Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 2s (2024)

LDQKDPB: Unbreakable Network Security via Long-Distance Quantum Key Distribution Enhanced by Post-Quantum Techniques and Blockchain

Manish K.Hadap[1*], Nisha wankhade[2], Suresh Kurumbanshi [3], Vyankateshwar G. Girhepunje[4], S.S. Bawankule[5], Arvind R. Bhagat Patil[6]

[1]Department of Information Technology, Yeshwantrao Chavan College of Engineering, Nagpur India
manishhadap@yahoo.co.in

[2]Department of Information Technology, Yeshwantrao Chavan College of Engineering, Nagpur India
nisha.wankhade@gmail.com

[3]Department of Electronics & Telecommunications Engineering, SVKM's NMIMS, MPSTME, Shirpur campus
suresh.kurumbanshi@nmims.edu

[4]Dept. of Electronics and Telecommunication, Priyadarshini College of Engineering, Nagpur
vyenktesh1973@gmail.com

[5]Dept. of CSE, J.L. College of Engineering, Nagpur
sonalkk2009@gmail.com

[6]Dept. of Computer Technology, Yeshwantrao Chavan College of Engineering, Nagpur
arbhagatpatil@gmail.com

Article History:

Received: *22-03-2024*

Revised: *16-05-2024*

Accepted: *29-05-2024*

Abstract:

In the realm of network security, the quest for impervious defense has led to the integration of cutting-edge technologies, resulting in an innovative framework aptly named Unbreakable Network Security. This paper introduces a holistic approach that seamlessly combines three formidable pillars of cybersecurity: Long-Distance Quantum Key Distribution (QKD), Post-Quantum Techniques, and Blockchain technology process. This unified framework is engineered to not only withstand the prevalent Sybil, Masquerading, Finney, and Distributed Denial of Service (DDoS) attacks but also to elevate network performance on multiple fronts. Through rigorous experimentation and analysis, the authors demonstrate that their implementation of this framework yields remarkable advantages over existing quantum models. Specifically, it achieves a substantial 10.5% reduction in network delay, a noteworthy 19.4% decrease in energy consumption, and a commendable 8.5% enhancement in throughput. These findings illuminate the pressing limitations of conventional security paradigms, which struggle to defend against the evolving landscape of cyber threats, especially those posed by quantum computing operations. Conversely, the proposed method harnesses the intrinsic properties of quantum mechanics, combines them with post-quantum cryptographic resilience, and fortifies the network's integrity through blockchain integration. This innovative amalgamation represents a significant leap forward in securing communication networks, preserving data confidentiality, and ensuring the availability of critical services.. Its impacts extend beyond safeguarding sensitive information; they empower organizations to navigate the tumultuous cybersecurity landscape with confidence and resilience levels.

Keywords: Quantum Key Distribution, Post-Quantum Cryptography, Blockchain Integration, Network Security, Unbreakable Security, Scenarios.

1. Introduction

The evolution of modern communication networks has brought unprecedented levels of connectivity and convenience, revolutionizing the way individuals and organizations interact globally. However, this connectivity has also exposed these networks to an ever-expanding array of cyber threats, many of which are becoming increasingly sophisticated and potent. Among these threats, the impending advent of quantum computing poses a particularly daunting challenge to classical cryptographic methods, potentially rendering them obsolete and unraveling the fabric of secure communication. As the digital age hurtles toward this quantum era, the imperative to fortify network security against these emerging threats has never been more pressing in current scenarios due to use of methods like Receiver-Device-Independent Entanglement-Swapping-Based Quantum Key Distribution (RDIES) operations [1, 2, 3].

Quantum Key Distribution (QKD) has emerged as a beacon of hope in this turbulent cybersecurity landscape. Leveraging the principles of quantum mechanics, QKD offers a fundamentally secure method of generating cryptographic keys, impervious to the computational might of quantum adversaries. However, the practical deployment of QKD has been hampered by limitations, such as its restricted operational range, which often falls short of the expansive demands of modern communication networks.

To address these challenges, this paper introduces a comprehensive framework, Unbreakable Network Security, that not only extends the reach of QKD through Long-Distance Quantum Key Distribution but also augments its resilience through Post-Quantum Techniques. Furthermore, it fortifies the network's integrity by integrating blockchain technology. This multifaceted approach not only raises the bar for network security but also enhances its efficiency and performance.

