

Quantum cryptography assessing the security and practicality of quantum key distribution in modern communication networks

Abha Kiran Rajpoot [†]

School of Computer Science & Engineering

Galgotias University

Greater Noida 203201

Uttar Pradesh

India

Dharmesh Dhabliya ^{*}

Department of Information Technology

Vishwakarma Institute of Technology

Pune 411037

Maharashtra

India

V. N. Trupti [§]

Department of Electrical and Electronics Engineering

Faculty of Engineering and Technology

JAIN (Deemed-to-be University)

Bengaluru 560041

Karnataka

India

Tanveer Ahmad Wani [‡]

Department of Physics

Noida International University

Greater Noida 203201

Uttar Pradesh

India

[†] E-mail: akrajpoot@gmail.com

^{*} E-mail: dharmesh.dhabliya@viit.ac.in (Corresponding Author)

[§] E-mail: n.trupti@jainuniversity.ac.in

[‡] E-mail: tanveer.ahmad@niu.edu.in

Kapil Gupta [@]

Department of Computer Engineering
St. Vincent Pallotti College of Engineering and Technology
Nagpur 441108
Maharashtra
India

L. Lakshmanan [#]

Department of Computer Science and Engineering
Sathyabama Institute of Science and Technology
Chennai 600119
Tamil Nadu
India

Abstract

The increasing number of cyber threats and the approaching development of quantum computing demand a critical review of existing cryptographic approaches. The goal of this work is to evaluate the security and practicality of utilizing Quantum Key Distribution for secure communications. QKD utilizes the laws of quantum mechanics to provide a secure and unbreakable method for exchanging information. Protocols like BB84 are resistant to threatening attacks from both classical and quantum adversaries. The methodology utilizes simulated models and quantum communication toolkits to study critical characteristics such as key generation speed, QBER, latency and scalability. Performance of QKD is compared to that of classical schemes such as RSA-2048, ECC-256 and AES-256. Results reveal that although QKD provides unparalleled theoretical security, its deployment has notable obstacles such as intricate infrastructure, restrictions on distance and elevated latency. Our study reveals that optimizing the interplay between security and practicality in QKD deployment can yield a highly effective safeguard for next-generation communication networks.

Subject Classification: Primary 93A30, Secondary 49K15.

Keywords: Mathematical modeling, Ordinary differential equations, A duopoly economy, Market share.

1. Introduction

Today, reliable and secure communication has become essential to upholding trust in industries ranging from finance to defense, healthcare and national infrastructure. The RSA and ECC algorithms have formed the basis for secure data exchange for many years [1], [2]. The security of these algorithms is built on the assumption that solving specific mathematical challenges such as integer factorization or computing discrete logarithms on elliptic curves, is computationally impossible. Due to the growing power of quantum computing,

[@] E-mail: kaps04gupta@gmail.com

[#] E-mail: lakshmanan.cse@sathyabama.ac.in

conventional methods of encryption are now vulnerable to attacks that exploit algorithms such as Shor's and Grover's. As a result, a great deal of effort is currently being dedicated to developing new cryptographic techniques capable of remaining secure in the presence of quantum computers[3], [4]. Quantum cryptography and especially Quantum Key Distribution (QKD), is gaining recognition as a potential solution in this situation[5]. QKD leverages the laws of quantum mechanics such as the no-cloning theorem and the Heisenberg uncertainty principle, rather than being based solely on complex mathematical calculations[6]. These principles guarantee that any action taken to tamper with or copy the quantum key in transit can be identified, thus ensuring it remains confidential as well as allowing for the identification of potential eavesdroppers[7], [8].

