p-ISSN: 2252-3006
e-ISSN: 2685-2411

Performance Analysis of Quantum Key Distribution B92 Protocol Using Qiskit

Eko Prasetyo[a1], Cahya Damarjati[a2], Muhammad Nazih Mahmudi[a3], Eko Fajar Cahyadi[b4]
[a]Information Technology, Universitas Muhammadiyah Yogyakarta, Indonesia
[b]Telecommunication Engineering, Telkom University Purwokerto, Indonesia
e-mail: [1]eko.prasetyo@umy.ac.id, [2]cahya.damarjati@umy.ac.id,
[3]nazih.mahmudi12@gmail.com, [4]ekofajarcahyadi@telkomuniversity.ac.id

Abstrak

Distribusi Kunci Kuantum merupakan landasan komunikasi yang aman, yang memanfaatkan mekanika kuantum untuk mencapai keamanan yang kuat. Studi ini mengevaluasi kinerja protokol B92, yang disederhanakan menggunakan status non-ortogonal, melalui simulasi dengan Python3 dan pustaka Qiskit. Penelitian ini berfokus pada variabilitas panjang kunci dan kemampuan protokol untuk mendeteksi upaya penyadapan. Hasil penelitian menunjukkan panjang kunci rata-rata 14,3 bit per 100 qubit yang ditransmisikan, dengan variabilitas berkisar antara 3 hingga 29 bit. Akurasi deteksi meningkat secara signifikan dengan ukuran sampel, mencapai akurasi 95% dengan ukuran sampel 5 dan 100% dengan ukuran sampel 10. Temuan ini menyoroti trade-off antara panjang kunci dan keandalan deteksi, yang menekankan pentingnya pengoptimalan. Sementara simulasi mengonfirmasi kehandalan protokol, studi lebih lanjut dalam kondisi sebenarnya sangat penting. Studi ini menambah pemahaman sistem kriptografi kuantum dan meletakkan dasar untuk komunikasi kuantum yang aman.

Kata kunci: *Quantum Key Distribution, B92 Protocol, Eavesdropping Detection, Secure Communication*

Abstract

Quantum Key Distribution is a cornerstone of secure communication, utilizing quantum mechanics to achieve unparalleled security. This study evaluates the performance of the B92 protocol, a simplified scheme using non-orthogonal states, through simulation with Python3 and the Qiskit library. The research focuses on the variability of key lengths and the ability of the protocol to detect eavesdropping attempts. Results show an average key length of 14.3 bits per 100 transmitted qubits, with variability ranging from 3 to 29 bits. Detection accuracy improves significantly with sample size, achieving 95% accuracy with a sample size of 5 and 100% with a sample size of 10. These findings highlight the trade-off between key length and detection reliability, emphasizing the importance of optimization. While simulations confirm the protocol's robustness, further studies under real-world conditions are essential. This work advances the understanding of quantum cryptographic systems and lays the foundation for secure quantum communication.

Keywords: *Quantum Key Distribution, B92 Protocol, Eavesdropping Detection, Secure Communication*

1. Introduction

The exponential growth of digital communications has underscored the critical importance of cryptographic techniques to safeguard sensitive information against unauthorized access. Classical cryptography, such as RSA, Diffie-Hellman, and elliptic curve cryptography (ECC), has served as the backbone of secure communications for decades. However, the advent of quantum computing poses a significant threat to the security of these classical methods due to the computational power of quantum algorithms, such as Shor's algorithm, which can efficiently solve problems that are intractable for classical computers. Consequently, the field of quantum cryptography, which leverages the principles of quantum mechanics to ensure communication security, has emerged as a pivotal area of research and development [16]. Quantum Key Distribution (QKD), a cornerstone of quantum cryptography, exploits the quantum properties of particles to generate unconditionally secure cryptographic keys, with the no-cloning theorem serving as a fundamental guarantee against eavesdropping [2,10].