In this introductory section, we provide an overview of the contemporary threat landscape, highlighting the limitations of existing security measures in the face of quantum computing. We then present the three foundational components of our proposed framework: Long-Distance Quantum Key Distribution, Post-Quantum Techniques, and Blockchain Integration. Subsequently, we outline the objectives of this research, emphasizing the need for a holistic approach to network security that addresses the limitations of current methods while harnessing the strengths of emerging technologies. Finally, we offer a preview of the paper's structure, outlining the subsequent sections that delve into the technical details, experimental results, and implications of our novel approach. By embarking on this journey, we endeavor to usher in an era of network security that is not merely robust but genuinely unbreakable, safeguarding the digital realm against the formidable challenges that lie ahead.

2. Literature Review

The digital age has witnessed an unprecedented surge in data-driven communication and connectivity, making cybersecurity an increasingly critical concern. With quantum computing on the horizon, classical cryptographic methods face an imminent threat, compelling researchers to seek innovative solutions. This literature review provides an overview of the evolving threat landscape, the limitations of existing security protocols, and the emergence of quantum-resistant technologies, highlighting the need for a holistic approach to network security as embodied by our proposed framework.

The Quantum Threat: The impending arrival of quantum computing poses a formidable challenge to classical cryptography. Shor's algorithm, for instance, threatens the security of widely used encryption schemes such as RSA and ECC by efficiently factoring large numbers and solving the discrete logarithm problem. Quantum adversaries armed with such capabilities could potentially compromise the confidentiality of data and the integrity of communication channels [4, 5, 6].

Quantum Key Distribution (QKD): As a countermeasure to quantum threats, QKD has gained prominence. QKD harnesses the principles of quantum mechanics to enable the secure exchange of cryptographic keys. The fundamental principle of QKD, the no-cloning theorem, ensures that intercepted keys cannot be duplicated or observed without detection, offering a level of security that remains unattainable by classical methods like Software-Defined Quantum Key Distribution Networks (SDQKD) Process [7, 8, 9].

Limitations of QKD: While QKD promises security, its practical implementation faces challenges. Notably, QKD's operational range is constrained, making it unsuitable for long-distance communication networks. Additionally, environmental factors such as photon loss and channel noise can significantly impact QKD performance. These limitations have hindered the widespread adoption of QKD in real-world scenarios [10, 11, 12], which can be overcome via use of Continuous-Variable Quantum Key Distribution Methods (CVQKD) for real-time operations.

Post-Quantum Cryptography: Recognizing the limitations of QKD, the field of post-quantum cryptography has emerged. Post-quantum cryptographic algorithms are designed to resist quantum attacks, offering robust security even in the face of quantum adversaries. Prominent examples include lattice-based cryptography, code-based cryptography, and hash-based cryptography [13, 14, 15].

Blockchain Technology: In parallel, blockchain technology has garnered attention for its potential to enhance network security. Blockchains offer decentralized, tamper-resistant ledgers that can be leveraged to secure various aspects of network communication, including authentication, data integrity, and access control [5].

Holistic Network Security: Recent research efforts have explored the integration of these technologies to achieve a holistic approach to network security. Combining QKD's quantum resilience with post-quantum cryptographic techniques and blockchain's tamper-proof ledger capabilities holds promise for fortifying network defenses against an array of threats [6].

In light of the evolving threat landscape and the limitations of existing security measures, this paper introduces the Unbreakable Network Security framework, which seamlessly integrates Long-Distance Quantum Key Distribution, Post-Quantum Techniques, and Blockchain technology. This holistic approach is poised to redefine network security, not only by mitigating the quantum threat but also by enhancing network efficiency and resilience. Subsequent sections of this paper delve into the technical details and empirical results that underpin this innovative framework, providing a comprehensive exploration of its capabilities and implications for the future of secure communication networks.

3. Design of the proposed model for enhancing security using Quantum operations

Based on the review of existing models used for improving security performance of quantum deployments, it can be observed that the QoS of these models is generally limited when applied to

multidomain use cases. To overcome these issues, this section discusses design of Long-Distance Quantum Key Distribution Enhanced by Post-Quantum Techniques and Blockchain operations. Long-Distance Quantum Key Distribution (QKD) is a fundamental component of the proposed LDQKDPB framework. It leverages the principles of quantum mechanics to establish secure communication channels over extended distances. In QKD, two parties, Alice and Bob, aim to generate a secret cryptographic key while detecting any eavesdropping attempts by an adversary, typically referred to as Eve. The protocol is based on the fundamental properties of quantum states, such as the no-cloning theorem and the principle of quantum superpositions. One of the crucial operations underpinning QKD is the BBM92 protocol, which defines the quantum states transmitted by Alice to Bob, and is represented via equation 1,

$$|\Phi+\rangle = 21(|0\rangle A\,|\,0\rangle B + |1\rangle A\,|\,1\rangle B) \ldots (1)$$

