(ANPA Conference 2025)
ISSN: 2392-473X(Print), 2738-9537 (Online)

Research Article ©Nepal Physical Society
DOI: https://doi.org/10.3126/jnphyssoc.v11i1.87467

Quantum Key Distribution Using BB84 Protocol: A Computational Study of Error Rates

Abhinav Pokharel,[a)] Rupisha Dangol,[a)] and Hari K. Neupane[b)]

Amrit Campus, Tribhuvan University, Kathmandu, Nepal

[a)]*These authors contributed equally.*
[b)]*Corresponding author: hari.neupane@ac.tu.edu.np*

Abstract. Quantum key distribution (QKD) enables secure communication using the principles of quantum physics. The BB84 protocol is not only effective for secure key sharing but also for detecting eavesdropping. This study simulates a computational model of QKD and analyzes error rates under varying numbers of bits. Using Python-based simulations with $n = 10$, $n = 100$, and $n = 1000$ bits, and a fixed noise probability of 0.02, we evaluated scenarios both with and without eavesdropping over 1000 trials. The results show an average error rate of 2% without eavesdropping and over 26% with eavesdropping. Standard deviation increases with lower n, indicating higher variability. This study validates BB84's robustness under noise and demonstrates its sensitivity to third-party interference.

Received: August 10, 2025; **Revised**: October 12, 2025; **Accepted**: October 21, 2025

Keywords: BB84 protocol, quantum cryptography, QKD simulation, eavesdropping detection, QBER, photon polarization

1. INTRODUCTION

Modern communication systems rely heavily on the transmission of information over the internet. For a safe transmission of messages, modern systems utilize classical encryption standards such as RSA and AES to safely transmit data over the internet. These systems assume that certain mathematical problems are computationally infeasible to solve. For example, RSA is based on the hardness of integer factorization as originally proposed by Rivest, Shamir, and Adleman, who stated that "The security of the system relies on the difficulty of factoring the product of two large primes"[1]. AES, as designed by Daeman and Rijmen, operates through substitution-permutation networks and is considered highly efficient and secure for symmetric encryption [2].

However, with new waves of quantum computing, these cryptographic assumptions are under serious threat. Shor introduced a polynomial-time quantum algorithm capable of factoring large integers, which "can factor an L-bit number in roughly L^3 steps" [3], making RSA and AES encryption methods vulnerable. As Michele Mosca pointed out, "we must act urgently to mitigate this quantum threat" [4], emphasizing that quantum advancements may change current encryption standards, making them obsolete in near future. To address the threats that quantum computing might pose, scientists have turned towards the use of quantum cryptography, an emerging field that combines the fundamental principles of quantum physics to ensure data integrity and privacy. Unlike classical encryption methods which utilizes mathematical complexities, quantum key distribution (QKD) leverages phenomena such as superposition, entanglement, and the no-cloning theorem. Among the myriads of QKD protocols, the BB84 protocol introduced by Bennett and Brassard in 1984 is the most foundational and widely studied [5]. The BB84 protocol enables two parties to establish a shared secret key through the transmission of Quantum Bits (Qubits) encoded in the polarised state of single photons. The security of BB84 lies in the laws of Quantum Physics, not in computational assumptions, which results in a scenario where eavesdropping is inevitably detectable.

1.1 Quantum Key Distribution

Quantum key distribution is a method of secure communication that uses the laws of quantum physics to generate and exchange encryption keys.Its security arises

from the fundamental behavior of quantum particles: any attempt to observe or intercept the transmitted quantum bits results in an altered state, allowing communicating parties to detect eavesdropping. Unlike all classical methods of encryption, which depend on computational difficulty of mathematical problems, which might fail when quantum computers are developed, QKD provides information-theoretic security, meaning its security is not dependent on an adversary's computational power but is guaranteed by the physical laws governing quantum systems. This makes QKD a critical component for the future quantum-safe infrastructure that combines classical quantum-resistant algorithms with quantum cryptographic solutions [6, 7]. In this paper, we simulate the BB84 protocol, which was also the first quantum key distribution protocol proposed by Bennett and Brassard in 1984 [5], which laid the foundation for practical implementations of QKD.

