IJARST

International Journal of Advanced Research in Science and Technology

https://doi.org/10.62226/ijarst20262701

ISSN 2319 – 1783 (Print)

ISSN 2320 – 1126 (Online)

Detection and Analysis of Eavesdropping Attacks on Quantum Key Distribution BB84 Protocol

Godala Madhu

Assistant Professor, Department of CSE, MVSR Engineering College, India

madhu_cse@mvsrec.edu.in

ARTICLEINFO

Article history:

Received	01 June 2026
Accepted	12 June 2026
Available online	18 June 2026

Keywords:

Quantum Key Distribution, BB84 Protocol, Eavesdropping Detection, Quantum Cryptography, QBER, Intercept-Resend Attack, Quantum Security.

Indexed in:

and in major libraries

ABSTRACT

Quantum Key Distribution (QKD) provides an innovative approach for secure communication by utilizing the principles of quantum mechanics. Among various QKD protocols, the BB84 protocol remains the most widely studied and implemented due to its simplicity and theoretical security guarantees. However, practical implementations of BB84 are vulnerable to several eavesdropping attacks and channel imperfections. This paper presents a comprehensive study on the detection and analysis of eavesdropping attacks in the BB84 protocol. The work focuses on common attacks such as intercept-resend attack, photon-number splitting attack, Trojan horse attack, and phase-covariant cloning attack. The effect of these attacks on Quantum Bit Error Rate (QBER) is analyzed in detail. Simulation-based observations are discussed to demonstrate how QBER increases under malicious interference. The study further explores statistical methods for detecting eavesdropping and examines practical countermeasures including decoy states, privacy amplification, and error correction techniques. The paper concludes that BB84 remains robust against eavesdropping when proper detection and mitigation mechanisms are employed.

1. Introduction

Secure communication has become a major requirement in modern digital infrastructure due to the rapid increase in cyber threats and computational capabilities. Classical cryptographic systems mainly rely on mathematical complexity for security. However, the emergence of quantum computing poses a serious challenge to classical encryption algorithms such as RSA and ECC because quantum algorithms can solve factorization and discrete logarithm problems efficiently.

