: Where Are We and Where Do We Go.” AAPPS Bulletin 32, no. 1: 27. https://doi.org/10.1007/s43673-022-00058-z.

[3] Ciccarino, Christopher J., and Prineha Narang. "Quantum information and algorithms for correlated quantum matter." Chemical Reviews 121. 2020. Head-Marsden vol. 5. Kade: Johannes Flick: 3061–120. https://doi.org/10.1021/acs.chemrev.0c00620

[4] Blais, Alexandre, Steven M. Girvin, and William D. Oliver. 2020. “Quantum Information Processing and Quantum Optics with Circuit Quantum Electrodynamics.” Nature Physics 16, no. 3: 247–56. https://doi.org/10.1038/s41567-020-0806-z.

[5] Cerezo, Marco, Andrew Arrasmith, Ryan Babbush, Simon C. Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R. McClean, K. Mitarai, X. Yuan, L. Cincio, and P. J. Coles. 2021. “Variational Quantum Algorithms.” Nature Reviews Physics 3, no. 9: 625–44. https://doi.org/10.1038/s42254-021-00348-9.

[6] Hassija, Vikas, Vinay Chamola, Vikas Saxena, Vaibhav Chanana, Prakhar Parashari, Shahid Mumtaz, and Mohsen Guizani. 2020. “Present Landscape of Quantum Computing.” IET Quantum Communication 1, no. 2: 42–8. https://doi.org/10.1049/iet-qtc.2020.0027.

[7] Marella, Surya Teja, and Hemanth Sai Kumar Parisa. 2020. “Introduction to Quantum Computing.” Quantum Computing & Communications.

[8] Bassman, Lindsay, Miroslav Urbanek, Mekena Metcalf, Jonathan Carter, Alexander F. Kemper, and Wibe A. de Jong. 2021. “Simulating Quantum Materials with Digital Quantum Computers.” Quantum Science & Technology 6, no. 4: 043002. https://doi.org/10.1088/2058-9565/ac1ca6.

[9] https://www.nii.ac.jp/qis/first-quantum/e/subgroups/quantumCommunication/index.html.

[10] Flamini, Fulvio, Fulvio, Nicolo Spagnolo, and Fabio Sciarrino. 2018. “Photonic Quantum Information Processing: A Review.” Reports on Progress in Physics 82, no. 1: 016001. DOI 10.1088/1361-6633/aad5b2

[11] Shannon, Keith, Elias Towe, and Ozan K. Tonguz. 2020. ‘On the use of quantum entanglement in secure communications: a survey.’ arXiv Preprint ArXiv:2003.07907. https://doi.org/10.48550/arXiv.2003.07907

[12] Gill, Sukhpal Singh, Minxian Xu, Carlo Ottaviani, Panos Patros, Rami Bahsoon, Arash Shaghaghi, Muhammed Golec, V. Stankovski, H. Wu, A. Abraham, M. Singh, H. Mehta, S. K. Ghosh, T. Baker, A. K. Parlikad, H. Lutfiyya, S. S. Kanhere, R. Sakellariou, S. Dustdar, O. Rana, I. Brandic, and S. Uhlig. 2022. "AI for Next Generation Computing: Emerging Trends and Future Directions." Internet of Things 19: 100514. https://doi.org/10.1016/j.iot.2022.100514.

[13] Čolaković, Alem, and Mesud Hadžialić. 2018. "Internet of Things (IoT): A Review of Enabling Technologies, Challenges, and Open Research Issues." Computer Networks 144: 17–39. https://doi.org/10.1016/j.comnet.2018.07.017.

[14] Awschalom, David, Karl K. Berggren, Hannes Bernien, Sunil Bhave, Lincoln D. Carr, Paul Davids, Sophia E. Economou, D. Englund, A. Faraon, M. Fejer, S. Guha, M. V. Gustafsson, E. Hu, L. Jiang, J. Kim, B. Korzh, P. Kumar, P. G. Kwiat, M. Lončar, M. D. Lukin, D. A. B. Miller, C. Monroe, S. W. Nam, P. Narang, J. S. Orcutt, M. G. Raymer, A. H. Safavi-Naeini, M. Spiropulu, K. Srinivasan, S. Sun, J. Vučković, E. Waks, R. Walsworth, A. M. Weiner, and Z. Zhang. 2021. "Development of Quantum Interconnects (Quics) for Next-Generation Information Technologies." PRX Quantum 2, no. 1: 017002. https://doi.org/10.1103/PRXQuantum.2.017002.

[15] Gonzalez-Zalba, M. F., S. De Franceschi, E. Charbon, Tristan Meunier, M. Vinet, and A. S. Dzurak. 2021. "Scaling Silicon-Based Quantum Computing Using CMOS Technology." Nature Electronics 4, no. 12: 872–84. https://doi.org/10.1038/s41928-021-00681-y.

[16] Abdelgaber, Nahed, and Chris Nikolopoulos. 2020. "Overview on Quantum Computing and Its Applications in Artificial Intelligence." In IEEE Third International Conference on Artificial Intelligence and Knowledge Engineering (AIKE): 198–9. IEEE Publications. https://doi.org/10.1109/AIKE48582.2020.00038.