1.2 Heisenberg Uncertainty Principle

The Heisenberg uncertainty principle is one of the fundamental principles of quantum mechanics. This principle presents a few postulates for the world around us. The following postulates hold grave importance in quantum computing.

- The measurement of position without disturbing the momentum is impossible, and the converse is also true.

- The position and momentum cannot be measured simultaneously. [9]

This principle applies to all the complementary quantum observables, including photon polarization states utilized by QKD. In the context of BB84 protocol, a photon polarization can be measured in two non-compatible bases (rectilinear or diagonal). When measured in wrong basis, photon state is disturbed, introducing errors. Thus, eavesdropping on a quantum message is therefore akin to making a measurement. In this way, the Heisenberg uncertainty principle underlines the security of QKD: any eavesdropper attempting to measure photons must choose a measurement basis, inevitably altering the quantum states and revealing their presence through an increased error rate. [10]

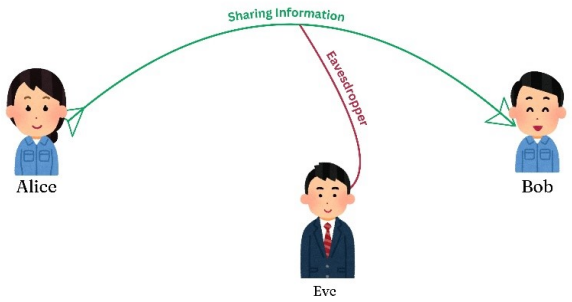

FIGURE 1: Sharing bits in presence of eavesdropper (Eve).

In the BB84 protocol, this uncertainty is implemented through two complementary polarization bases. When a photon is polarized through one basis and measured in the other, the measurement outcome becomes fundamentally random. Any eavesdropper measuring photons in wrong basis introduces detectable errors in the key exchange. The formal representation of bases of BB84 protocol are as follows:

1. $|0\rangle$ and $|1\rangle$ in rectilinear basis, where $|0\rangle = (1,0)$ and $|1\rangle = (0,1)$

2. $|+\rangle$ and $|-\rangle$ in the diagonal basis, where $|+\rangle = (1/\sqrt{2})$ $(1,1)$ and $|-\rangle = (1/\sqrt{2})$ $(1, -1)$

These two bases are mutually unbiased, meaning that photon prepared in one base has an equal probability of yielding either measurement outcome in the other. This property ensures that any eavesdropper attempting an intercept-resend attack will unavoidably disturb the transmitted quantum states, leading to an increased Quantum Bit Error Rate (QBER) that reveals intrusion[10]

Bases	0	1
Rectilinear	↕	↔
Diagonal	↗	↘

FIGURE 2: Representation of bit value and polarization state.

The working principle of BB84 protocol is shown in the figure below.

The working of BB84 protocol is explained through the following steps:

- **Alice's Random Bits:** Alice generates a random binary sequence.

Alice's Random Bits	0	1	0	1	0	0	0	1	0	0	1	1	0	1	0	1	0	0	1	1
Alice's Basis	D	R	D	D	R	R	D	R	D	D	D	R	R	R	D	R	D	D	R	R
Photons Alice Sends	↘	↕	↗	↗	⟷	↕	↘	⟷	↗	↘	↘	⟷	↕	↕	↗	⟷	↘	↗	⟷	↕
Random Receiving Bases	D	D	R	D	R	D	R	D	D	R	D	R	D	R	R	R	D	R	D	D
Bits Received By Bob	0	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	0	0	1	1
	✓			✓	✓			✓		✓	✓		✓		✓	✓				
Bob Reports bases of bits	D	D	R	D	R	D	R	D	D	R	D	R	D	R	R	R	D	R	D	D
Alice Reports Correct Bases	D			D	R			D		D	R			R			R	D		
Shared Information	1			1	0			0		1	1			1			1	0		
Random Key Bits Revealed by Bob				1				0						1				0		
Alice Confirms the Matches				✓				✓						✓				✓		
Remaining Shared Secret Bits	1				0					1	1						1			

D = Diagonal Base
R = Rectilinear Base

Note: This is an idealized situation where Bob receives all the bits, in real-world conditions Bob might fail to detect a photon. Reasons might include: Photon loss due to distance, timing issues, detector inefficiency, and environmental noise.