The BB84 protocol, introduced by Bennett and Brassard in 1984 [6], is the first and most extensively studied QKD protocol. It utilizes four quantum states across two measurement bases to establish secure communication. Despite its theoretical robustness, the practical implementation of BB84 is resource-intensive, requiring precise control over quantum states and high-fidelity equipment. To address these challenges, Bennett proposed the B92 protocol in 1992, which reduces complexity by utilizing only two non-orthogonal quantum states [5]. This streamlined approach has made the B92 protocol a compelling alternative for practical quantum communication systems, particularly in environments with limited quantum resources [7].

The increasing reliance on quantum-safe communication systems has spurred substantial research into optimizing QKD protocols, particularly regarding their resilience to eavesdropping and their efficiency in key generation. Key distribution in quantum cryptography is inherently probabilistic, relying on the interaction between quantum states and measurement bases to produce shared cryptographic keys. However, real-world implementations are subject to variability in key length, which can impact the overall security and performance of the protocol. Furthermore, the detection of eavesdropping, a critical feature of QKD, depends on the protocol's ability to identify inconsistencies caused by unauthorized measurements, such as those introduced by an eavesdropper (Eve). Thus, understanding and enhancing these aspects of QKD protocols, particularly B92, remains a focal point in quantum cryptography research [11].

In the face of these challenges, prior studies have explored various strategies to enhance the effectiveness of QKD protocols. One common approach is to simulate the performance of protocols under controlled conditions to identify and mitigate factors that affect their reliability. For example, Adu-Kyere et al. [2] demonstrated the use of simulation to analyze the BB84 protocol's performance and its susceptibility to eavesdropping, providing valuable insights into protocol optimization. Similarly, Iqbal and Krawec [11] explored extensions to the B92 protocol, incorporating high-dimensional quantum states to improve key generation rates and enhance security. These studies highlight the importance of computational simulation in advancing QKD technologies and underscore the potential for further exploration in this domain.

The B92 protocol has been particularly intriguing due to its simplicity and reduced resource requirements compared to other QKD protocols. Its reliance on two non-orthogonal states aligns well with the constraints of practical quantum systems, where the generation, transmission, and measurement of quantum states are prone to noise and loss. Despite its advantages, the protocol is not immune to challenges, such as variability in key length and susceptibility to advanced eavesdropping strategies. Previous studies have investigated the performance of the B92 protocol in idealized settings, identifying key parameters that influence its effectiveness, such as the choice of measurement bases and the impact of sample size on eavesdropping detection [4,7].

While these studies provide a solid foundation for understanding the B92 protocol, they leave several critical questions unanswered, particularly regarding its behavior under realistic conditions and its response to different eavesdropping scenarios. For instance, the relationship between sample size and detection accuracy remains an area of active investigation, with implications for both theoretical security and practical implementation. Additionally, the effect of quantum system imperfections, such as decoherence and measurement errors, on the protocol's performance warrants further study. Addressing these gaps is essential to developing robust and scalable QKD systems.

This study aims to address these challenges by conducting a performance analysis of the B92 protocol using Python3 and the Qiskit library. As an open-source quantum computing framework, Qiskit allows researchers to simulate and analyze its performance under various conditions. It also provides tools for constructing quantum circuits, executing them on simulators or real quantum hardware, and analyzing the results. For instance, the simulation of the B92 protocol can include error reconciliation techniques to address discrepancies arising from channel noise and detector imperfections [12].

By simulating the protocol under varying conditions, this research seeks to evaluate its key generation efficiency, analyze its resilience to eavesdropping, and explore the impact of parameters such as sample size on detection accuracy. The novelty of this study lies in its comprehensive simulation-based approach, which combines theoretical insights with practical considerations to provide a deeper understanding of the B92 protocol's capabilities and limitations. Furthermore, this work contributes to the broader effort of advancing quantum

p-ISSN: 2252-3006
e-ISSN: 2685-2411

cryptographic technologies, with potential implications for secure communication in the quantum era.