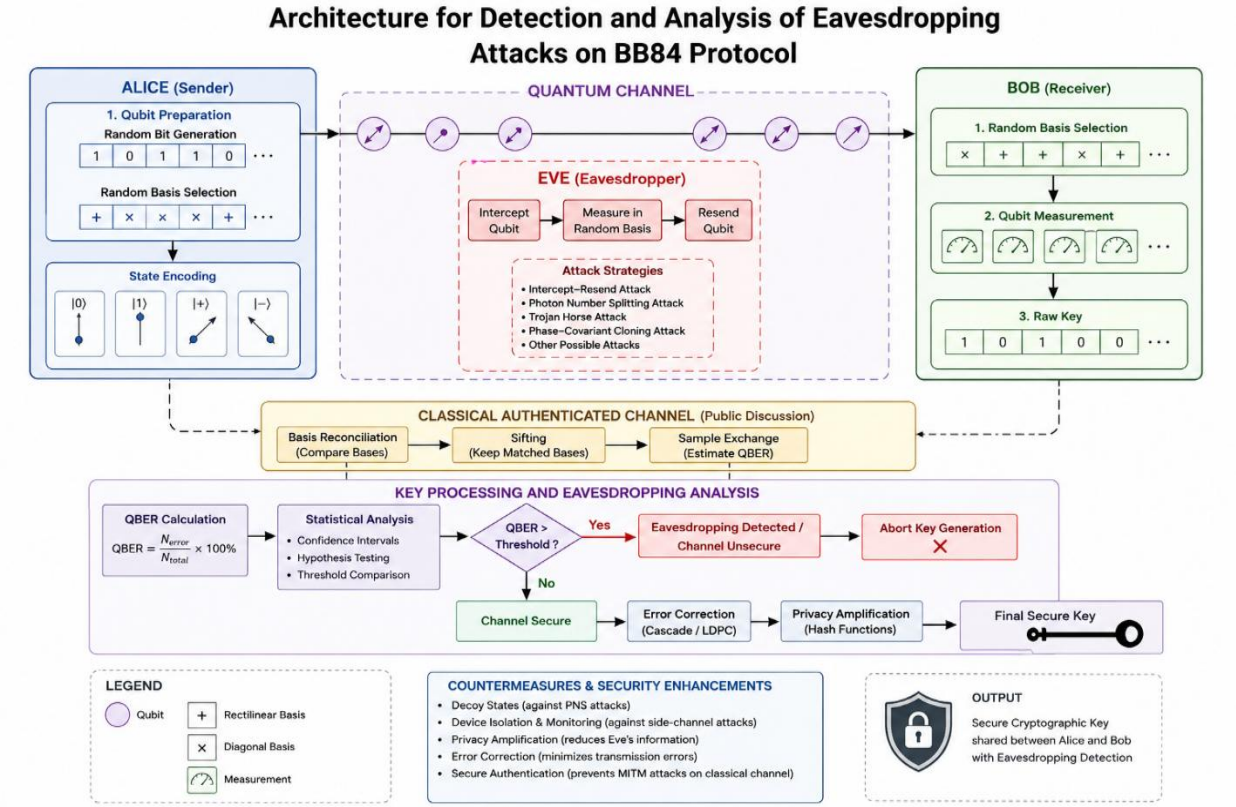
Quantum Key Distribution (QKD) offers a fundamentally different approach to secure communication. Instead of relying on computational assumptions, QKD uses the laws of quantum mechanics to establish secure cryptographic keys between communicating parties. The BB84 protocol, proposed by Charles Bennett and Gilles Brassard in 1984, was the first practical QKD protocol and remains one of the most important protocols in quantum cryptography.

The primary advantage of BB84 is its ability to detect the presence of an eavesdropper. According to the principles of quantum mechanics, measuring an unknown quantum state disturbs that state. Therefore, any attempt by an attacker to intercept quantum bits introduces detectable errors in the communication channel.

Despite its theoretical security, practical implementations of BB84 face several vulnerabilities due to imperfect devices, noisy channels, and side-channel attacks. This paper investigates different eavesdropping strategies and analyzes their impact on protocol security. Special emphasis is placed on Quantum Bit Error Rate (QBER) analysis and detection mechanisms.

2. Background of BB84 Protocol

The BB84 protocol involves two communicating parties traditionally called Alice and Bob. Alice encodes classical bits into quantum states using two conjugate bases:



1. Rectilinear Basis (+)
   - $|0\rangle$
   - $|1\rangle$
2. Diagonal Basis (×)
   - $|+\rangle$
   - $|-\rangle$

Alice randomly selects a bit value and basis for each qubit transmission. Bob independently selects random measurement bases. After transmission, Alice and Bob publicly compare the chosen bases through a classical authenticated channel and discard mismatched measurements. The remaining bits form the sifted key.

The security of BB84 depends on two important quantum principles:

1. Heisenberg Uncertainty Principle
2. No-Cloning Theorem

These principles ensure that unknown quantum states cannot be measured or copied without introducing disturbances.

3. Eavesdropping Attacks on BB84

3.1 Intercept-Resend Attack

In this attack, the eavesdropper Eve intercepts each transmitted qubit, measures it using a randomly selected basis, and resends a new qubit to Bob based on the measurement result.

If Eve selects the wrong basis, the qubit state collapses incorrectly, causing detectable errors. The attack introduces an average QBER of approximately 25%.

Working Procedure

1. Eve intercepts the qubit.
2. Eve randomly selects a measurement basis.
3. Eve measures the qubit.
4. Eve prepares a new qubit and sends it to Bob.
5. Bob measures the received qubit.

The increase in QBER reveals Eve's presence.