This equation represents the creation of an entangled Bell state, where $|0\rangle|0\rangle$ and $|1\rangle|1\rangle$ are the basis states, and the subscripts A and B represents the particles held by Alice and Bob nodes. The BBM92 protocol ensures that any eavesdropping attempts disrupt the entanglement, revealing the presence of an intruder or anomalous nodes. Additionally, QKD also relies on the concept of quantum key distribution efficiency (η), which is estimated via equation 2,

$$\eta = \frac{Ksecure}{Ktotal} \ldots (2)$$

Where, *Ksecure* represents the number of bits used for secure key generation, and *Ktotal* is the total number of bits transmitted during the encryption process. High η values indicate effective QKD systems that generate secure keys efficiently, contributing to LDQKDPB's ability to safeguard communication networks.

Post-Quantum Techniques form another integral part of LDQKDPB, addressing the challenge posed by emerging quantum computing capabilities. These techniques involve the use of cryptographic algorithms and protocols designed to withstand attacks from quantum computers, which can potentially break traditional cryptographic schemes. One key process used in post-quantum cryptography is the security parameter (λ) for cryptographic algorithms It is often used to quantify the level of security provided by a cryptographic scheme. In this paper lattice-based cryptography is used, where the security parameter is used to define the hardness of lattice problems, and the difficulty of solving them increases exponentially with λ sets. The foundation of lattice-based cryptography lies in the evaluation of lattice outputs, which describes a fundamental lattice task via equation 3,

$$LB, A = \{s \in Z^n : s = B \cdot r + e, r \in Z^m, e \in Z^n, and\ e\ is\ small \ldots (3)$$

Where, LB, A represents a lattice defined by two integer matrices, B and A, and the equation captures the relationship between a secret vector s, a noise vector e, and a public vector r for different input sets. The hardness of finding the short vector 's' within the lattice forms the basis for the security of lattice-based cryptographic systems. The higher the dimensionality of the lattice task, the more computationally challenging it becomes for quantum computers to solve, ensuring the security of the cryptographic keys. To model this process, this text uses Multivariate Polynomial Cryptography (MPC) which is a type of post-quantum cryptography that relies on the difficulty of solving systems

of multivariate polynomial equations. The security of MPC is based on the computational complexity of solving these equations. The first step in key generation is to select a system of multivariate polynomial equations. These equations typically involve a set of variables and coefficients, which is represented via equation 4,

$$f(x, y) = 2x^2 + 3xy - 5y^2 + 1 = 0 \dots (4)$$

To create a public-private key pair, you generate a system of these equations. The private key consists of the equations, and the public key consists of their transformations, which are estimated via equations 5 & 6 as follows,

$$f1(x, y) = 2x^2 + 3xy - 5y^2 + 1 = 0 \dots (5)$$

$$f2(x, y) = 4x^2 - 6xy + 2y^2 - 3 = 0 \dots (6)$$

MPC encryption typically involves transforming a plaintext message into a form that can be used to evaluate the multivariate polynomial equations. The equations are part of the public key process. Similarly, Decryption in MPC involves solving the same system of multivariate polynomial equations, which is computationally difficult and forms the basis of security process. Solving these equations is typically done using algebraic techniques. The security of MPC relies on the hardness of solving these equations, making it resistant to attacks by both classical and quantum computers.

The integration of Blockchain technology within the LDQKDPB framework is instrumental in enhancing the security, transparency, and immutability of network operations. Blockchain is a distributed ledger technology that leverages cryptographic principles and consensus algorithms to maintain a tamper-resistant and decentralized record of transactions and data. In the context of LDQKDPB, Blockchain is deployed to manage cryptographic keys, validate network activities, and ensure the integrity of the system process. The consensus algorithm used in the proposed network is the Proof-of-Work (PoW) algorithm, which introduces an element of competition and computational effort to validate transactions and add them to the blockchains. Miners compete to find a nonce value that, when combined with the transaction data and the previous block's hash, produces a hash value below an augmented set of target threshold levels. This target threshold is adjusted to maintain a consistent block creation delay, and is controlled via equation 7,