[17] Kerenidis, Iordanis, Jonas Landman, and Natansh Mathur. 2021. 'Classical and quantum algorithms for orthogonal neural networks.' arXiv Preprint ArXiv:2106.07198.

[18] Zeng, Bei, Xie Chen, Duan-Lu Zhou, and Xiao-Gang Wen. 2015. 'Quantum Information Meets Quantum Matter—From Quantum Entanglement to Topological Phase in Many-Body Systems.' arXiv Preprint ArXiv:1508.02595 https://doi.org/10.48550/arXiv.1508.02595

[19] Majumdar, M. G. 2018 "Quantum Information Processing Using the Exchange Interaction." Journal of Quantum Information Science 08, no. 4: 139–60. https://doi.org/10.4236/jqis.2018.84010.

[20] Stajic, Jelena. 2013. "The Future of Quantum Information Processing." Science 339, no. 6124: 1163–. https://doi.org/10.1126/science.339.6124.1163.

[21] https://www.researchgate.net/figure/An-illustration-showcasing-the-process-of-quantum-information-processing_fig2_373574906.

[22] Svore, Krysta M., and Matthias Troyer. 2016. "The Quantum Future of Computation." Computer 49, no. 9: 21–30. https://doi.org/10.1109/MC.2016.293.

[23] Bauer, Bela, Sergey Bravyi, Mario Motta, and Garnet Kin-Lic Kin-Lic Chan. 2020. "Quantum Algorithms for Quantum Chemistry and Quantum Materials Science." Chemical Reviews 120, no. 22: 12685–717. https://doi.org/10.1021/acs.chemrev.9b00829.

[24] Kumar, Ajay, and Sunita Garhwal. 2021. "State-of-the-Art Survey of Quantum Cryptography." Archives of Computational Methods in Engineering 28, no. 5: 3831–68. https://doi.org/10.1007/s11831-021-09561-2.

[25] Lidar, Daniel A., and Todd A. Brun, eds. 2013. Quantum Error Correction. Cambridge University Press.

[26] Schuld, Maria, Ilya Sinayskiy, and Francesco Petruccione. 2015. "An Introduction to Quantum Machine Learning." Contemporary Physics 56, no. 2: 172–85. https://doi.org/10.1080/00107514.2014.964942.

[27] Chen, Jiajun. 2021. "Review on Quantum Communication and Quantum Computation." In Journal of Physics: Conference Series. IOP Publishing 1865, no. 2: 022008. https://doi.org/10.1088/1742-6596/1865/2/022008.

[28] Wehner, Stephanie, David Elkouss, and Ronald Hanson. 2018. "Quantum Internet: A Vision for the Road Ahead." Science 362, no. 6412: eaam9288. https://doi.org/10.1126/science.aam9288.

[29] Wang, L., Kai-Heng Zou Zou, Wei Sun, Yingqiu Mao, Yi-Xiao Zhu, Hua-Lei Yin, Qing Chen, Y. Zhao, F. Zhang, T. Chen, and J. Pan. 2017. "Long-Distance Copropagation of Quantum Key Distribution and Terabit Classical Optical Data Channels." Physical Review. Part A 95, no. 1: 012301. https://doi.org/10.1103/PhysRevA.95.012301.

[30] Dixon, A. R., J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields. 2015. "High-Speed Prototype Quantum Key Distribution System and Long Term Field Trial." Optics Express 23, no. 6: 7583–92. https://doi.org/10.1364/OE.23.007583.

[31] Broadbent, Anne, and Christian Schaffner. 2016. "Quantum Cryptography Beyond Quantum Key Distribution." Designs, Codes, & Cryptography 78, no. 1: 351–82. https://doi.org/10.1007/s10623-015-0157-4.

[32] Xu, Minrui, Xiaoxu Ren, Dusit Niyato, Jiawen Kang, Chao Qiu, Zehui Xiong, Xiaofei Wang, and Victor C. M. Leung. 2023. "When Quantum Information Technologies Meet Blockchain in Web 3.0." IEEE Network: 1–8. https://doi.org/10.1109/MNET.134.2200578.

[33] Yanagimoto, Ryotatsu, Rajveer Nehra, Ryan Hamerly, Edwin Ng, Alireza Marandi, and Hideo Mabuchi. 2023. "Quantum Nondemolition Measurements with Optical Parametric Amplifiers for Ultrafast Universal Quantum Information Processing." PRX Quantum 4, no. 1: 010333. https://doi.org/10.1103/PRXQuantum.4.010333.

[34] Burd, S. C., J.-P. Penttinen, P.-Y. Hou, H. M. Knaack, S. Ranta, M. Mäki, E. Kantola et al. 2023. "VECSEL Systems for Quantum Information Processing with Trapped Beryllium Ions." JOSA B40, no. 4: 773–81 https://doi.org/10.1364/JOSAB.475467

[35] Pomorski, K. 2023, Mar. "Analytical Solutions for N-Electron Interacting System Confined in Graph of Coupled Electrostatic Semiconductor and Superconducting Quantum Dots in Tight-Binding Model with Focus on Quantum Information Processing." In Nanomaterials and Nanocomposites, Nanostructure Surfaces, and Their Applications: Selected. Proceedings of the IX International Conference Nanotechnology and Nanomaterials, Lviv, Ukraine: 67–165. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-18096-5_7.

