Quantum Communication Networks: Design, Reliability, and Security

Brian Hildebrand, Ashutosh Ghimire, Fathi Amsaad, Abdul Razaque, and Saraju P. Mohanty

Abstract— ***The overall purpose of this study*** is to explore the potential of quantum-based communication networks, leveraging the unique properties of quantum entanglement and superposition, to address critical applications such as image processing, machine learning, data mining, and encryption. Additionally, this research aims to overcome the limitations of traditional binary systems in the field of computing. ***The basic methodology of this research involves*** a comprehensive investigation into the establishment of end-to-end entanglement between two quantum computers, which is fundamental for building robust quantum networks. Performance measures for quantum computers within the context of quantum networks are defined and evaluated, with a specific focus on network design, reliability, security, and trust. Quantum-dot Cellular Automata (QCA) devices are introduced as a technological advancement to enhance security and trust mechanisms within quantum communication networks. ***Furthermore, the study addresses network congestion issues and outlines quantum-based solutions***, while also examining emerging standards for their assessment. A distinctive contribution of this research lies in the exploration of quantum key distribution (QKD) and the utilization of advanced cryptosystem methodologies to strengthen security and trust within quantum-based networks. ***In conclusion,*** this research seeks to bridge existing gaps by addressing the challenge of achieving end-to-end entanglement, evaluating critical performance metrics, introducing innovative technologies, and proposing enhancements to security and trust mechanisms. The findings of this study hold promise for not only advancing the field of quantum networking but also impacting a wider range of applications that require secure and future-oriented communication solutions in an increasingly interconnected world.

Index Terms—Quantum Networking Design, Quantum-dot Cellular Automata devices (QCA), Quantum Key Distribution (QKD), Quantum Networking Reliability, Quantum Cryptosystem Security and Trust.

1 Introduction

The next-generation technology has paved the way for the realization of quantum networking, enabling efficient communication between quantum devices to solve complex problems more effectively than traditional computing algorithms. In the realm of next-generation quantum networking, researchers have explored harnessing quantum computer features such as circuit design, entanglement, and superposition to accelerate specific calculations.

This paper begins by defining quantum computing and its inherent features, such as quantum design, entanglement, and superposition, among other attributes that enhance specific communications. We delve into the concept of quantum entanglement, a distinctive trait of quantum computing involving quantum bits, or qubits Fig. 2, that exhibit strong correlation. Furthermore, the paper demonstrates how measuring a qubit leads to its collapse into one of two potential values, similar to a classical binary digit. Our discussion extends to quantum routing Fig. **??**, highlighting the coordination of entangled quantum bits and their correlated movement. Ultimately, the paper provides a comprehensive view of performance measures for evaluating quantum networks, encompassing quantum routing, scheduling, reliability, security, and standards for Quantum Key Distribution (QKD) protocols.

Fig. 2 illustrates a generalized quantum network comprising both quantum and classical communication channels. The showcases a teleportation technique that establishes end-to-end entanglement between quantum computers, a pivotal operation for constructing basic quantum networks. Multiple quantum repeaters integrated along quantum channels extend the entanglement range, enabling connectivity over greater distances. As seen in Fig. 2, teleportation is crucial in quantum networking, allowing quantum circuits to extend across computers. This entails entangling qubits across the network, interconnecting qubits between computers. These interlinked qubits, referred to as ″flying qubits,″ encode photon spin or polarization, traversing optical fibers or wireless mediums. Thoughtfully sequenced flying qubits facilitate quantum state transfer across extended distances.

At the core of a quantum computer lies the quantum bit (qubit), analogous to the classical binary digit (bit). Unlike classical bits that represent only 0 or 1, qubits span the full range between 0 and 1, justified by the principles of quantum mechanics. In classical computing, a bit can exist in one of two discrete states, 0 or 1. However, in quantum computing, qubits can exist in a state of superposition, meaning they can represent a combination of both 0 and 1 simultaneously, as well as any value between these two states. This property is a fundamental aspect of quantum mechanics and serves as a foundation for quantum computation. The concept that qubits can exist in a superposition of states between 0 and 1 is a fundamental principle of quantum mechanics. This idea is often explained through Schrödinger′s equation, which describes how quantum states evolve over time. In quantum computing, qubits leverage this property to perform multiple calculations simultaneously, leading to the potential for exponential speedup in certain computations compared to classical computers.