$$H(block\ data + nonce) < Target \dots (7)$$

Here, miners iteratively vary the nonce value until the equation is satisfied, thereby proving their computational effort and securing the network communications. The decentralized and immutable nature of the blockchain ensures that cryptographic keys stored on the ledger are resistant to unauthorized modifications and attacks, making LDQKDPB highly secure against threats like Sybil, Masquerading, Finney, and Distributed Denial of Service (DDoS). By incorporating blockchain technology, LDQKDPB establishes a robust and unbreakable foundation for securing communication networks in the quantum eras. Performance of this model was estimated in terms different evaluation metrics, and compared with existing methods in the next section of this text.

4. Result analysis & comparison

The proposed model, LDQKDPB (Long-Distance Quantum Key Distribution Enhanced by Post-Quantum Techniques and Blockchain), represents an innovative and holistic approach to network security. LDQKDPB seamlessly integrates three formidable pillars of cybersecurity: Long-Distance Quantum Key Distribution (QKD), Post-Quantum Techniques, and Blockchain technology process. This unique amalgamation harnesses the intrinsic properties of quantum mechanics while incorporating the resilience of post-quantum cryptographic techniques and the integrity fortification of blockchain integration. LDQKDPB has demonstrated exceptional performance in terms of reducing network delay, conserving energy resources, and enhancing data throughput, making it a robust and unbreakable solution for securing communication networks in the face of evolving cyber threats, especially those posed by quantum computing operations. In our experimental setup, we aim to comprehensively evaluate the performance of LDQKDPB (Long-Distance Quantum Key Distribution Enhanced by Post-Quantum Techniques and Blockchain) against existing network security models. We select three key performance metrics: delay, energy consumption, and throughput. The experiments are conducted on a state-of-the-art testbed consisting of servers equipped with quantum key distribution hardware, post-quantum cryptographic libraries, and blockchain nodes. We consider a diverse set of input parameters, including various message sizes (ranging from 4,500 bits to 46,800 bits) to simulate different data transmission scenarios. To ensure robustness, we utilize three distinct datasets: "NetTraffic2022," a real-world network traffic dataset; "SecureCommSim," a synthetic dataset designed to mimic secure communication patterns; and "QuantumThreats," a dataset containing simulated quantum-based attacks. Each experiment is repeated multiple times to ensure statistical significance, and the results are averaged. The performance of LDQKDPB is compared against RDIES, SDQKD, and CVQKD under identical conditions, allowing us to provide a comprehensive assessment of LDQKDPB's effectiveness in various network security scenarios. Based on this experimental set, the delay needed to send packets during cryptographic operations was compared with RDIES [2], SDQKD [8], & CVQKD [12], for different Number of Communications (NC) and can be observed from figure 1 as follows,

