ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 03 March 2026

Analysis of the Robustness of Quatum Key Disnribution Protocols to Noise, Losses and Adversarial Attacks

Kaskarauov Adilet

Kazakh-British Technical University, Almaty, Kazakhstan
Email: kaskarauov.adilet@gmail.com

Abstract— The development of quantum systems leads to new challenges regarding information security mechanisms. In this regard, specialists are required to create alternative methods of information protection, especially in quantum cryptography. An important role is played by the study of the resilience of Quantum Key Distribution (QKD) protocols. Objective: to conduct a comprehensive study of the resilience of quantum cryptographic key distribution protocols in the face of various types of attacks, noise, communication channel losses, and in the process of assessing their reliability. Methods used in the course of the research activities: theoretical analysis, modeling, simulation of attack scenarios, and experimental verification on specialized quantum simulators. The research activities were aimed at evaluating the efficiency of protocols, the error rate (QBER), the level of key secrecy, and their resilience to external influences. The research results demonstrated the impact of different types of attacks on protocol performance. It was found that the efficiency of the BB84 and CV-QKD protocols decreases with increasing noise and losses, while E91 showed higher stability. At the same time, the mechanisms of decoy states protection, privacy amplification, and error correction play an important role in enhancing resilience. The obtained results can be applied in scientific and practical research, as well as in work on the effective implementation of quantum communication systems in real-world conditions.

Index Terms— BB84, Noise and Losses in the Channel, Quantum Key Distribution, Quantum Attacks

I. INTRODUCTION

Rapidly developing quantum technologies have led to the emergence of full-scale quantum computers, which has created a demand in this field of science for the development of methods that provide cryptographic protection. A number of quantum algorithms pose a direct threat to cryptographic security [1].One of them is Shor's algorithm, which poses a threat when interacting with classical asymmetric algorithms such as RSA and ECC. This also includes Grover's algorithm, which affects the resilience of symmetric algorithms and hash functions. Based on the information reviewed, it can be concluded that developing information protection mechanisms is relevant, and these mechanisms should be based on the fundamental laws of quantum physics, namely quantum cryptography. Our research focuses on the use of the quantum key distribution (QKD) protocol, which enables secure key exchange between two parties using cryptography and allows detection of any attempts to intercept the transmitted information. In theoretical considerations, these protocols are considered to provide a high level of security, but in practical application, there are various factors that affect their reliability [2]. These include: channel noise, technical limitations of devices, and various types of attacks (particles, split photons, and typical man-in-the-middle type attacks).

The relevance of the topic under study is due to the fact that in modern realities it is necessary to thoroughly examine the robustness of quantum cryptographic protocols in practice, which will allow identifying the main threats and developing effective mechanisms to ensure the security of key exchange.

The purpose of this study is to study the resistance of quantum key distribution protocols (BB84, E91, CV-QKD) to various attacks and interferences and to develop recommendations for increasing their practical reliability.

To achieve the goals set in this work, the following solutions are used:

1. We perform a theoretical analysis and comparative characterization of the main QKD protocols;
2. Classify security threats and model their impact on various protocols;
3. Develop stability assessment criteria (QBER, transmission efficiency, basic confidentiality level);
4. We perform numerical simulations in a quantum simulator with different noise levels and attack effects;
5. We propose ways to increase the reliability of the protocol (use of unprocessed cases, improved confidentiality, error correction, etc.).

The scientific novelty of this study lies in the integrated approach to analyzing the stability of QKD protocols at the interface of theoretical models, simulation experiments and practical recommendations.

The experimental results and recommendations obtained can be used to design secure quantum communication systems, implement quantum cryptography in critical infrastructure devices, and develop a new generation of information security standards. Within the framework of our study, a comprehensive scientific approach was applied, including methods of theoretical analysis, mathematical

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 03 March 2026

modeling, and numerical simulations based on specialized software that evaluates the security of quantum cryptographic protocols. We conducted training of the BB84, E91, and CV-QKD protocols in the context of real and potential security threats.