3.2 Photon Number Splitting (PNS) Attack

Practical BB84 systems often use weak coherent laser pulses instead of ideal single-photon sources. Some pulses may contain multiple photons.

In a PNS attack, Eve splits one photon from multi-photon pulses and stores it in

quantum memory while allowing the remaining photons to reach Bob. After basis reconciliation, Eve measures the stored photon using the correct basis without introducing significant errors.

This attack is difficult to detect because it does not substantially increase QBER.

Countermeasure

Decoy-state BB84 protocols are commonly used to defend against PNS attacks by introducing additional random intensity levels.

3.3 Trojan Horse Attack

In a Trojan horse attack, Eve sends bright light pulses into Alice's or Bob's device and analyzes the reflected signals to obtain information about internal configurations such as basis selection.

This is a side-channel attack that exploits implementation weaknesses rather than the protocol itself.

Countermeasures

- Optical isolators
- Wavelength filters
- Monitoring detectors
- Device shielding

3.4 Phase-Covariant Cloning Attack

In this attack, Eve uses approximate quantum cloning techniques to copy transmitted qubits. Although perfect cloning is impossible due to the no-cloning theorem, approximate cloning can provide partial information while minimizing detectable disturbances.

This attack attempts to balance information gain and introduced errors.

4. Quantum Bit Error Rate (QBER)

QBER is a critical parameter for detecting eavesdropping in BB84 systems. It is defined as the ratio of erroneous bits to the total number of sifted key bits.

QBER = (N_error / N_total) × 100%

Where:

- **N_error** represents the number of mismatched bits.
- **N_total** represents the total sifted key bits.

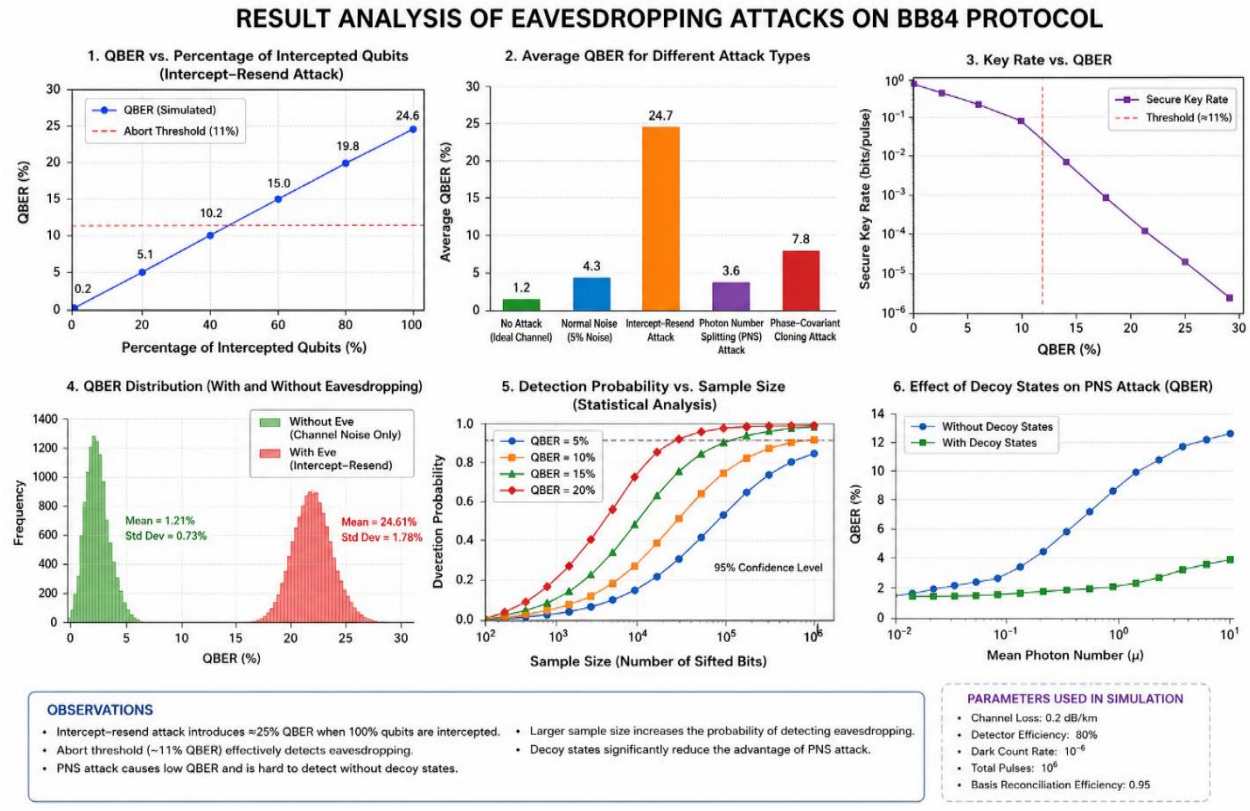
Under ideal conditions, QBER remains very low. During eavesdropping, QBER increases significantly.