FIGURE 3: Working principle of BB84 protocol.

- **Alice's Basis:** Each bit is assigned a random basis: Diagonal (D) or Rectilinear (R).
- **Photon Transmission:** Bits are encoded into photons according to the selected bases and sent to Bob.
- **Random Receiving Bases:** Bob independently chooses random bases to measure the incoming photons.
- **Bits Received by Bob:** Measurement outcomes depend on whether Bob's chosen basis matches Alice's.
- **Bob Reports Bases of Bits:** Bob announces the bases he used over a public channel.
- **Alice Reports Correct Bases:** Alice identifies which of Bob's bases match her own.
- **Shared Information:** Only bits from matching bases are retained as the sifted key.
- **Random Key Bits Revealed by Bob:** A small sample of sifted bits is revealed to estimate the Quantum Bit Error Rate (QBER).
- **Alice Confirms the Matches:** Alice checks if the revealed bits correspond correctly to her originals.
- **Remaining Shared Secret Bits:** If the error rate is below threshold, the remaining bits form the final secure key.

2. METHODOLOGY

This paper performs a computational study of error rates of the BB84 protocol to examine how error rates vary under various number of bits (n) with and without the presence of eavesdropper while maintaining a constant noise probability. This custom written code was designed to simulate bits preparation, transmission, and measurement process of quantum key distribution.

A computational research design was adapted to evaluate the error rates in the BB84 protocol in quantum key distribution under controlled, repeatable conditions. Computational approach was the most appropriate one due to several reasons. Real-world quantum information systems are still in their early stages and are often inaccessible in regions like Nepal due to high cost, fragility, or limited availability. A simulation-based approach, therefore, allows us to explore the theoretical aspect of BB84 without the need of expensive physical quantum systems. With the same, computational approach easily allows us to precisely control all our parameters, such as, number of bits exchanged, absence or presence of eavesdropper, and the probability of noise. This level of control is difficult to achieve in physical experimental setups.

Moreover, simulations can be repeated multiple times to verify the consistency of results. This would also help us to observe statistical patterns and trends over extended period-of-time. Likewise, testing cryptographic methods raise ethical concerns in real world situations. Simulations offer risk-free environment to model and study such scenarios in detail. Lastly, use of computational methods helps to expand the usability of this paper for educational purpose. This computational design provides an effective, ethical, and reproducible framework to visualize, understand complex protocol like BB84's performance and pedagogical performance.

2.1 Simulation Design and Overview

The simulation reproduces the operational logic of the BB84 protocol. First, Alice generates a random sequence of bits representing the way key and assigns each bit a random polarization basis, rectilinear or diagonal, for photon encoding. Bob, the receiver, independently selects random filters to measure the encoded photons. When the bases of Alice and Bob match, Bob measures the correct bit value; when they differ, his result becomes random, reflecting quantum measurement uncertainty

To model eavesdropping, a memoryless intercept-resend attack is simulated. The eavesdropper measures each photon using random bases and resends each of them according to her measured basis. Because Eve does not know Alice's original basis, she measures some photons in the wrong basis, disturbing their quantum states, introducing errors in the comparison stage.

After transmission, Alice and Bob publicly compare their chosen bases over a classical channel and retain only those bits measured in matching bases. The key-sifting step produces a shared sifted key from which the Quantum Bit Error Rate (QBER) is obtained. The complete source code and implementation details are available in the GitHub repository linked in the Appendix.

2.2 Data Collection Method

In this study, data was collected through a custom-designed simulation of BB84 protocol. The entire process, from bit generation to transmission, measurement, and error calculation, was implemented in Python code. The data was not gathered from a physical source, but rather automatically generated through a computational simulation.

The following steps outline the process of data collection:
Parameter Definition: For each experiment run, key parameters were defined:

- Number of Bits (n): Varied across three values (10, 100, 1000).
- Noise Probability: Set to a constant value of 0.02.
- Presence of eavesdropper: Two cases — present and absent — to study both secure and compromised situations.