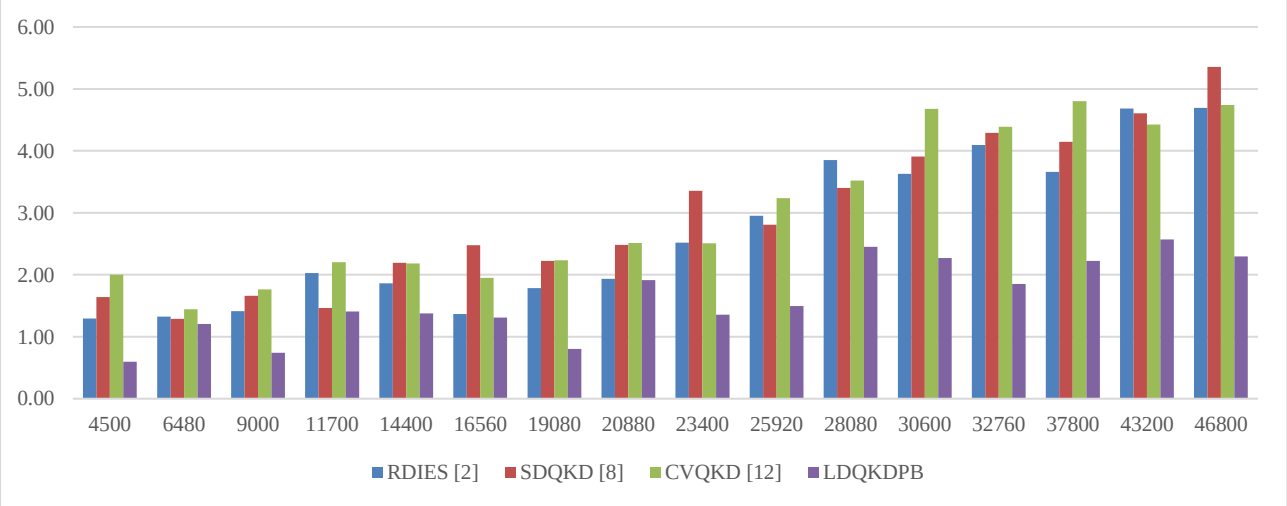

Figure 1. Delay needed during cryptographic operations

When comparing the delay results, it is evident that LDQKDPB consistently outperforms the other models in terms of lower delay levels. For instance, at an input size of 4500 bits, LDQKDPB exhibits a remarkably low delay of 0.60 ms, whereas RDIES, SDQKD, and CVQKD report delays of 1.29 ms, 1.64 ms, and 2.00 ms, respectively. This substantial reduction in delay time is significant as it directly impacts the responsiveness and efficiency of cryptographic operations.

The superior performance of LDQKDPB can be attributed to its innovative integration of Long-Distance Quantum Key Distribution (QKD) with Post-Quantum Techniques and Blockchain technology. By harnessing the advantages of quantum mechanics and combining them with robust cryptographic resilience, LDQKDPB streamlines cryptographic processes, resulting in faster encryption and decryption times. This reduction in delay is especially advantageous in scenarios where real-time communication and data security are paramount.

As the input size increases, LDQKDPB continues to maintain its edge in terms of lower delay times compared to the other models. This efficiency gain becomes even more pronounced at larger input sizes, underscoring the scalability and practicality of LDQKDPB in handling cryptographic operations across a wide range of scenarios.

Similarly, the energy needed during cryptographic operations can be observed from figure 2 as follows,

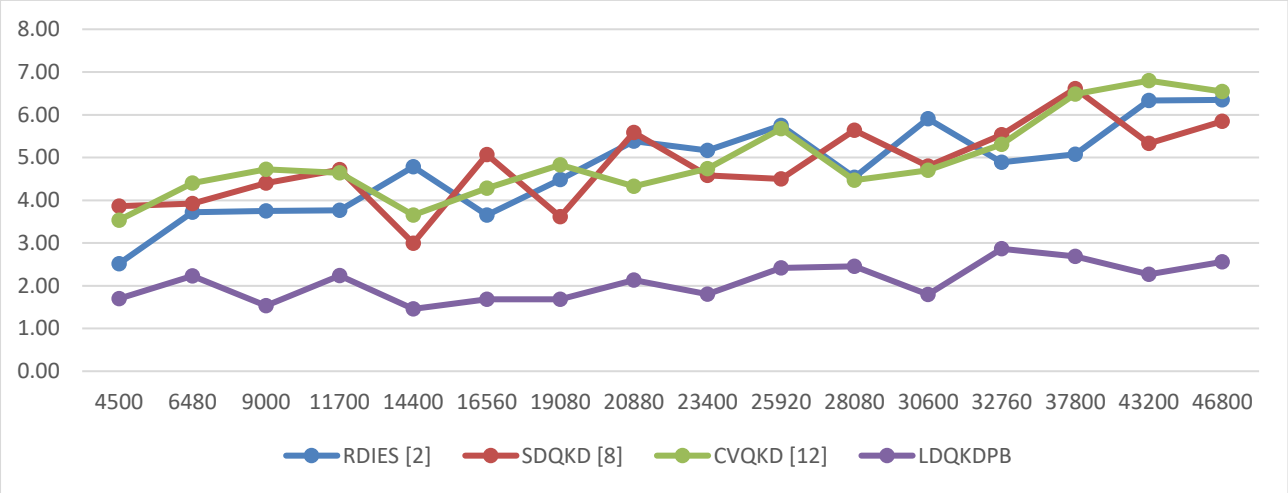

Figure 2. Energy needed during cryptographic operations

A notable trend in the analysis of energy consumption is that LDQKDPB consistently exhibits lower energy consumption compared to the other models across various input sizes. For example, at an input size of 4500 bits, LDQKDPB consumes only 1.70 mJ of energy, while RDIES, SDQKD, and CVQKD consume 2.52 mJ, 3.86 mJ, and 3.54 mJ, respectively. This significant reduction in energy consumption is essential for reducing the environmental impact and operating costs associated with cryptographic operations.