Typical QBER observations:

Scenario	Approximate QBER
Ideal channel	0–2%
Noisy channel	2–10%
Intercept-resend attack	~25%

If QBER exceeds a threshold value, Alice and Bob abort the key generation process.

5. Detection Mechanisms



5.1 Statistical Error Analysis

Alice and Bob compare a subset of sifted bits publicly to estimate the QBER. Statistical confidence intervals can determine whether observed errors arise from noise or malicious interference.

Methods include:

- Wald interval
- Wilson interval
- Hoeffding inequality
- Clopper-Pearson interval

5.2 Privacy Amplification

After detecting partial information leakage, Alice and Bob apply privacy amplification techniques to reduce Eve's knowledge of the final key.

Hash functions are commonly used for this process.

5.3 Error Correction

Noise and eavesdropping both introduce errors. Error correction algorithms such as Cascade and LDPC codes help synchronize keys while minimizing information leakage.

6. Simulation and Analysis

Simulation studies demonstrate the relationship between eavesdropping intensity and QBER. As Eve intercepts more qubits, the QBER increases nearly linearly.

Simulation Observations

1. Without Eve:
    - QBER remains close to zero.
2. Partial Interception:
    - QBER increases gradually.
3. Full Intercept-Resend:
    - QBER approaches 25%.

The simulation confirms the theoretical security predictions of BB84.

7. Advantages and Limitations

Advantages

- Information-theoretic security
- Detection of eavesdropping
- Resistance to brute-force attacks
- Future-proof against quantum computers

Limitations

- Expensive hardware requirements
- Distance limitations
- Sensitivity to channel noise
- Practical device vulnerabilities

8. Future Research Directions

Future research in BB84 security includes:

1. Machine learning-based eavesdropping detection
2. Hybrid BB84-E91 protocols
3. Satellite-based QKD systems
4. Noise-resilient quantum channels
5. Device-independent QKD
6. AI-assisted QBER estimation

9. Conclusion

This paper presented a detailed analysis of eavesdropping attacks on the BB84 Quantum Key Distribution protocol. Various attack models including intercept-resend, photon-number splitting, Trojan horse, and phase-covariant cloning attacks were examined. The study highlighted the significance of Quantum Bit Error Rate in identifying malicious activities within quantum communication channels. Simulation analysis demonstrated that eavesdropping introduces measurable disturbances that can be detected statistically. Although practical implementations face several challenges, appropriate countermeasures such as decoy states, privacy amplification, and secure hardware design significantly strengthen BB84 security. The findings confirm that BB84 continues to be a foundational and reliable protocol for future quantum-secure communication systems.