In summary, this research provides a critical examination of the B92 protocol, focusing on its performance in generating secure keys and detecting eavesdropping attempts. By addressing key gaps in the existing literature, this study not only enhances our understanding of the protocol but also lays the groundwork for future advancements in quantum cryptography. Through rigorous analysis and simulation, this work aims to contribute to the ongoing quest for secure and reliable communication systems in an increasingly quantum-driven world.

2. Proposed Method

This study focuses on evaluating the performance of the Quantum Key Distribution (QKD) B92 protocol through simulation using Python3 and the Qiskit library. The methodology is designed to provide a systematic approach for analyzing key length variability, the protocol's ability to detect eavesdropping, and the influence of key parameters such as sample size on detection accuracy. The following sections outline the procedural steps, computational setup, and analytical framework employed in this research.

2.1 Research Framework

The research follows a simulation-based approach to evaluate the B92 protocol under controlled conditions. By leveraging computational tools, the study aims to replicate the behavior of the protocol during key distribution and assess its performance in detecting eavesdropping attempts. The framework includes two primary phases:

1. Baseline Simulation of the B92 Protocol: This phase analyzes the protocol's ability to generate secure keys in the absence of eavesdropping.
2. Eavesdropping Simulation: This phase examines the protocol's resilience by introducing an eavesdropper (Eve) and evaluating its ability to detect such intrusions.

2.2 B92 Protocol Implementation

2.2.1 Quantum Key Distribution Process

The B92 protocol utilizes two non-orthogonal quantum states for key distribution. The simulation process involves the following steps:

1. Key Initialization by Alice: Alice generates a random sequence of classical bits.
2. Quantum State Encoding: Based on the bit sequence, Alice encodes the quantum states using two polarizations: vertical (0°) and diagonal (45°). This encoding ensures that the quantum states are non-orthogonal.
3. Transmission to Bob: The encoded quantum states are transmitted through a quantum channel.
4. Random Measurement by Bob: Bob randomly selects a measurement basis—either linear (0°/90°) or diagonal (45°/135°)—to measure the incoming qubits.
5. Key Reconciliation: Bob communicates the positions of qubits with null measurements to Alice over a public channel. Both parties discard these bits to form the shared key.

2.3 Simulation Parameters

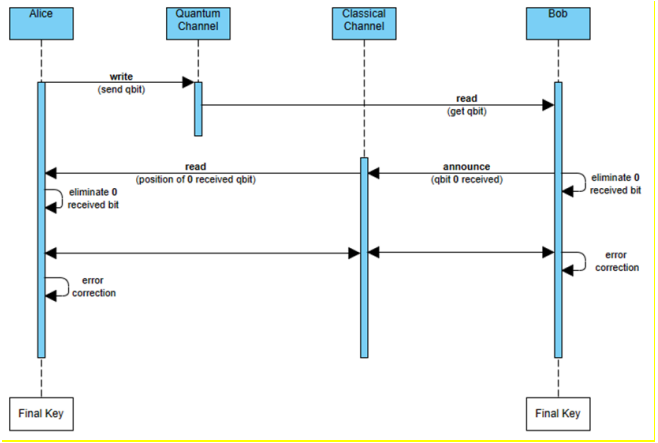

Figure 1. Sequence diagram of B92 protocol *[4]*

p-ISSN: 2252-3006
e-ISSN: 2685-2411

2.3.1 Baseline Configuration

Based on the sequence diagram shown in Figure 1, a program was developed to implement the B92 protocol using Python3 and the Qiskit library to perform quantum computing processes. The simulation for the baseline protocol is conducted with the following parameters:

- Number of Experiments: 100
- Number of Bits per Experiment: 100

These parameters are chosen to provide a statistically significant dataset for evaluating the protocol's key length distribution and variability.

2.3.2 Eavesdropping Simulation Configuration

For the eavesdropping scenario, an additional parameter, sample size, is introduced to assess the protocol's effectiveness in detecting Eve. Two sample sizes are tested:

- Sample Size: 5 bits
- Sample Size: 10 bits

This variation allows the study to compare detection accuracy across different sample sizes.