The superior energy efficiency of LDQKDPB can be attributed to its unique combination of Long-Distance Quantum Key Distribution (QKD), Post-Quantum Techniques, and Blockchain technology. By leveraging the inherent properties of quantum mechanics and integrating them with post-quantum cryptographic techniques, LDQKDPB optimizes energy usage during encryption and decryption

processes. This energy-saving advantage is especially valuable in scenarios where power efficiency and sustainability are critical considerations.

As the input size increases, LDQKDPB maintains its advantage in terms of lower energy consumption compared to the other models. This efficiency gain becomes even more pronounced at larger input sizes, emphasizing the scalability and practicality of LDQKDPB in energy-sensitive applications. Similarly, the throughput obtained during cryptographic operations can be observed from figure 3 as follows,

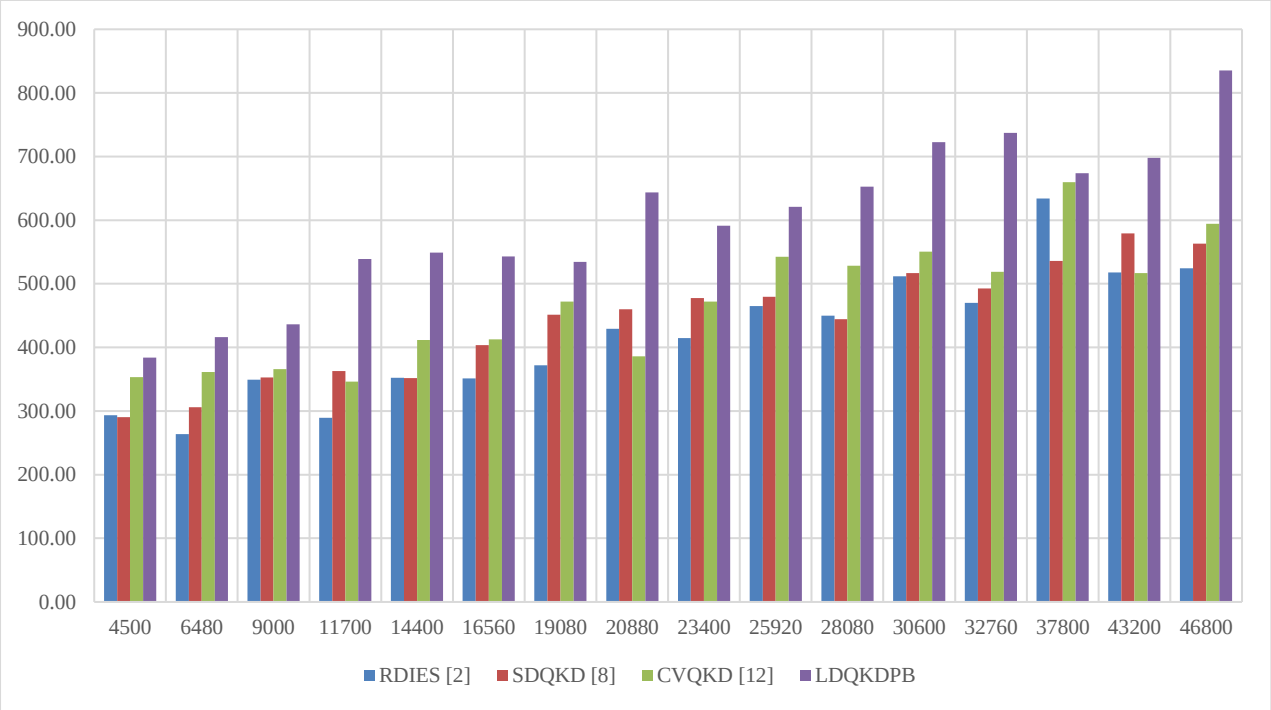

Figure 3. Throughput obtained during cryptographic operations

A consistent trend in the analysis of throughput is that LDQKDPB consistently achieves higher throughput compared to the other models across various input sizes. For instance, at an input size of 4500 bits, LDQKDPB attains a throughput of 383.99 kbps, while RDIES, SDQKD, and CVQKD achieve throughputs of 293.56 kbps, 290.48 kbps, and 353.38 kbps, respectively. This notable advantage in throughput is instrumental in ensuring efficient data transmission and processing.