- *Brian Hildebrand and Ashutosh Ghimire contributed equally to this paper.*

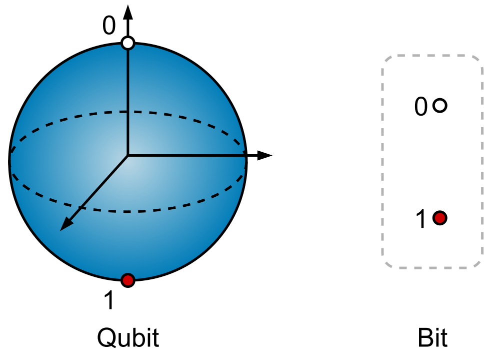

Fig. 1. Graphical representation of qubit and a traditional binary digit (bit).

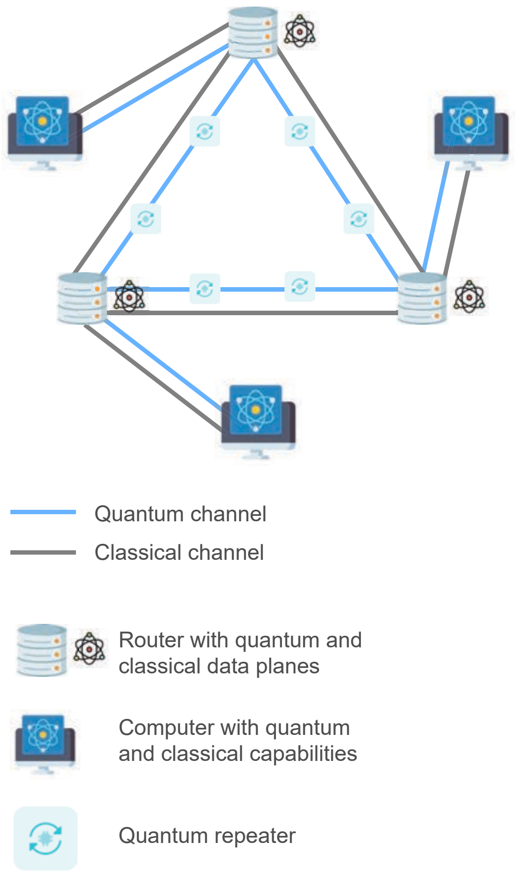
Quantum channel
Classical channel
Router with quantum and classical data planes
Computer with quantum and classical capabilities
Quantum repeater

Fig. 2. Quantum Network with quantum and classical channels. Quantum repeaters are used to extend the range of quantum entanglement.

The subsequent sections are organized as follows: Section 2 presents an overview of Quantum Design. Section 3 covers Quantum Network Routing. Section 4 delves into Quantum Network Reliability. Section 5 explores Quantum Communication Security, and the paper concludes with Section 6.

2 Quantum Design

Implementing quantum algorithms within quantum-based computers requires designing quantum circuits for executing arithmetic operations, including addition, subtraction, and multiplication. Our journey into quantum algorithms, covering tasks such as integer factoring, searching, and quantum mechanical modeling, begins with the quantum circuit for multiplication. Quantum bits (qubits) serve as the fundamental unit of quantum information. In Figure 1, we illustrate the distinction between the conventional binary digit (bit) and the qubit. While a bit can only adopt values of 0 or 1, a qubit can represent 0 or 1 as well as any value between them or on the surface of a sphere. A distinctive attribute of the qubit is its superposition property, wherein it exists in multiple states until measured. Following measurement, the qubit collapses to a specific state. Given the limited availability of qubits in existing quantum computers, researchers often consider the qubit cost, which represents the total number of qubits used in constructing a quantum circuit, as a critical performance measure.