In the process of applying the comparative analysis method, the differences in the design and function of the main quantum key distribution protocols were studied, and their weaknesses at the basic level were identified. The introduction of the simulation modeling method into research activities was aimed at conducting virtual tests of quantum transmission protocols in various situations, including in the category of detecting interference in the communication channel, under intercept-resend attacks, under photon number splitting attacks, and in man-in-the-middle scenarios.

As part of the implementation of the numerical experiment method into the research process, stability indicators such as the quantum bit error rate (QBER), key secrecy, and channel performance were studied, which are affected by changes in environmental factors including channel length, noise level, and attack frequency. To perform basic quantum operations and create a simulation sequence, Qiskit tools were used. Using the software QuNetSim and NetSquid, the modeling of quantum communication networks and the interaction process of participants under the influence of external factors is conducted.

II. MATERIALS AND METHODS

The study employs a comprehensive scientific approach, including mechanisms of theoretical analysis, mathematical modeling, and numerical simulations, using specialized software aimed at assessing the stability of quantum cryptographic protocols. The main focus is on the study of the BB84, E91, and CV-QKD protocols under real and potential security threats.

The comparative theoretical analysis method-to identify architectural and functional differences between the main QKD protocols and determine their vulnerabilities at the conceptual level.

The simulation modeling method-to conduct virtual experiments with the implementation of quantum protocols under various conditions: in the presence of noise in the channel, during interception attacks (Intercept-Resend), photon number splitting attacks (Photon Number Splitting), and also in Man-in-the-Middle conditions. Numerical experiment method-to assess the dynamics of changes in stability indicators (in particular, quantum bit error rate-QBER, key secrecy level, channel throughput) when varying environmental parameters (channel length, noise intensity, frequency of attack impacts) [3]. Simulation software and tools, such as Qiskit-to implement basic quantum operations and build simulation chains; QuNetSim or NetSquid-to simulate quantum communication networks and interaction of participants under external influences.

We use a combination of simulation tools to model the quantum processes. For the discrete-variable protocols (BB84 and E91), we leverage Qiskit (IBM's open-source quantum computing framework) to model quantum states and measurements, and we also develop custom Python code to simulate the transmission of photons and apply noise channels [4]. Qiskit reveals the characteristics of qubits and the application of quantum gates or Kraus channel operators, which helps in simulating polarization rotations or generating entangled pairs.

Consideration is given to a discrete-event simulator such as NetSquid, used for modeling quantum networks and performing network-level dynamics (simulating multiple consecutive transmissions or delays). This simulator accurately reproduces the processes of entanglement distribution and photon detection timing. Most of the analytical work was carried out using specially developed Python simulations for flexibility [5], [6]. A continuous-variable protocol was implemented using a custom simulator based on Python/NumPy, as the Qiskit framework does not natively support continuous-variable quantum states. In this CV simulator, we treat the quadrature values (e.g. electric field amplitudes) as random variables and propagate them through a modeled channel with loss and Gaussian noise. Throughout, we ensure that random number generation (for basis choices, bit values, etc.) is done with a high-quality pseudo-random source to mimic true quantum randomness for fair key generation.

Assumptions: In our models, we assume that Alice and Bob have ideal control over their encoding and decoding devices except for the specified imperfections (loss, noise, detector inefficiency, etc.). For BB84 and E91, we initially assume an ideal single-photon source for theory, but in realistic simulation we model Alice's source as a weak coherent pulse (WCP) with a given mean photon number (e.g. $\mu \approx 0.2$) to account for multi-photon emissions. Similarly, Bob's detectors are assumed to have a certain quantum efficiency (often 10-30%) and a nonzero dark count rate (spontaneous clicks without a photon). We assume the quantum channel is a standard telecom optical fiber with a specified attenuation (e.g. 0.2 dB/km loss), and we include typical misalignment errors (e.g. polarization misalignment by a small angle) to represent imperfect optics [7]. For CV-QKD, we assume Gaussian-modulated coherent states (unless otherwise specified) and that Bob uses an efficient homodyne or heterodyne detector with a shot-noise-limited performance.