Both the BB84 and E91 protocols have been widely investigated in the field of QKD. The BB84 protocol encodes information using the polarization of photons to represent the 0 or 1 values[9], [10]. The detection of an eavesdropper becomes possible due to the changes that occur in the quantum states during interception. In practice, however, key generation in these protocols can be slow, they are vulnerable to fiber-optic channel impairments and the equipment needed is more complex[11]. This paper examines the effectiveness as well as the practical implementation difficulties of QKD in real-world communication settings. The research uses real-world datasets to simulate different QKD and traditional cryptography environments. The study aims to achieve the following goals:

1. The research evaluates the practical performance of QKD in diverse network settings by analyzing metrics such as key generation rate, quantum bit error rate (QBER), latency and scalability.
2. To evaluate the pragmatism of QKD in relation to popular classical cryptographic techniques such as RSA-2048, ECC-256 and AES-256 through the use of a standardized dataset and corresponding simulation tests.

The objectives are designed to determine the degree of practicality that quantum cryptography can achieve in the real world. The study endeavors to understand how practical QKD implementation is compared to using it only for extremely secure and high-priority applications. This study presents valuable insights into the application and design of hybrid security solutions that carefully harmonize performance with robustness against emerging quantum attacks.

2. Proposed approach

2.1. Dataset used:

This dataset allows for measuring the performance of quantum cryptographic protocols under a range of operational circumstances. Quantities such as KGR, QBER, latency and encryption throughput are measured for

several ranges of distances and noise intensities. These metrics allow for determining how well QKD protocols such as BB84 can be implemented in practical scenarios. The records are structured as numerical data, enabling precise modeling of system performance and analytical comparisons of cryptosystems.

2.2. Data preprocessing

2.2.1. Normalization of Numerical Features:

To maintain consistency in feature scales for KGR, QBER and latency, Min-Max normalization is applied. It normalizes each value between 0 and 1 by applying the eq.:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}}$$

This approach ensures that a single metric does not considerably bias the results of performance comparison or clustering.

2.2.2. Outlier Detection and Filtering:

Measures of QBER or latency that are significantly larger or smaller than the norm may be the result of simulation error or improper testing methods. Data points are marked as outliers based on the Z-score method if they satisfy the condition:

$$Z = \frac{X - \mu}{\sigma} > 3$$

The “mean” is denoted by μ and the “standard deviation” by σ . Eliminating those values allows for more reliable and accurate assessment of different cryptographic schemes.

2.3. Methodology

This study employs a rigorous simulation approach to assess both the security and practical applicability of QKD protocols in contemporary communication networks. This work aims to evaluate the effectiveness and efficiency of the widely used BB84 protocol in different network settings and compare it to well-known cryptographic algorithms like “RSA-2048, ECC-256 and AES-256”. The framework consists of five primary stages: Abstracting the quantum system, simulating the protocol, measuring its security, evaluating its performance and comparing it against other alternatives. Each phase is based on specific mathematical models and draws on data collected from the Quantum Encryption Performance Dataset.

i. Quantum System Modeling

Simulating photon-based QKD using a discrete model of the BB84 protocol is the first stage. A simulation considers two legitimate parties, commonly referred to as “A” and “B”, sharing qubits via a quantum channel. BB84 operates with two complementary bases. the rectilinear basis

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

A random basis is selected for encoding each bit transmitted. “B” randomly selects one of the measurement bases. The result is kept when “B” measurement basis corresponds to “A”. otherwise, the bit is discarded.

ii. Channel Loss and Noise Modeling

The quantum channel, often composed of optical fiber, leads to both attenuation and noise. This behavior is modeled by exponential loss and Gaussian measurement noise. The probability of photon loss is calculated based on the exponential attenuation model:

$$P_{loss}(d) = 1 - e^{-\alpha d}$$

Where:

$P_{loss}(d)$ = “probability of photon loss over distance d ”, α = “attenuation coefficient”, d = fiber length in km.