However, quantum computers face a significant challenge in increased susceptibility to noise errors, known as decoherence. This phenomenon deteriorates qubit state functions, reducing the accuracy of quantum calculations. Decoherence arises from entanglement with external factors such as light, vibration, sound, cosmic rays, and interference from wireless devices, as well as internal interactions between qubits within the same system. The task of isolating individual qubits further compounds this challenge. A potential solution involves constructing quantum circuits that incorporate Clifford+T gates, leveraging their inherent fault tolerance capabilities. Clifford gates, which use conjugation to normalize qubits, offer a means of error mitigation. When combined with T gates, these circuits gain resilience through the application of error-correcting codes, a vital technique for safeguarding quantum information from noise-induced errors.

The introduction of fault tolerance brings with it additional challenges of computational overhead. Unlike classical bits with discrete ”1” or ”0” states, qubits exist in superposition. Maintaining fault tolerance necessitates resources to restore qubit states, which extends to the complexity of T gate implementation. Managing this supplementary layer of overhead is crucial for ensuring the reliability and robustness of quantum computations. Table 1 provides a summarized of compassion between different quantum networking performance measures. Quantum-dot Cellular Automata (QCA) offers an energy-efficient solution for circuits with limited resources. QCA utilizes quantum circuits and internal connections to interlink building blocks, enabling the design of low-power circuits and high-throughput networks. In Figure 3, you can see an overview of a typical QCA configuration, with shaded dots representing two charged electrons capable of tunneling across the cell. Governed by electrostatic repulsion, these electrons strive to position themselves as far apart as possible within the cell, representing two distinct states. Recent research highlights QCA's potential to replace conventional integrated circuits, making it a compelling option for low-power circuit design.

In the realm of digital circuits, an adder is responsible for performing addition operations. Among these, the carry look-ahead adder (CLA) stands out as a pivotal component in digital arithmetic processing. The CLA excels in its abil-

TABLE 1
Compassion Between Different Quantum Networking Performance Measures

Quantum Circuit Design	T-Count	T gates employed to build quantum design
	T-Depth	Layers of T gate in quantum design
	Qubit Cost	Number of qubits used to build quantum circuit
Quantum Routing	Entanglement fidelity	Measure of the difference between actual & desired states of a quantum system
	Throughput	Rate of successful delivery of data across network
Quantum Solutions to Network Congestion	Routing time	Time it takes packet to choose a route
	Travel time	Time it takes packet to travel to destination
	Total transmission time	Sum of routing time & travel time
	Fault tolerance to noise	Effect of noise on qubit states
QKD for 5G Networks	Latency	Communication delay over network
	Bandwidth	Maximum amount of data transmitted over network in a given time frame
	Massive connectivity	Ability to connect to a large amount of devices/computers

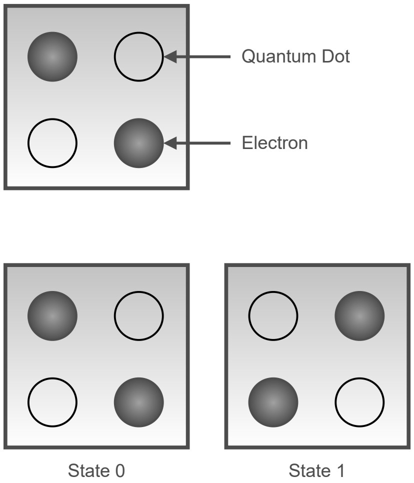

Fig. 3. Quantum-dot Cellular Automata (QCA). The shaded dots represent two charged electrons free to move to any part of the cell. Based on the principle of electrostatic repulsion, the charged electrons will attempt to move as far as possible from each other in the cell. The two electrons represent two possible states.