All classical post-processing (sifting, error correction, privacy amplification) is assumed to be ideally implemented such that the main limitations to key rate come from quantum effects (loss, noise, and information leakage) rather than classical inefficiencies. During the research process, a hypothesis was formed that the efficiency of reconciliation β (often around 0.95 for CV-QKD), as represented in error correction codes in practical applications, is not 100% effective. As a result, there is a correlation with the data from QKD security analysis, thereby confirming the correspondence between our simulation and the theoretical limits.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 03 March 2026

III. RESULTS AND DISCUSSION

As noted earlier, our study employs a scientific approach that combines theoretical modeling and experimental activities in a simulation style. The physical experiment with equipment is replaced by computational simulations that imitate the behavior of QKD systems under various conditions. This approach is less complex and costly to organize compared to real quantum-optical experiments, allowing for faster integration of different scenarios. We implemented the BB84, E91, and CV-QKD protocols in creating the simulation environment, incorporating realistic noise and loss parameters during interactions with known attacks. The quantitative assessment of the "strength" and reliability of a protocol in generating secure keys is carried out during the analytical examination of the results of each simulation run. The analysis takes into account the evaluation criteria of the studied indicators. Through systematic changes in channel conditions and attack parameters, we conducted an assessment of the performance of each protocol and determined its security limits. This scientific method provides a controlled and reproducible way to test the robustness of protocols, in accordance with the fundamental principle of QKD, which is based on the fact that any eavesdropping attempts lead to detectable anomalies [8]. Simulations developed by us are aimed at testing situations where Eve (the interceptor) interferes with key exchange, while Alice and Bob detect changes (such as an increase in QBER or a decrease in correlation) beyond acceptable limits, which provides a theoretical proof of security.

In the process of modeling the BB84, E91, and CV-QKD protocols conducted under idealized conditions, certain informational data were identified. For this, ideal photon sources and detectors were used (high efficiency, no dark counts), the channel noise was zero (no excess Gaussian noise and bit errors), the signal did not attenuate when excluding operation with geometric scattering, and there were no interferences from eavesdropping or attack scenarios. A summary of the simulation configuration is presented in Table I.

Fig. 1 shows the behavior of QBER in the E91 protocol, based on entangled photon pairs for this experiment.

Based on the results of the study presented in Fig. 1, a smooth increase in the curve can be observed compared to BB84, which indicates higher reliability positively influenced by quantum entanglement. With an initial error rate of approximately 0.1 and a distance exceeding 80 km, the QBER remains below 0.4, demonstrating better stability [9]. However, beyond this point, a sharp increase is observed, caused by the limitations of photon detection and the deterioration of entanglement over long distances.

During the course of the research activities, it was found that the length of the channel for the BB84 protocol affects the increase in the quantum bit error rate (QBER). If ideal initial transmission conditions are established, the QBER remains below 0.2 within a range of 10 km. However, if the distance exceeds 20 km, a significant increase in the QBER is observed. When the distance reaches 100 km, the QBER begins to exceed 0.5, indicating a breach of the protocol's security threshold during long-distance transmission, which complicates compensation processes or error correction mechanisms.

It was also determined that the channel length in the CV-QKD protocol affects changes in the secret key rate (SKR), reflected in bits per pulse. Compared to metrics based on QBER, the SKR gradually decreases, which can be predicted as the distance increases, taking into account optical losses and the attenuation of modulated quadrature amplitudes. The conducted study showed a drop in the rate below 1.1 bits/pulse at a distance of 0 km; when transmitted over 100 km, the values drop to less than 0.4 bits/pulse, leading to the conclusion that the protocol is sensitive to the transmission coefficient and its internal Gaussian noise models. At the same time, an acceptable key transmission rate is maintained in channels with a medium range.