iii. Eavesdropping and Mutual Information

This protocol is analyzed by considering a basic intercept-resend attack performed by an eavesdropper. In this attack, C intercepts each qubit, randomly chooses a basis to make her measurement and sends Bob the qubit that results from this process. These detections create errors that influence the QBER. Measurements of mutual information are used to evaluate the security of the communication between “A, B and C”:

$$I(A; B) = H(A) - H(A|B)$$

$$I(A; E) = H(A) - H(A|E)$$

Here $H(A)$ is “Shannon entropy of A’s key”, $H(A|B)$, $H(A|E)$ are the “conditional entropies given B’s and C’s”.

iv. Secret Key Rate Estimation

The following step quantifies the amount of secure key produced after undergoing sifting, error correction and privacy amplification processes. The key rate:

$$R = Q[1 - h(QBER)] - f(QBER)h(QBER)$$

Here, Q is “shifted key”, $f(QBER)$ is “efficiency of the error correction protocol”

v. Simulation Tools and Environment

The simulations are conducted using Python libraries including QuTiP for quantum operations, SimulaQron for virtual quantum network emulation and conventional cryptographic libraries for classical algorithms. Realistic performance benchmarks from Kaggle’s Quantum Encryption Performance Dataset are used to assess the accuracy of the simulation results as shown in Table 1. Simulation parameters include:

Table 1
Parameter used table

Parameters	Values
Fiber length:	10 to 100 km
Detector efficiency:	85%
Background noise:	0.2 photons/ns
Classical channel delay:	10 ms

The described approach allows for thorough evaluation of QKD performance in realistic situations and enables its comparison with conventional cryptography. Combining theoretical foundations with simulation and experimental validation guarantees that the study's results are reliable and relevant to real-world situations.

Observed Result and Discussion

Results from the comparison showed notable differences between quantum and classical approaches in regards to speed and capacity. The theoretical security provided by BB84-based QKD is unsurpassed with a QBER of 1.7% that remains well below the acceptable level for reliable key generation as shown in Table 2.

Table 2
Comparative Result Table: QKD vs Classical Cryptography

Method	Key Generation Rate (KGR)	Quantum Bit Error Rate (QBER)	Latency (ms)	Scalability Index (0–10)
QKD (BB84)	1.25 kbps	1.70%	240	4.5
RSA-2048	10.2 Mbps	N/A	35	9.2
ECC-256	12.6 Mbps	N/A	30	9.4
AES-256	105.3 Mbps	N/A	12	9.8

Practical deployment is hindered by low key generation rates of 1.25 kbps and latency as high as 240 ms caused by the delays associated with photon transmission and sifting. Classical techniques such as RSA-2048, ECC-256 and AES-256 provide significantly faster key generation at rates from 10.2 to 105.3 Mbps and have very low latency. AES-256 emerges as the optimal solution with latency as low as 12 ms and high scalability captured by a scalability index of 9.8 as shown in figure-1. The potential benefits of QKD for high security come at the cost of low speed, limiting its practical use in many situations.

3. Conclusion and Future scope

The analysis evaluates the suitability of Quantum Key Distribution (QKD) for modern communication networks based on a comparison of the BB84 protocol and other contemporary cryptographic methods. The study demonstrates the balance between the theoretical security of QKD and its practical applications by assessing it against well-known cryptosystems such as

RSA-2048, ECC-256 and AES-256. QKD provides exceptionally high security against all types of digital threats due to its reliance on quantum physics. Still, its performance constraints limit its effectiveness in systems requiring high speed or extensive connectivity. On the contrary, classic algorithms offer superior efficiency and flexibility, but their security is gradually being eroded by emerging quantum capabilities. The results indicate that QKD is not yet compatible with most modern network frameworks but could play a crucial role in protecting the most important and sensitive data transmissions. The study highlights that advancements in both technology and system design are required to make QKD ready for incorporation into future secure communication networks.