ity to perform addition with higher efficiency and speed compared to alternatives such as the ripple carry adder (RCA). This efficiency stems from its capability to predict carry bits before determining the sum, effectively reducing computation time. The quantum carry look-ahead adder (QCLA) serves as the quantum counterpart to the CLA, executing addition with a time complexity of O(log(n)). The QCLA leverages ripple carry adders and is characterized by a linear depth equivalent to its input bit count. This results in significantly improved speed compared to RCAs, which require O(n) time for similar operations. Quantum-dot Cellular Automata (QCA) offers an energy-efficient solution for circuits with limited resources. By utilizing quantum circuits and internal connections, QCA can interlink building blocks, enabling the design of low-power circuits and high-throughput networks. The general QCA setup, as depicted in Fig. 3, features charged electrons capable of tunneling across the cell. Governed by electrostatic repulsion, these electrons assume positions that maximize their separation within the cell, representing distinct states.

Recent research underscores QCA's potential to replace conventional integrated circuits, making it a compelling avenue for achieving low-power circuit design. In digital circuits, the task of addition is typically performed by an adder. The carry look-ahead adder (CLA) stands out as a pivotal component in digital arithmetic processing. It excels in performing addition with higher efficiency and speed compared to alternatives like the ripple carry adder (RCA). This efficiency stems from its ability to predict carry bits before determining the sum, effectively reducing computation time. The quantum carry look-ahead adder (QCLA) serves as the quantum counterpart to the CLA, executing addition with a time complexity of O(log(n)). Leveraging ripple carry adders, the QCLA's linear depth corresponds to its input bit count, resulting in significantly improved speed compared to RCAs, which require O(n) time for similar operations. Direct connections between inputs and outputs of a quantum circuit often introduce complexities, necessitating ancillae (auxiliary) qubits and producing output garbage. Ancillae are involved when a constant input is applied to the quantum circuit, while garbage output arises when a quantum circuit's work doesn't contribute as input to another circuit. Removing garbage output is crucial for reducing the quantum circuit's overall qubit and T gate costs. QCLAs can be categorized as in-place and out-of-place. An in-place QCLA replaces a direct input with the sum, while an out-of-place QCLA returns the sum on ancillae. For quantum computing applications, QCLAs should ideally produce no garbage output without significantly impacting qubit and T gate costs. Achieving this goal requires efficient utilization of T-gate-efficient Toffoli gates, which serve as reversible logic building blocks.

3 Quantum Network Routing

Efficiently constructing quantum-based network topologies necessitates the creation and optimization of network routing. Quantum routing is centered around identifying the optimal channel for teleporting qubits, a process crucial for extending quantum circuits beyond individual computers. Unlike classical bits, qubits cannot be copied, but they can be teleported between quantum systems, establishing quantum entanglement. This unique feature, characterized by strong correlations among specific groups of qubits, demands a

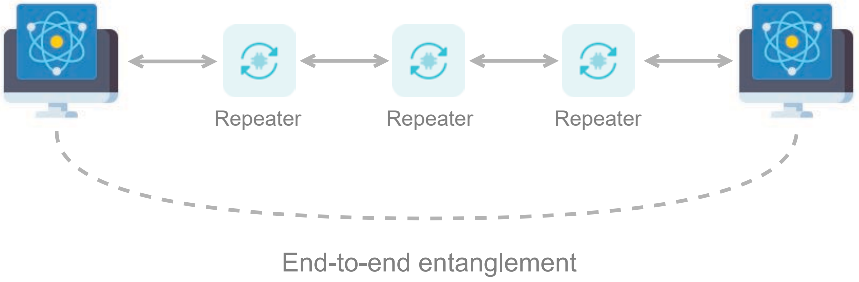

Fig. 4. End-to-end entanglement between two quantum computers using a series of three quantum repeaters

holistic consideration of potential qubit values due to interdependent probabilities. Entangling qubits is facilitated by ’flying qubits,’ which encode states in photon spin or polarization for transmission through fiber optic cables or wireless methods. However, flying qubits experience fidelity degradation with increased distance. Quantum repeaters serve as intermediaries to extend their range, utilizing entanglement swapping between two flying qubits to generate end-to-end entanglement. Challenges such as signal power attenuation and transmission imperfections influence entanglement quality along the chain. Evaluation measures for quantum network quality encompass throughput and entanglement fidelity, reflecting data delivery success rates and the variance between desired and actual quantum states.