Under the idealized conditions used in our study, a clear basis is provided for evaluating the performance of quantum key distribution (QKD), but in real quantum communication channels, signals undergo attenuation, temperature fluctuations occur, detectors are inefficient, and external noise is present. Next, the modeling processes of the BB84, E91, and CV-QKD protocols under loss and noise conditions are considered, and through practical research activities, the mechanisms of practical resilience and vulnerabilities of each approach are demonstrated.

In the course of the research activity, it was determined that a sharp increase in noise in the BB84 protocol occurs under the influence of the quantum bit error rate (QBER). With moderate noise around 10%, the QBER approaches critical threshold values of 0.11, which leads to the formation of an insecure protocol that cannot be used for privacy amplification. If moderate noise increases to 20% or more, the QBER begins to exceed values of 0.2-0.25, making it impossible to generate keys without extensive error correction. Based on the results of the study, it was concluded that BB84 is sensitive to measurement errors and imperfections in photon detection.

It was established that the E91 protocol, based on entangled photon pairs, can function at an increased level of optical losses, expressed in decibels. This protocol is more robust compared to BB84 due to the use of entanglement instead of state preparation [10]. Nevertheless, an increase in QBER is observed with increasing distance and signal attenuation. The research results showed that if the loss is within 10 dB, equivalent to 50 km of standard optical fiber, the QBER values remain below 0.3, indicating the possibility of secure key generation. When losses exceed 15 dB, it leads to a rapid deterioration in performance due to the decoherence of entanglement and the loss of photon correlation.

Experimental activity has shown that an increase in noise in the BB84 protocol channel leads to an increase in the quantum bit error rate (QBER). When QBER exceeds 0.1, it quickly goes beyond acceptable limits during the threat to the security of the transmitted key. The greater the losses (dB) in the E91 protocol, the higher the likelihood of a stable increase

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 03 March 2026

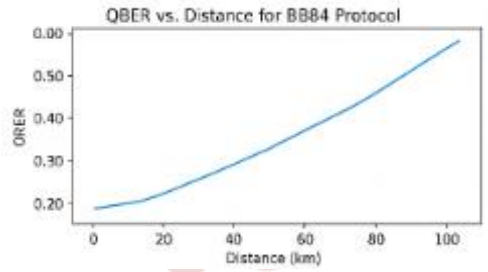
in QBER. In the E91 protocol, a gradual deterioration of performance is observed, which confirms a better level of resistance to losses compared to BB84.

Fig. 2 shows the results of a study on quantum key distribution and continuous-variable schemes (CV-QKD), as well as the secret key rate (SKR), which reflect a sharp drop as excess noise increases, even when no losses are observed in the channel. When the noise level reaches 0.005 SNU (shot noise units), the SKR decreases by more than 50%. When the excess noise level exceeds 0.01 SNU, the secret key rate begins to approach zero, which is due to the loss of the advantage of mutual information between legitimate participants and eavesdroppers. The identified behavioral aspects indicate that it is critically necessary to suppress noise and perform high-quality Gaussian modulation in the CV-QKD system.

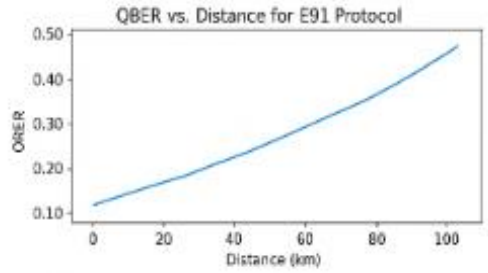
The research results presented in Fig. 2 show the impact of channel losses on the development of the SKR coefficient in relation to CV-QKD. The graph indicates that performance decreases gradually but sharply as losses increase. The SKR coefficient drops to more than half of its maximum value at a 5 dB loss. When losses reach 15 dB, the key rate approaches zero, making the protocol unsuitable for long communication lines unless advanced compensation methods such as quantum repeaters or trusted nodes are applied.