Each experiment was repeated over 1000 times to ensure statistical significance and minimize random fluctuations. Mean and standard deviation were computed.
In this study, the variables are defined as follows:

The noise probability was set at 0.02. This represents a mid-value commonly found in quantum communication literature (0.01–0.05) and aligns with typical quantum bit error rates in short-distance fiber optic implementations.

The dependent variable in this study is the Error Rate (%), or Quantum Bit Error Rate (QBER), defined as the percentage of mismatched bits between Alice's and Bob's sifted keys.

3. RESULTS AND DISCUSSION

Following are the results obtained from simulating the BB84 quantum key distribution protocol under varying conditions. Three-bit lengths 10, 100, and 1000 bits were tested. All the lengths were each simulated over 1000 independent trials. The two major experimental conditions were: (1) absence of eavesdropping, and (2) presence of eavesdropping. Noise was kept constant at a low probability of 0.02 to simulate minimal background interference.

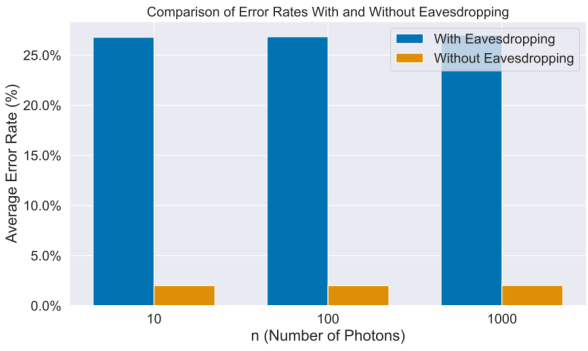

FIGURE 4: Average error rate (%) as a function of the number of photons (n) with and without the presence of an eavesdropper.

Figure 4 illustrates the average error rate in percentage in direct relation with number of bits with and without the presence of eavesdropper. It can be clearly seen that, the average rate of error within the presence of eavesdropper was consistently higher than without the presence of an

TABLE I: Independent variables.

Variable	Values	Description of Variable
Number of bits (n)	10, 100, 1000	To study how the size of the quantum key affects the error rate.
Eavesdropping	True, False	Presence and absence of eavesdropper.

eavesdropper. The average of error when an eavesdropper was present ranged from 26.78% to 27.00%, whereas the average rate of error without eavesdropper ranged from 2.00% to 2.02%.

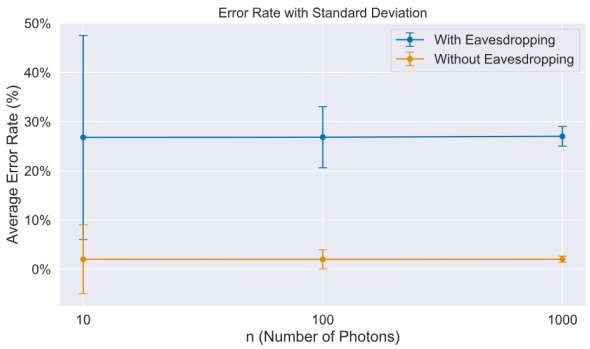

FIGURE 5: Average error rate (%) as a function of the number of photons (n) with and without the presence of an eavesdropper.

Figure 5 shows how increasing the number of photons can dramatically reduce the variability of error rate. A noticeable trend can be observed: as the number of photons increases, the variability in error rate decreases. In the absence of an eavesdropper, the standard deviation of the error rate declined from 7.01% at 10 photons to 0.62% at 1000 photons, signalling greater stability with larger photon counts. A similar but more rapid decline was noted under eavesdropping conditions, from 20.75% to 1.99%, further highlighting the influence of photon count on error consistency. Overall, the consistent pattern across the figures validates the robustness of QKD error detection and highlights the importance of optimizing photon transmission volume for secure quantum communication. The results indicate a clear impact of eavesdropping on the error rate in quantum key distribution (QKD). Across all the photon counts, eavesdropping consistently increased the error rate, validating theoretical predictions about QKD's sensitivity to third-party interference [5]. The effect of eavesdropping was more visible at lower photon counts. This suggests that BB84 is far more prone to disturbances when fewer photons are encoded, possibly due to the reduced redundancy in photon polarization patterns. As the number of photons increased, the system demonstrated greater resilience, likely due to statistical stabilization. Our findings support previously accomplished simulations and experimental studies emphasizing QKD's error rate as a reliable indicator of the presence of an eavesdropper [11]. Moreover, the increasing divergence in error rates between the two conditions (especially at low 'n') could inform future calibration thresholds in real-world QKD implementations.