In Figure 4, you can see the illustration of the establishment of end-to-end entanglement between quantum computers via three quantum repeaters. This emphasizes the significance of quantum entanglement and repeaters within networks that integrate both quantum and classical communication. The efficiency of quantum entanglement relies on the effectiveness of quantum routing strategies, which involve finding the right balance between scheduling and path selection. Scheduling entails selecting quantum couples to establish end-to-end entanglement within specific time slots. The choice of optimal paths or quantum repeater sets plays a vital role in entanglement creation. Effective quantum routing utilizes strategies such as weighted round-robin or iterative selection for path optimization, enhancing both the entanglement rate and fidelity. Certain quantum routing algorithms pre-allocate qubits to prevent resource conflicts during entanglement swapping. However, resource fragmentation can hinder network efficiency. Strategies like Q-CAST aim to mitigate this issue by considering fragmentation during entanglement and using priority connections for recovery in case of failures. Another approach involves employing entanglement purification techniques to enhance entanglement quality between sets of qubits across nodes. Q-PATH identifies purification choices based on cost considerations, while Q-LEAP minimizes fidelity loss along the shortest route, using efficient purification decision methods to streamline computations.

4 Quantum Network Reliability

In the realm of network communications, users and computers often compete for the shortest and quickest paths. However, network reliability becomes a concern when multiple users or computers choose the same route. The criteria for evaluating quantum solutions to network reliability are succinctly outlined in Table 1. Navigating network reliability requires a delicate balance between transmission latency and cost. For example, network congestion can be assessed through total transmission time, which combines routing time and travel time. Travel time represents the duration for a network packet to reach its destination, while routing time signifies the time taken for a packet to select a route. As more packets opt for a common route, the travel time for each packet increases. Therefore, each packet faces two choices: (1) Opt for the shortest path and risk potential delays due to congestion, or (2) choose a longer path with lower congestion-induced delays. Classical approaches treat these options as binary decisions (0 or 1). In contrast, quantum computing allows for representing various options through multiple states between 0 and 1 within a qubit. Additionally, the impact of noise on qubit states, termed fault tolerance to noise, is a crucial consideration. Novel proposed solutions leverage quantum game theory to address network congestion and reliability concerns. In this paradigm, packets engage in self-interested competition for optimal routes. Initially, quantum states are assigned to represent each possible strategy. Subsequently, each packet adapts its local qubit’s state to choose the optimal strategy. Such approaches hold potential to reduce travel and routing times, providing innovative solutions to alleviate network congestion and enhance reliability.

5 Quantum Communication Security

Security concerns loom over end-to-end quantum networks, encompassing challenges in cybersecurity across cloud and edge computing, privacy and security attacks in fog computing architectures, and vulnerabilities in IoT-based devices. To address these concerns, Quantum Key Distribution (QKD) emerges as a novel security paradigm, harnessing the unique properties of quantum mechanics for cryptographic operations such as encryption and decryption. QKD also provides a means to obtain critical cryptanalysis information, serving as a countermeasure against attempts to exploit quantum-based physical characteristics for constructing distributed symmetric keys. In Fig. 5, you can see a typical QKD scenario where two computers establish a network link via classical and quantum channels. In this illustration, one computer generates a secret key and transmits it to the other computer through the quantum channel, established