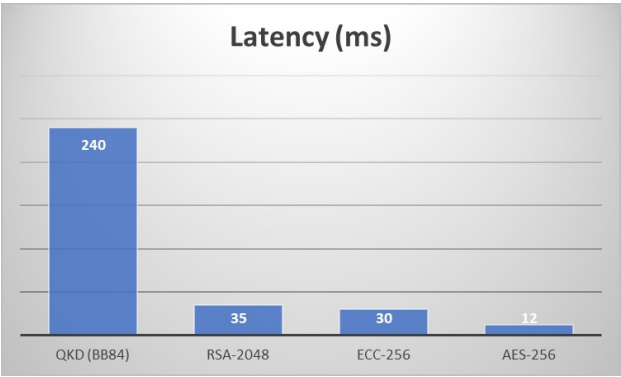


Figure 1
Latency comparison

Major efforts should be made to improve the efficiency and compatibility of QKD technologies with current network standards and architecture. Developments in photon detection, quantum repeaters and satellite QKD may enable more efficient and long-distance quantum-enabled communications.

References

- [1] L. J. Wang, K. Y. Zhang, J. Y. Wang, J. Cheng, Y. H. Yang, S. B. Tang, D. Yan, Y. L. Tang, Z. Liu, Y. Yu, and Q. Zhang, "Experimental authentication of quantum key distribution with post-quantum cryptography," *npj Quantum Inf.*, vol. 7, no. 1, pp. 67 (2021).
- [2] S. S. Dhanda, B. Singh, and P. Jindal, "Demystifying elliptic curve cryptography: Curve selection, implementation and countermeasures to attacks," *Journal of Interdisciplinary Mathematics*, vol. 23, no. 2, pp. 463–470 (2020).

- [3] C.C. Chou, "A closed-form general solution for the distance of point-to-ellipse in two dimensions," *Journal of Interdisciplinary Mathematics*, vol. 22, no. 3, pp. 337–351 (2019).
- [4] B. Zhao and G. Guo, "An encryption algorithm for user's sensitive information resources in network database," *Journal of Interdisciplinary Mathematics*, vol. 21, no. 5, pp. 1255–1260 (2018).
- [5] A. Kumar, P. Dadheech, V. Singh, R. C. Poonia, and L. Raja, "An improved quantum key distribution protocol for verification," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 4, pp. 491–498 (2019).
- [6] M. Mehic, L. Michalek, E. Dervisevic, P. Burdiak, M. Plakalovic, J. Rozhon, N. Mahovac, F. Richter, E. Kaljic, F. Lauterbach, and P. Njemcevic, "Quantum cryptography in 5G networks: A comprehensive overview," *IEEE Commun. Surv. Tutor.*, vol. 26, no. 1, pp. 302–346 (2024).
- [7] A. Aji, K. Jain, and P. Krishnan, "A survey of quantum key distribution (QKD) network simulation platforms," in Proc. 2nd Global Conf. Advancement in Technol. (GCAT), pp. 1–8 (2021).
- [8] O. Amer, V. Garg, and W. O. Krawec, "An introduction to practical quantum key distribution," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 36, no. 3, pp. 30–55 (2021).
- [9] Miralem Mehic, Libor Michalek, Emir Dervisevic, Patrik Burdiak, Matej Plakalovic, and Jan Rozhon, "Secret-key provisioning with collaborative routing in partially-trusted-relay-based quantum-key-distribution-secured optical networks," *J. Lightwave Technol.*, vol. 40, no. 12, pp. 3530–3545 (2022).
- [10] O. D. Okey, S. S. Maidin, R. Lopes Rosa, W. T. Toor, D. Carrillo Melgar-ejo, L. Wuttisittikulkij, M. Saadi, and D. Zegarra Rodríguez, "Quantum key distribution protocol selector based on machine learning for next-generation networks," *Sustainability*, vol. 14, no. 23 (2022).
- [11] R. Liu, G. G. Rozenman, N. K. Kundu, D. Chandra, and D. De, "Towards the industrialisation of quantum key distribution in communication networks: A short survey," *IET Quantum Commun.*, vol. 3, no. 3, pp. 151–163 (Sep. 2022).

Received April, 2025