2.4 Simulation Design

2.4.1 Encoding Quantum States

Alice's classical bit sequence is encoded into quantum states using the encode_message function. For each bit, the following logic is applied:

- A '0' bit is encoded as a vertical polarization (0°).
- A '1' bit is encoded as a diagonal polarization (45°).

This encoding is implemented using Qiskit, where the Hadamard gate is applied to achieve the desired quantum state.

2.4.2 Measurement by Bob

Bob measures the received quantum states using the measure_message function. His choice of measurement basis—linear or diagonal—is determined randomly for each qubit. The measurement outcomes guide the construction of Bob's key.

2.4.3 Key Reconciliation

Key reconciliation involves two steps:

1. Bob identifies the positions of null measurement outcomes (qubits where no information was retrieved) and communicates them to Alice.
2. Both parties remove the corresponding bits from their respective keys to form a reconciled shared key.

2.5 Introduction of Eavesdropper (Eve)

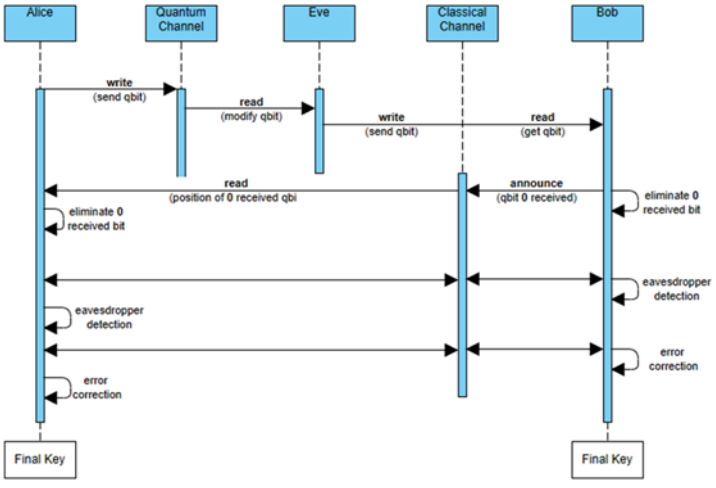

Figure 2. Eavesdropping scenario

To simulate an eavesdropping scenario, as depicted in Figure 2, Eve intercepts and measures the qubits sent by Alice before they reach Bob. Eve's measurements alter the state of the qubits, introducing inconsistencies detectable during the reconciliation phase. The steps are as follows:

1. Interception: Eve randomly selects a measurement basis for each intercepted qubit.
2. State Disturbance: Eve's measurement collapses the quantum state, potentially affecting Bob's subsequent measurement.
3. Detection: The inconsistencies caused by Eve's interference are identified during the key reconciliation process.

2.6 Data Analysis

2.6.1 Key Length Evaluation

The average key length and standard deviation are calculated from the reconciled keys across all experiments, are shown in (1) and (2). These metrics provide insights into the protocol's efficiency and variability.

- Mean Key Length:

$$Mean\ Key\ Length = \frac{\sum Key\ Lengths}{Number\ of\ Experiments} \quad (1)$$

- Standard Deviation:

$$\sigma = \sqrt{\frac{\sum L_i - \mu^2}{N}} \quad (2)$$

Where L_i represents individual key lengths, μ is the mean, and N is the total number of experiments.

2.6.2 Eavesdropping Detection Accuracy

Detection accuracy is measured as the percentage of experiments in which Eve's interference was successfully identified. The comparison of sample sizes (5 and 10) allows for assessing the impact of sample size on detection reliability.

2.7 Tools and Software

This research utilizes Python3 and the Qiskit library for quantum computing simulation. Qiskit provides a comprehensive platform for constructing quantum circuits, simulating quantum states, and analyzing outcomes. The simulations are executed on Qiskit Aer simulators, which offer high fidelity for quantum experiments.

2.8 Ethical Considerations

All simulations are conducted in a controlled computational environment, ensuring the integrity of the experiments and the reproducibility of results. The study adheres to academic standards for transparency and reproducibility, with all code and datasets made available for peer review.