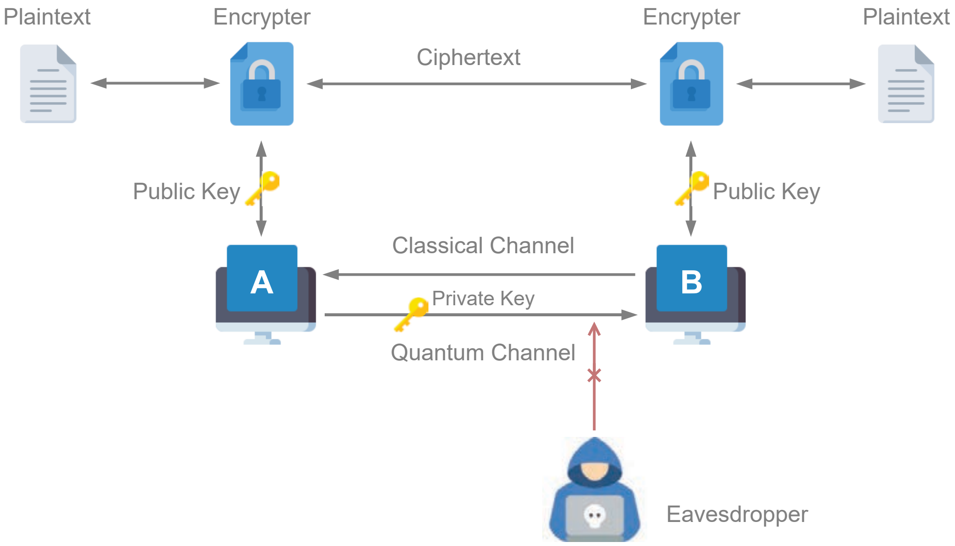

Fig. 5. Quantum Key Distribution (QKD). Two computers, A and B, establish a connection via classical and quantum channels. A transmits the secret key to B over a quantum channel established using quantum entanglement and teleportation techniques. An eavesdropper cannot measure the qubits on a quantum channel without disturbing the integrity of the qubits. The loss of integrity of the message sent over the quantum channel is indicative of an eavesdropping attempt. B can use the private and public keys to decrypt if message integrity is good. Otherwise, the secret key needs to be present.

via end-to-end entanglement and teleportation techniques. The quantum nature of the channel ensures that any eavesdropping attempt results in the qubit's consumption upon measurement. Upon receiving an intact message containing the secret key, the second computer uses the private and public keys for decryption. If the integrity of the secret key is compromised, the key must be resent, ensuring robust security in the quantum communication network.

Table 1 provides a summary of evaluation criteria for QKD implementations in 5G networks. The key performance indicators of 5G networks include latency, bandwidth, and massive connectivity. Latency is the measure of communication delay over a network. Bandwidth is the maximum amount of data a network is capable of having transmitted over it at any given time frame. Massive connectivity is the measure of a network's ability to connect to a large number of computers or devices. To meet the ambitious performance goals of 5G networks, including low latency, ample bandwidth, and widespread connectivity, researchers have embraced advancements like software-defined networks (SDNs) and network function virtualization (NFV) to rapidly deploy network services. While NFV orchestrators (NFVOs) facilitate the creation and implementation of services like NFVs, their current scope is confined to single administrative domains.

Progress is being made in the realm of multi-domain orchestration, empowering service providers to establish comprehensive network services that span distinct network administration domains. However, this advancement introduces overarching security concerns that encompass the entire end-to-end network. These concerns include potential security threats associated with mobile edge computing (MEC) and Internet of Things (IoT) devices, as well as security and privacy vulnerabilities tied to fog computing architectures. Addressing these security challenges, some proposals advocate the use of Quantum Key Distribution (QKD). For instance, the q-ROADM, a QKD switch-enabled flex-grid architecture, supports classical and quantum data channels across a 5G optical network. q-ROADM aims to enhance end-to-end security across heterogeneous networks, a significant objective of 5G. Expanding on the 5GUK Exchange orchestrator, the q-ROADM framework demonstrates a quantum-secured diverse multi-domain 5G network. This network facilitates the seamless deployment of services by chaining virtual network functions (VNFs) across various domains. The architecture integrates a quantum-secured optical network, catering to both quantum and classical channels, and offers dynamic quantum key switching and inter-domain optical network connectivity. This approach enables efficient VNF chaining while ensuring robust quantum protection.