[36] Howe, Connor, Xinran Wang, and Ali Anwar. 2023. "Robust and Efficient Quantum Communication." In Proceedings of the 2023 International Workshop on Quantum Classical Cooperative: 13–6. https://doi.org/10.1145/3588983.3596687.

[37] Awan, U., L. Hannola, A. Tandon, R. K. Goyal, and A. Dhir. 2022. "Quantum Computing Challenges in the Software Industry. A Fuzzy AHP-Based Approach." Information & Software Technology 147: 106896. https://doi.org/10.1016/j.infsof.2022.106896.

[38] Ponce, and André Luiz Marques Meritxell Cabrejo. "Muniz, Marcus Huber, and Fabian Steinlechner." Unlocking the Frequency Domain for High-Dimensional Quantum Information Processing arXiv preprint arXiv:2206.00969 (2022).

[39] Coccia, Mario. 2022. "Technological Trajectories in Quantum Computing to Design a Quantum Ecosystem for Industrial Change." Technology Analysis & Strategic Management: 1–16. https://doi.org/10.1080/09537325.2022.2110056.

[40] Sisodia, Mitali, Abhishek Shukla, Kishore Thapliyal, and Anirban Pathak. 2017. "Design and Experimental Realization of an Optimal Scheme for Teleportation of an n-qubit Quantum State." Quantum Information Processing 16: 1–19 https://doi.org/10.1007/s11128-017-1744-2.

[41] Pirandola, Stefano, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. 2017. "Fundamental Limits of Repeaterless Quantum Communications." Nature Communications 8, no. 1: 15043. https://doi.org/10.1038/ncomms15043.

[42] Ding, Yunhong, Davide Bacco, Kjeld Dalgaard, Xinlun Cai, Xiaoqi Zhou, Karsten Rottwitt, and Leif Katsuo Oxenløwe. 2017. "High-Dimensional Quantum Key Distribution Based on Multicore Fiber Using Silicon Photonic Integrated Circuits." npj Quantum Information 3, no. 1: 25. https://doi.org/10.1038/s41534-017-0026-2.

[43] Alléaume, Romain, Cyril Branciard, Jan Bouda, Thierry Debuisschert, Mehrdad Dianati, Nicolas Gisin, Mark Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, C. Monyk, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger. 2014. "Using Quantum Key Distribution for Cryptographic Purposes: A Survey." Theoretical Computer Science 560: 62–81. https://doi.org/10.1016/j.tcs.2014.09.018.

[44] Bennett, Charles H., and Gilles Brassard. 2014. "Quantum Cryptography: Public Key Distribution and Coin Tossing." Theoretical Computer Science 560: 7–11. https://doi.org/10.1016/j.tcs.2014.05.025.

[45] Diamanti, Eleni, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan. 2016. "Practical Challenges in Quantum Key Distribution." npj Quantum Information 2, no. 1: 1–12. https://doi.org/10.1038/npjqi.2016.25.

[46] Cacciapuoti, Angela Sara, Marcello Caleffi, Rodney Van Meter, and Lajos Hanzo. 2020. "When Entanglement Meets Classical Communications: Quantum Teleportation for the Quantum Internet." IEEE Transactions on Communications 68, no. 6: 3808–33. https://doi.org/10.1109/TCOMM.2020.2978071.

[47] Pirandola, Stefano, Jens Eisert, Christian Weedbrook, Akira Furusawa, and Samuel L. Braunstein. 2015. "Advances in Quantum Teleportation." Nature Photonics 9, no. 10: 641–52. https://doi.org/10.1038/nphoton.2015.154.

[48] Luo, Yi-Han, Han-Sen Zhong, Manuel Erhard, Xi-Lin Wang, Li-Chao Peng, Mario Krenn, Xiao Jiang, L. Li, Nai-Le Liu, Chao-Yang Lu, Anton Zeilinger, and Jian-Wei Pan. 2019. "Quantum Teleportation in High Dimensions." Physical Review Letters 123, no. 7: 070505. https://doi.org/10.1103/PhysRevLett.123.070505.

[49] Alenoghena, Caroline Omoanatse, Adeiza James Onumanyi, Henry Ohiani Ohize, Achonu Oluwole Adejo, Maxwell Oligbi, Shaibu Ibrahim Ali, and Supreme Ayewoh Okoh. 2022. "EHealth: A Survey of Architectures, Developments in Mhealth, Security Concerns, and Solutions." International Journal of Environmental Research & Public Health 19, no. 20: 13071. https://doi.org/10.3390/ijerph192013071.

[50] Saharia, Ankur, Ravi Kumar Maddila, Jalil Ali, Preecha Yupapin, and Ghanshyam Singh. 2019. "An Elementary Optical Logic Circuit for Quantum Computing: A Review." Optical & Quantum Electronics 51: 1–13 https://doi.org/10.1007/s11082-019-1944-3