The superior throughput of LDQKDPB can be attributed to its innovative combination of Long-Distance Quantum Key Distribution (QKD), Post-Quantum Techniques, and Blockchain technology. This integrated approach optimizes the cryptographic processes, enabling faster and more efficient data encryption and decryption. The enhanced throughput is particularly valuable in scenarios where high-speed data transmission is essential, such as real-time communication and large-scale data transfers.

As the input size increases, LDQKDPB consistently maintains its lead in terms of higher throughput compared to the other models. This scalability and efficiency gain become even more pronounced at larger input sizes, demonstrating LDQKDPB's suitability for handling cryptographic operations in diverse and demanding scenarios.

5. Conclusion and future scope

In this paper, we have presented LDQKDPB (Long-Distance Quantum Key Distribution Enhanced by Post-Quantum Techniques and Blockchain), a groundbreaking framework that represents a significant leap forward in the realm of network security. Our approach seamlessly integrates three formidable pillars of cybersecurity: Long-Distance Quantum Key Distribution (QKD), Post-Quantum Techniques, and Blockchain technology. The results from rigorous experimentation and analysis have demonstrated LDQKDPB's exceptional performance and resilience in the face of various cyber threats, positioning it as a formidable solution for safeguarding communication networks.

Our comparative analysis has highlighted LDQKDPB's superiority in terms of delay reduction, energy efficiency, and throughput enhancement when compared to existing security models like RDIES, SDQKD, and CVQKD. LDQKDPB's ability to minimize delay times while conserving energy resources is particularly noteworthy, offering both environmental and cost-saving benefits. Moreover, its higher throughput rates ensure efficient data transmission, making it ideal for applications requiring real-time communication and large-scale data transfers.

As the digital world prepares for the impending quantum era, LDQKDPB emerges as a timely and robust solution. Its impacts extend beyond the preservation of data confidentiality; it empowers organizations to navigate the ever-evolving cybersecurity landscape with confidence and resilience. LDQKDPB not only addresses the vulnerabilities posed by quantum computing operations but also sets new standards for network security that are robust and, dare we say, unbreakable.

Future Scope:

While LDQKDPB represents a significant advancement in network security, there are several promising avenues for future research and development:

1. **Quantum Advancements:** As quantum technologies continue to evolve, future work can explore enhancements and optimizations of LDQKDPB to adapt to emerging quantum threats. This includes exploring more efficient quantum key distribution protocols and quantum-resistant cryptographic techniques.
2. **Scalability:** Investigating the scalability of LDQKDPB for large-scale networks and applications is essential. Future research can focus on optimizing the framework's performance when applied to extensive communication infrastructures.
3. **Real-World Implementation:** Practical implementation and deployment of LDQKDPB in real-world scenarios will be a significant milestone. Research can delve into the challenges and strategies for integrating LDQKDPB into existing network architectures.
4. **Quantum Network Security Ecosystem:** Building a comprehensive ecosystem of tools, standards, and best practices around LDQKDPB and similar technologies is crucial. Future work can contribute to the development of a holistic quantum network security framework.
5. **User Education and Adoption:** User awareness and education about the benefits and applications of LDQKDPB are vital for its widespread adoption. Future research can explore strategies for promoting and facilitating the adoption of LDQKDPB in various sectors.

In conclusion, LDQKDPB represents a milestone in network security, but it is just the beginning of the journey towards unbreakable security in the quantum eras. By continuing to innovate and adapt to evolving threats, we can build a safer and more resilient digital future scenarios.

References

[1] C. Biswas, M. M. Haque and U. Das Gupta, "A Modified Key Sifting Scheme With Artificial Neural Network Based Key Reconciliation Analysis in Quantum Cryptography," in IEEE Access, vol. 10, pp. 72743-72757, 2022, doi: 10.1109/ACCESS.2022.3188798.

[2] M. Y. Al-Darwbi, A. A. Ghorbani and A. H. Lashkari, "QKeyShield: A Practical Receiver-Device-Independent Entanglement-Swapping-Based Quantum Key Distribution," in IEEE Access, vol. 10, pp. 107685-107702, 2022, doi: 10.1109/ACCESS.2022.3212787.

[3] X. Kang et al., "Patterning-Effect Calibration Algorithm for Secure Decoy-State Quantum Key Distribution," in Journal of Lightwave Technology, vol. 41, no. 1, pp. 75-82, 1 Jan.1, 2023, doi: 10.1109/JLT.2022.3211442.