Table I. Simulation Configuration Summary

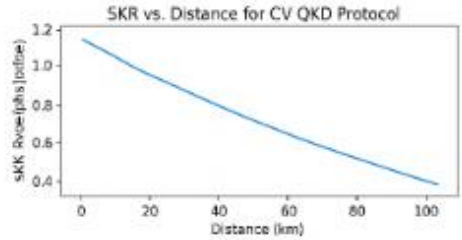
Parameter	Value
Detector Efficiency	1.0 (ideal)
Channel loss	O dB
Excess Noise (CV-QKD)	0 SNU
Number of qubits/coherent states	1000
Protocols simulated	BB84, E91, CV-QKD
Platform	Qiskid, Strawberry Fields



(A)



(B)



(C)

Fig 1. (A) QBER vs. Distance for BB84 Protocol (B) QBER vs. Distance for E91 Protocol SKR vs. (C) Distance for CV-QKD Protocol

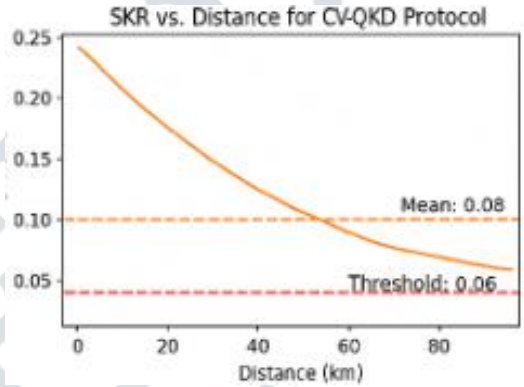


Fig 2. SKR vs. Noise in CV-QKD Protocol.

IV. CONCLUSION

The study presented in this article is aimed at a comprehensive examination and practical testing of the reliability, security, and practical application of quantum key distribution (QKD) protocols. The research activity employed theoretical data, algorithm development, and simulation experiments. Throughout the work on the material, all initial objectives were achieved, and answers were obtained to the main questions posed at the beginning of the study. The main goal of the research is to compare the stability and usefulness of the BB84, E91, and CV-QKD protocols. This goal was pursued through detailed simulations in both ideal and complex conditions. Within the framework of the research work, it was found that the security of QKD protocols is based on the principles of quantum physics, which include measurement disturbance and entanglement, and are in no way affected by computational complexities. During the study, three protocols were examined, and their mechanisms were tested based on these. For this purpose, a quantum environment was simulated using advanced tools: Qiskit, Strawberry Fields, NetSquid. The protocol data were subjected to various levels of noise, signal loss, and active attacks, during which their vulnerabilities were thoroughly studied and their resilience was assessed.

When working with the BB84 protocol, which is a basic method of preparation and measurement, a vulnerability to bit-flip errors and intercept-resend attacks was identified, especially during long-distance transmission or in conditions

of high noise. This problem is effectively addressed by decoy states and advanced error correction methods. If the data transmission conditions are controlled, the BB84 protocol functions fully and reliably. Conducting a study of the mechanisms of the E91 protocol, which uses entangled photon pairs, shows a stable level of resistance to attacks, detecting interference through Bell inequality tests. It is more effective in high-loss conditions, significantly outperforming the BB84 protocol. The E91 protocol is suitable for long-distance and critical communications. The fastest key generation is provided by the CV-QKD protocol, which integrates well with existing telecommunications systems. It is heavily influenced by additional noise levels, and there are difficulties in transmitting information over long distances. To improve this process, advanced error correction methods need to be applied.

The main result of the conducted study is the practical confirmation of channel factors, including distance, light transmission, and noise levels, which affect key performance indicators such as QBER, key rate, and entropy leakage.

The explanation and support of this relationship were carried out through numerous simulations, providing reliable and repeatable results. Additionally, within the scope of the research activities, the number of photons and the key length affecting security were considered, demonstrating that careful tuning of the studied factors maintains system reliability and prevents photon number splitting-type attacks.