2.9 Limitations

While the simulation provides valuable insights into the B92 protocol's performance, it is constrained by the idealized nature of computational models. Real-world factors such as noise, decoherence, and hardware imperfections are not fully accounted for. Future research should incorporate these factors to validate the findings in practical settings.

3. Literature Study

The development of secure communication systems has significantly advanced with the integration of quantum mechanics into cryptographic protocols. Quantum Key Distribution (QKD) is a prominent technology leveraging quantum properties such as superposition and entanglement to establish secure communication. This section discusses the theoretical

foundation of QKD, the specific characteristics of the B92 protocol, and prior advancements, highlighting the state of research and identifying areas for further exploration.

3.1 Quantum Key Distribution

QKD enables two distant parties, commonly referred to as Alice and Bob, to generate shared secret keys using quantum states transmitted through a quantum channel. Unlike classical cryptographic methods, QKD's security is grounded in the no-cloning theorem, which states that quantum information cannot be duplicated without disturbance. This property ensures that any eavesdropping attempt, typically by an adversary referred to as Eve, introduces detectable inconsistencies in the transmitted quantum states [8,10].

The BB84 protocol, proposed by Bennett and Brassard in 1984, was the first QKD protocol and remains the most extensively studied. It uses four quantum states across two measurement bases to encode and decode cryptographic keys. However, the practical implementation of BB84 requires precise control over quantum states, making it resource-intensive and challenging in noisy environments [2,14].

3.2 B92 Protocol

In response to the challenges posed by BB84, Bennett introduced the B92 protocol in 1992. It is notable for its simplicity and reliance on non-orthogonal states for key distribution [3]. This protocol reduces complexity by using only two non-orthogonal quantum states, simplifying the implementation and requiring fewer quantum resources. Alice encodes her classical bits into two quantum states, while Bob selects a random measurement basis to decode the received qubits. The probabilistic nature of quantum measurements enables the protocol to identify shared secret keys while ensuring that any eavesdropping attempt disturbs the system [5,7].

The B92 protocol's simplicity makes it particularly suitable for resource-constrained environments. It has been applied in various simulated and experimental settings to demonstrate its feasibility and robustness. However, the protocol's efficiency depends on parameters such as the choice of measurement bases, sample size for eavesdropping detection, and the alignment of quantum state properties between sender and receiver [4].

Moreover, practical implementations of the B92 protocol have been explored in various contexts, including free-space communication systems, which can overcome the limitations of fiber-based QKD [13,17]. These advancements highlight the protocol's versatility and potential for secure communication in diverse environments, including satellite-based systems [1]. The integration of Qiskit in these studies not only aids in theoretical analysis but also bridges the gap between theoretical constructs and practical applications, paving the way for future developments in quantum communication technologies.

3.3 Qiskit in Quantum Key Distribution Simulations

Qiskit, an open-source quantum computing framework developed by IBM, has become a valuable tool for simulating and implementing quantum cryptographic protocols. Written in Python, Qiskit enables researchers to model quantum circuits, execute simulations, and analyze results using high-performance backends such as Qiskit Aer. The framework bridges theoretical quantum mechanics and practical computational requirements, making it an essential component for studying QKD protocols like B92 [15].

Qiskit provides several features that make it particularly suitable for quantum cryptography research:

1. Quantum Circuit Modeling: Researchers can design quantum circuits using qubits and quantum gates, such as Hadamard gates for creating superposition states and measurement gates for decoding qubits.
2. Simulator Integration: Qiskit Aer simulators offer a controlled environment for testing quantum algorithms without requiring physical quantum hardware.
3. Programming Flexibility: As a Python-based library, Qiskit integrates seamlessly with scientific computing tools, enabling efficient data processing and visualization.