To bolster security and trust in future quantum and post-quantum cryptographic standardization, cryptosystem approaches have emerged. These implementations, including LDPC and MDPC, Reed-Solomon designs, and McEliece, address the security challenges of convolutional cryptography and safeguard quantum systems against cyberattacks. These techniques find applications in consumer electronics, A.I., and blockchain-based technologies like Bitcoin. The approaches involve generating binary codes for system authentication, secure digital signatures, and cryptographic key exchange over untrusted mediums, offering resilience against various attacks. Emerging cyberattacks targeting quantum computing, such as side-channel and power analysis attacks, are also being countered. One unique approach focuses on mitigating side-channel attacks during the implementation of the McEliece cryptosystem on resource-constrained platforms. Utilizing quantum arithmetic benchmarks, this approach evaluates cryptosystem measures benchmarked on FPGA, incorporating error detection mechanisms to thwart fault attacks in quantum computing design.

6 Conclusion

Quantum communication networks have emerged to allow devices to communicate efficiently, reliably, and securely and perform critical tasks such as image processing, science computations, and searching and breaking encryption. This work stands out due to the merit of its comprehensive exploration of quantum communication networks, offering a novel perspective on quantum computing's performance and security aspects. By delving into both foundational and advanced concepts, the paper provides a unique blend of fundamental principles and cutting-edge techniques, showcasing its novelty. The focus on quantum networking security and design introduces a novel angle, addressing critical concerns in an evolving field. Additionally, the study's systematic approach, encompassing quantum circuit analysis, routing strategies, congestion solutions, and QKD integration, showcases the paper's pioneering approach to addressing various challenges within quantum communication networks. The careful consideration of evaluation criteria throughout the study adds a distinct merit, ensuring a rigorous analysis and presenting a practical framework for assessing quantum-based solutions. This paper thus offers valuable insights and contributions to advancing the field of quantum communication networks, both in terms of its merit and the innovative perspectives it presents.

7 Future Work

Building upon the comprehensive exploration of quantum communication networks presented in this paper, several avenues for future research and development emerge. Firstly, further investigations can be conducted to enhance the practical implementation of the proposed quantum circuit designs, entanglement-based routing strategies, and congestion solutions. As quantum communication networks advance, the development of optimized protocols and algorithms could substantially improve their efficiency and reliability. Moreover, the integration of emerging technologies such as Quantum-dot Cellular Automata devices (QCA) could be explored to enhance the performance and scalability of quantum communication systems. Research efforts could focus on developing QCA-based components that offer faster processing and improved error correction mechanisms, addressing the issue of decoherence and enhancing the overall security of quantum communication. Additionally, the integration of quantum communication networks with existing classical communication infrastructures presents a promising area for further investigation. Developing seamless interoperability protocols, efficient gateways, and hybrid network architectures could pave the way for practical implementations that leverage the strengths of both classical and quantum communication. Finally, the study of quantum communication networks could expand to consider the implications of multi-party communication scenarios, enabling the development of robust and scalable protocols for secure multiparty quantum communication. Further exploration of quantum key distribution (QKD) methods, including advancements in post-processing techniques, could lead to enhanced security protocols that withstand potential attacks and vulnerabilities.