References

1. C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984.
2. A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem," Physical Review Letters, vol. 67, no. 6, pp. 661–663, 1991.
3. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography," Reviews of Modern Physics, vol. 74, pp. 145–195, 2002.
4. V. Scarani et al., "The Security of Practical Quantum Key Distribution," Reviews of Modern Physics, vol. 81, pp. 1301–1350, 2009.
5. Jaydeep Rath, Prajwal Panth, and P. S. N. Bhaskar, "Quantum Bit Error Rate Analysis in BB84 Quantum Key Distribution: Measurement, Statistical Estimation, and Eavesdropping Detection," arXiv, 2026.
6. Brian Pigott et al., "Eavesdropping on the BB84 Protocol using Phase-Covariant Cloning: Experimental Results," arXiv, 2024.
7. María Lourdes Simón Codina, "Quantum Key Distribution with BB84: Breidbart-Based Eavesdropping and Channel Noise Effects," Universitat de Barcelona, 2025.
8. Ivan Sushchev et al., "Realistic Vulnerabilities of Decoy-State Quantum Key Distribution," Scientific Reports, 2025.

9. T. Decker, M. Gallezot, S. F. Kerstan, A. Paesano, and W. Wormsbecher, "Quantum Key Distribution as a Quantum Machine Learning Task," npj Quantum Information, vol. 11, no. 140, 2025.
10. G. Thakur, P. Chouksey, M. Chopra, and S. Kumar, "A Comprehensive Review on the Hybrid BB84-E91 QKD Protocol for Enhanced Security Efficiency and Practical Hardware Implementation in Quantum Cryptography," Discover Computing, vol. 28, no. 343, 2025.
11. A. M. Reforgiato et al., "Estimating Interception Density in the BB84 Protocol: A Study with a Noisy Quantum Simulator," Future Internet, vol. 16, no. 8, pp. 275, 2024.
12. D. Scalcon, E. Bazzani, G. Vallone, P. Villoresi, and M. Avesani, "Low-Error Encoder for Time-Bin and Decoy States for Quantum Key Distribution," npj Quantum Information, vol. 11, no. 22, 2025.
13. Y. Zhang et al., "Imperfect Preparation and Trojan Attack on the Phase Modulator in the Decoy-State BB84 Protocol," Optics Communications, vol. 593, pp. 132175, 2025.
14. L. A. Lizama-Perez and J. M. López-Romero, "Loop-Back Quantum Key Distribution for Secure and Scalable Multi-Node Quantum Networks," Symmetry, vol. 17, no. 4, pp. 521, 2025.
15. H. Termos, "Quantum Authentication Evolution: Novel Approaches for Securing Quantum Key Distribution," Entropy, vol. 26, no. 6, pp. 447, 2024.
16. X. Liu et al., "Enhanced QKD Protocol Based on Zero-Knowledge Proof and Post-Quantum Signature," Optics Communications, vol. 596, pp. 132431, 2025.
17. M. Manimozhi and R. K. Mugelan, "Post-Quantum AES Encryption Using ECC Points Derived from BB84 Sifted Keys," EPJ Quantum Technology, vol. 12, no. 109, 2025.
18. J. Rath, P. Panth, and P. S. N. Bhaskar, "Quantum Bit Error Rate Analysis in BB84 Quantum Key Distribution: Measurement, Statistical Estimation, and Eavesdropping Detection," arXiv preprint arXiv:2603.27278, 2026.
19. C. Dunne, "High Dimensional Quantum Eavesdropping: A Hypothetical Attack on BB84 and SSP," arXiv preprint arXiv:2412.08487, 2024.
20. S. K. Reddy and C. Mohan, "Comprehensive Analysis of BB84, A Quantum Key Distribution Protocol," arXiv preprint arXiv:2312.05609, 2023.
21. A. Pokharel, R. Dangol, and H. K. Neupane, "Quantum Key Distribution Using BB84 Protocol: A Computational Study of Error Rates," Journal of Nepal Physical Society, vol. 11, no. 1, pp. 75–80, 2025.
22. M. Young, M. Lucamarini, and S. Pirandola, "Autonomous Recognition of Erroneous Raw Key Bit Bias in Quantum Key Distribution," Scientific Reports, vol. 16, Article no. 598, 2026.