The integration of Qiskit into this study facilitated a detailed performance analysis of the B92 protocol, enabling a deeper understanding of its strengths and limitations. The framework's capabilities in simulating both ideal and adversarial scenarios provided insights into the protocol's robustness and its potential for practical applications.

p-ISSN: 2252-3006
e-ISSN: 2685-2411

4. Result and Discussion

This section discusses the results obtained from the simulations of the B92 Quantum Key Distribution (QKD) protocol. The findings are presented in two parts: the performance of the protocol in generating secure keys and its effectiveness in detecting eavesdropping attempts. The results are analyzed based on key metrics, including average key length, standard deviation, and eavesdropping detection accuracy

4.1 Simulation Results of the B92 Protocol

4.1.1 Key Length Analysis

The performance of the B92 protocol was evaluated through simulations involving 100 experiments, with each experiment simulating the transmission of 100 qubits. The results showed that the protocol generates an average key length of 14.3 bits per experiment. The key lengths ranged from a minimum of 3 bits to a maximum of 29 bits, indicating variability in key generation, as depicted in Figure 3.

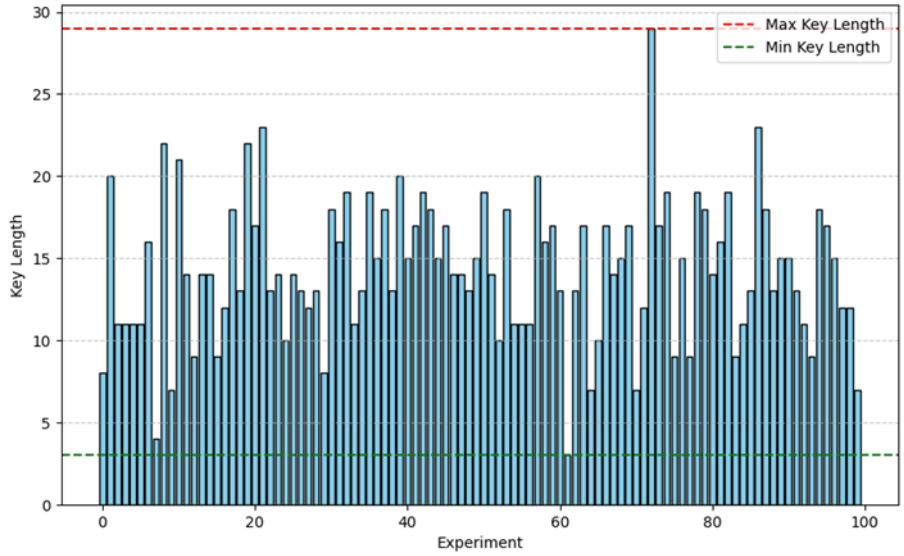

Figure 3. Key length generated in B92 protocol simulations

This variability reflects the probabilistic nature of the protocol. The interaction between Alice's transmitted qubits and Bob's randomly selected measurement bases significantly influences the number of valid key bits obtained. The maximum key length achieved in the simulation was 29 bits. This indicates that the simulated B92 protocol has the potential to produce significantly longer keys, which enhances security as longer keys are inherently more resistant to unauthorized decryption attempts.

Conversely, the minimum key length observed was 3 bits. This minimal length reflects instances where the system encountered challenges in generating longer keys. These challenges are likely due to a lower level of alignment between the qubits transmitted by Alice and the measurement bases randomly chosen by Bob, which directly impacts the measurement outcomes and, consequently, the effective key length.

The distribution of key lengths across the experiments was illustrated in Figure 4. The distribution appears to follow a Gaussian pattern, centered around the mean of 14.3 bits. The standard deviation of the key lengths was calculated as 4.3 (using (2)), indicating moderate variability in the protocol's performance. While most experiments resulted in key lengths close to the mean, occasional outliers (both higher and lower) highlight the influence of quantum measurement randomness and protocol dynamics.