Read more about it

1) T. G. Tan, J. Zhou, V. Sharma, and S. P. Mohanty, "Post-Quantum Adversarial Modelling: A User's Perspective", IEEE Computer, Vol. XX, No. YY, ZZ 2022, pp. Accepted on 23 Oct 2022, DOI: XXX.
2) A. Nanda, D. Puthal, S. P. Mohanty, and U. Choppali, "A Computing Perspective of Quantum Cryptography", IEEE Consumer Electronics Magazine, Volume 7, Issue 6, November 2018, pp. 57–59.
3) H. Thapliyal, E. Muñoz-Coreas and V. Khalus, "Special Session: Quantum Carry Lookahead Adders for NISQ and Quantum Image Processing," 2020 IEEE 38th International Conference on Computer Design (ICCD), 2020, pp. 5-8.
4) S. E. Venegas-Andraca, M. Lanzagorta and J. Uhlmann, "Maritime applications of quantum computation," OCEANS 2015 - MTS/IEEE Washington, 2015, pp. 1-8.
5) M. Amy, D. Maslov and M. Mosca, "Polynomial-Time T-Depth Optimization of Clifford+T Circuits Via Matroid Partitioning," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 33, no. 10, pp. 1476-1489, Oct. 2014.
6) M. Amy, D. Maslov, M. Mosca and M. Roetteler, "A Meet-in-the-Middle Algorithm for Fast Synthesis of Depth-Optimal Quantum Circuits," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 32, no. 6, pp. 818-830, June 2013.
7) Munoz-Coreas and H. Thapliyal, "Quantum Circuit Design of a T-count Optimized Integer Multiplier," in IEEE Transactions on Computers, vol. 68, no. 5, pp. 729-739, 1 May 2019.
8) A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider and M. Hamdi, "A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4004-4022, 15 March15, 2021.
9) J. Ni, K. Zhang, X. Lin and X. Shen, "Securing Fog Computing for Internet of Things Applications: Challenges and Solutions," in IEEE Communications Surveys and Tutorials, vol. 20, no. 1, pp. 601-628, Firstquarter 2018.
10) Y. Zhao and C. Qiao, "Redundant Entanglement Provisioning and Selection for Throughput Maximization in Quantum Networks," IEEE INFOCOM 2021 - IEEE Conference on Computer Communications, 2021, pp. 1-10.
11) M. Caleffi and A. S. Cacciapuoti, "Quantum Switch for the Quantum Internet: Noiseless Communications Through Noisy Channels," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 3, pp. 575-588, March 2020.
12) A. Cintas Canto, M. M. Kermani and R. Azarderakhsh, "Reliable Architectures for Composite-Field-Oriented Constructions of McEliece Post-Quantum Cryptography on FPGA," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 40, no. 5, pp. 999-1003, May 2021.

Acknowledgement

The authors extend their heartfelt gratitude for the technical and financial support provided by the Air Force Research Lab (AFRL) through the Assured and Trusted Digital Microelectronics Ecosystem (ADMETE) grant, BAA-FA8650-18-S-1201, awarded to Wright State University in Dayton, Ohio, USA. This project was carried out in accordance with CAGE Number: 4B991 and DUNS Number: 047814256. Additionally, the paper received partial support from the National Pathway to Success, an NSA grant with grant number 671757.

About the Authers

Brian Hildebrand (bhildeb1@emich.edu) is *a Ph.D. student* in the School of Information Security and Applied Computing at Eastern Michigan University (EMU). He earned his Master's in Computer Science from EMU in 2019. His research interests include Quantum Communication and Security.

Ashutosh Ghimire (ghimire.18@@wright.edu) is *an M.Sc. student* in the Computer Science and Engineering at Wright State University (WSU). His research interests include Quantum Communication and Security.

Fathi Amsaad (fathi.amsaad@wright.edu)) is *an Assistant Professor* of the Computer Science and Engineering at Wright State University (WSU). His research interests include Cyber and Physical Systems Security and Trust.

Abdul Razaque (a.razaque@edu.iitu.kz) holds the position of *Professor* within the domain of Computer Science and Engineering at the International Information Technology University, situated in Almaty, Kazakhstan. In 2014, he accomplished his doctoral studies, obtaining a Ph.D. in Computer Science & Engineering from the University of Bridgeport in the United States. His scholarly pursuits encompass a focus on Wireless Sensor Networks and the realm of security in Cloud Computing.

Saraju P. Mohanty (Saraju.Mohanty@unt.edu) is holds the title of *a Senior Member of IEEE* and serves as a Professor within the Department of Computer Science and Engineering (CSE) at the University of North Texas (UNT). He completed his Ph.D. in Computer Science and Engineering at the University of South Florida (USF) in 2003. His primary research focus centers around "Intelligent Electronic Systems," which has garnered financial support from notable institutions including the National Science Foundation (NSF), Semiconductor Research Corporation (SRC), U.S. Air Force, IUSSTF, and Mission Innovation.