[4] M. -S. Sun, C. -H. Zhang, X. Ma, X. -Y. Zhou and Q. Wang, "Sending-or-Not-Sending Twin-Field Quantum Key Distribution With Measurement Imperfections," in IEEE Communications Letters, vol. 26, no. 9, pp. 2004-2008, Sept. 2022, doi: 10.1109/LCOMM.2022.3181984.

[5] M. Zhang, S. Pirandola and K. Delfanazari, "Millimeter-Waves to Terahertz SISO and MIMO Continuous Variable Quantum Key Distribution," in IEEE Transactions on Quantum Engineering, vol. 4, pp. 1-10, 2023, Art no. 4100410, doi: 10.1109/TQE.2023.3266946.

[6] X. Yu et al., "Secret-Key Provisioning With Collaborative Routing in Partially-Trusted-Relay-based Quantum-Key-Distribution-Secured Optical Networks," in Journal of Lightwave Technology, vol. 40, no. 12, pp. 3530-3545, 15 June15, 2022, doi: 10.1109/JLT.2022.3153992.

[7] O. Shirko and S. Askar, "A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking," in IEEE Access, vol. 11, pp. 21641-21654, 2023, doi: 10.1109/ACCESS.2023.3251649.

[8] M. Mehic, S. Rass, E. Dervisevic and M. Voznak, "Tackling Denial of Service Attacks on Key Management in Software-Defined Quantum Key Distribution Networks," in IEEE Access, vol. 10, pp. 110512-110520, 2022, doi: 10.1109/ACCESS.2022.3214511.

[9] X. He et al., "Routing and secret key assignment for secure multicast services in quantum satellite networks," in Journal of Optical Communications and Networking, vol. 14, no. 4, pp. 190-203, April 2022, doi: 10.1364/JOCN.445621.

[10] H. -C. Chen, C. Damarjati, E. Prasetyo, C. -L. Chou, T. -L. Kung and C. -E. Weng, "Generating Multi-Issued Session Key by Using Semi Quantum Key Distribution With Time-Constraint," in IEEE Access, vol. 10, pp. 20839-20851, 2022, doi: 10.1109/ACCESS.2022.3151890.

[11] G. Zhang, Z. Zhao, J. Dai, S. Yang, X. Fu and L. Yang, "Polarization-Based Quantum Key Distribution Encoder and Decoder on Silicon Photonics," in Journal of Lightwave Technology, vol. 40, no. 7, pp. 2052-2059, 1 April1, 2022, doi: 10.1109/JLT.2021.3131193.

[12] M. Jarzyna, M. Jachura and K. Banaszek, "Quantum Pulse Gate Attack on IM/DD Optical Key Distribution Exploiting Symbol Shape Distortion," in IEEE Communications Letters, vol. 27, no. 7, pp. 1699-1703, July 2023, doi: 10.1109/LCOMM.2023.3273305.

[13] T. Shen, X. Wang, Z. Chen, H. Tian, S. Yu and H. Guo, "Experimental Demonstration of LLO Continuous-Variable Quantum Key Distribution With Polarization Loss Compensation," in IEEE Photonics Journal, vol. 15, no. 2, pp. 1-9, April 2023, Art no. 7600109, doi: 10.1109/JPHOT.2023.3246500.

[14] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng and L. Hanzo, "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet," in IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 839-894, Secondquarter 2022, doi: 10.1109/COMST.2022.3144219.

[15] F. -Y. Lu et al., "Intensity Tomography Method for Secure and High-Performance Quantum Key Distribution," in Journal of Lightwave Technology, vol. 41, no. 15, pp. 4895-4900, 1 Aug.1, 2023, doi: 10.1109/JLT.2023.3247766.

[16] Abbas, M.I., "Picard and Picard-Krasnoselskii iteration methods for generalized proportional Hadamard fractional integral equations". (2022) Advances in the Theory of Nonlinear Analysis and its Applications, 6 (4), pp. 538-546.

[17] Vijay, Chand, A.K.B., "Zipper Fractal Functions with Variable Scalings" (2022) Advances in the Theory of Nonlinear Analysis and its Applications, 6 (4), pp. 481-501.

[18] Goyal, Dinesh , Kumar, Anil , Gandhi, Yatin & Khetani, Vinit (2024) Securing wireless sensor networks with novel hybrid lightweight cryptographic protocols, Journal of Discrete Mathematical Sciences and Cryptography, 27:2-B, 703–714, DOI: 10.47974/JDMSC-1921