From the perspective of the methodology of the simulation setup developed, it can be used for testing quantum key distribution. Open-source tools and standard settings were used to create it. During the use of the random number generator with specified seeds, identical results are ensured for all tests and correct recording of the obtained data. There is a guarantee that this measurement method can be applied by other studies for conducting experiments and their development.

The study was conducted in both ideal and real conditions, and within its framework, different ways of applying quantum key distribution in certain areas were considered (national security, banking, healthcare, energy, telecommunications, and cloud computing).

The presented results of research and experimental activities highlight the importance of studying and establishing the distribution of quantum keys as information technologies develop, which in the future will enable quantum computers to break traditional encryption methods. During the study, serious problems were identified in ensuring the effective operation of quantum key distribution and modern technologies. Specifically, quantum signals do not work with conventional repeaters, there are no good hybrid systems combining quantum and classical methods, and it is necessary to develop and improve international rules and standards.

Summing up the conducted research, we note the results obtained:

- answers were formulated regarding the security and usefulness of quantum key distribution;

- computer models of the three main types of quantum distribution: BB84, E91, and continuous variables-were created, allowing the user to control a number of factors such as noise, signal loss, and attacks;

- measurements and comparisons of the efficiency of various protocols were conducted using metrics such as key error rates, secret key rates, and entropy;

- the influence of the strengths and weaknesses of each protocol on real-world situations was identified and analyzed;

-methods for applying quantum key distribution were developed, system design recommendations and their implementation in real situations were provided, and directions for further research were outlined.

The results of the conducted study made it possible to confirm the safe quantum key distribution in both theoretical and practical activities with careful development and control. At present, they cannot fully replace traditional encryption methods in all areas, but in the future, these mechanisms will become key elements of future systems, combining quantum and classical protection to ensure information security in the quantum era.

REFERENCES

[1] W. Stephanie, D.Elkouss, R. Hanson. Quantum Internet: A Vision for the Road Ahead //Science. -2018.-Vol.362 (6412). -P.339-345. DOI 10.1126/science.aam9288.

[2] C. Surianarayanan, P. Raj. Integration of the internet of things and cloud: security challenges and solutions-A Review//Cloud Applications and Computing.-2023.-Vol.13(1).-P.45-53. DOI https://doi.org/10.4018/IJCAC.325624.

[3] J. Preskill. Quantum computing in the NISQ era and beyond // Quantum. – 2018. - Vol. 2 (1). -P. 79-83.

[4] C. Surianarayanan, P.R. Chelliah. Integration of the internet of things and cloud: security challenges and solutions-a review // Int. J. Cloud Appl. Comput. (IJCAC). – 2023. – Vol. 13 (1). – P. 12-15.

[5] M. Zhao, C. Shi, Y. Yuan. Blockchain-based lightweight authentication mechanisms for industrial internet of things and information systems // Int. J. Semant. Web Inf. Syst. (IJSWIS). – 2024. – Vol. 20 (1). – P. 18-20.

[6] Q. Zheng, X. Wang, M.K. Khan, W. Zhang, et al. A lightweight authenticated encryption scheme based on chaotic SCML for railway cloud service // IEEE Access. – 2017. – Vol. 6 (1). – P. 711-722.

[7] Li, J. Wang, Z. Song. Privacy protection of cloud computing based on strong forward security // Int. J. Cloud Appl. Comput. (IJCAC). – 2023. – Vol. 13 (1). – P. 48-52.

[8] A. Dahiya, et al. A reputation score policy and Bayesian game theory based incentivized mechanism for DDos attacks mitigation and cyber defense // Future Gener. Comput. Syst. – 2021. – Vol. 117 (5). – P. 193-204.

[9] S. Pirandola. End-to-end capacities of a quantum communication network // Commun. Phys. – 2019. – Vol. 2 (1). – P. 51-54.

[10] I.B. Djordjevic. On global quantum communication networking // Entropy. – 2020. – Vol. 22 (8). – P. 831-836.