3.1 Limitations

While this simulation effectively models the fundamental aspects of the BB84 protocol, certain limitations must be acknowledged. This model assumes a memoryless quantum channel with a fixed noise probability of $p = 0.02$, which simplifies the analysis but fails to account for the real world imperfections. Factors such as photon loss, detector dark counts, afterpulsing, basis-dependent efficiencies, and timing jitter are excluded from the present design.

Moreover, this study did not include finite-key effects, statistical uncertainties that arise when only a limited number of bits are exchanged. A more comprehensive analysis could employ Chernoff or Hoeffding bounds to infer confidence intervals in the estimated Quantum Bit Error Rate. Similarly, classical authentication overhead, including the use of Wegman-Carter Message Authentication Codes (MACs), has not been considered. These factors consume a portion of the generated key material and would affect the net secure key rate in a practical implementation.

In future work, extending this simulation to include these real-world scenarios and finite-key analyses would enhance its applicability and provide a more accurate assessment of BB84 performance under real-world conditions.

4. CONCLUSION

This study presented a computational analysis of the BB84 quantum key distribution protocol to examine how error rates vary with the number of transmitted bits under both eavesdropping and non-eavesdropping conditions. Our results confirm that eavesdropping significantly increases the error rate in the quantum key distribution (QKD), demonstrating BB84's inherent capability to detect intrusion through the principles of quantum measure-

ment disturbance. This effect becomes most evident at lower photon counts. By analysing error rates and their variability, the study demonstrated that increasing the photon count makes the system robust, further proving QKD's potential as a secure communication method.

The findings not only validate the theoretical foundations of QKD but also emphasize the importance of optimizing photon transmission to enhance eavesdropping detection. Although this study focuses on the BB84 protocol due to its foundational importance, this study could be expanded in the future by comparing BB84 with other QKD variants like six-state, SARG04, decoy-state BB84, and measurement-device-independent (MDI) QKD, as well as by adding more realistic channel imperfections, finite-key effects, and classical authentication overheads. Such extensions would offer deeper insight into protocol efficiency, scalability, and noise resilience in real-world quantum communication systems.

While the present model adopts a simplified, memoryless channel, its results provide a useful computational framework for understanding the practical implications of QKD and for introducing QKD concepts in educational setting.

ACKNOWLEDGMENTS

Authors thank Prof. Dr. Vijay Kumar Jha for his endless support, motivation, and guidance.

EDITOR'S NOTE

This manuscript was submitted to the Association of Nepali Physicists in America (ANPA) Conference 2025 for publication in the special issue of the Journal of Nepal Physical Society.

APPENDIX

You can find the full code of this paper by clicking on this github link. All figures were created by the authors using Python (Matplotlib) and vector design tools for illustrative purposes.

REFERENCES

1. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, **21**(2), 120–126.
2. Daemen, J., & Rijmen, V. (2002). *The design of Rijndael* (Vol. 2). New York: Springer-Verlag.
3. Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, **41**(2), 303–332.
4. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, **16**(5), 38–41.
5. Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, **560**, 7–11.
6. Mayers, D. (2001). Unconditional security in quantum cryptography. *Journal of the ACM*, **48**(3), 351–406.
7. Diamanti, E., Lo, H. K., Qi, B., & Yuan, Z. (2016). Practical challenges in quantum key distribution. *npj Quantum Information*, **2**(1), 1–12.
8. Liliana, Z. I. S. U. Efficiency of the quantum key distribution systems – A comparative study of BB84 protocol with its improved versions.
9. Busch, P., Heinonen, T., & Lahti, P. (2007). Heisenberg's uncertainty principle. *Physics Reports*, **452**(6), 155–176.
10. National Institute of Standards and Technology (NIST). (2021, March 1). Cryptography in the quantum age: Introduction to the new quantum revolution. `https://www.nist.gov/physics/introduction-newquantum-revolution/cryptography-quantum-age`
11. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, **81**(3), 1301–1350.