p-ISSN: 2252-3006
e-ISSN: 2685-2411

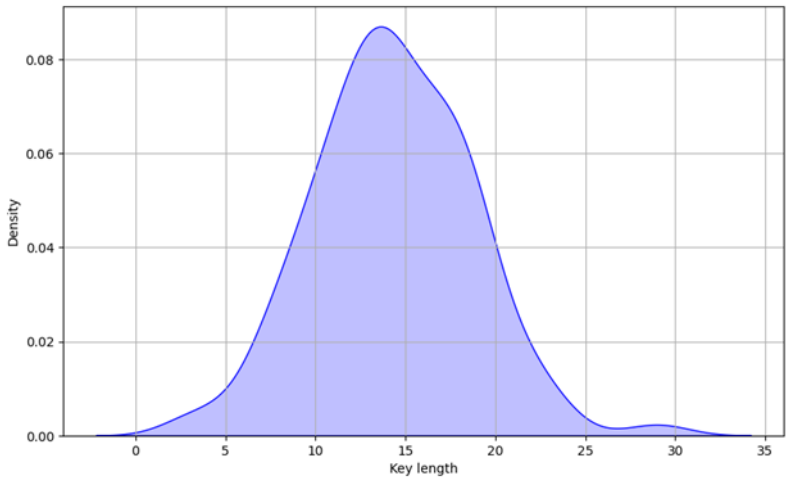

Figure 4. Key length distribution in B92 protocol simulations

4.1.2 Factors Influencing Key Length Variability

The variability in key lengths can be attributed to several factors:

- Measurement Basis Selection: Bob's random choice of measurement basis may not always align with Alice's transmitted states, resulting in null measurements that reduce the effective key length.
- Quantum State Properties: The inherent probabilistic nature of quantum states, governed by superposition and no-cloning theorem, introduces additional randomness in key generation.

While the average key length is sufficient for many cryptographic applications, the lower bound of 3 bits observed in some experiments suggests that the protocol may occasionally face challenges in generating a robust key. Addressing this limitation could involve optimizing the measurement basis selection process or incorporating redundancy to enhance reliability.

4.2 Impact of Eavesdropping on Key Distribution

4.2.1 Eavesdropping Simulation Results

In the presence of an eavesdropper (Eve), the protocol's performance was evaluated across 100 experiments for two sample sizes: 5 bits and 10 bits. The objective was to assess the protocol's ability to detect inconsistencies introduced by Eve's measurements.

With 5 bits sample Size 5 out of 100 experiments, Eve was successfully detected in 95 cases, resulting in a detection accuracy of 95%. The remaining 5 experiments failed to detect Eve's interference. The detection failure is caused because Eve luckily has guess the same qubits gate in the selected sample. Thus, Alice and Bob could not detected the Eve interference. With 10 bits Sample Size, detection accuracy improved to 100%, with all experiments successfully identifying Eve's presence. This result demonstrates the critical role of sample size in enhancing the protocol's security against eavesdropping. This study suggests that at least 10% of qubits need to be sacrificed from key candidates and become sample bits.

The detection accuracy results are summarized in Table 1, highlighting the correlation between sample size and detection effectiveness.

Table 1. The correlation between sample size and detection effectiveness

Sample Size	Detection Accuracy	Failure Rate
5	95%	5%
10	100%	0%

4.2.2 Mechanisms of Detection

Eavesdropping detection in the B92 protocol relies on the inconsistencies introduced by Eve's measurements. When Eve intercepts and measures qubits, the no-cloning theorem ensures that the original quantum state collapses, altering the qubits received by Bob. These changes

manifest as discrepancies during the reconciliation phase, where Alice and Bob compare a subset of their keys. A mismatch in this subset indicates the presence of an eavesdropper.

The improvement in detection accuracy with larger sample sizes aligns with theoretical expectations. A larger sample provides more opportunities to identify inconsistencies, reducing the likelihood of Eve remaining undetected. This finding underscores the importance of selecting an appropriate sample size based on the desired security level.

4.3 Discussion on Key Length Variability and Eavesdropping Detection

4.3.1 Balancing Key Length and Security

The dual objectives of key length maximization and robust eavesdropping detection present a trade-off in the protocol's design. While longer keys enhance cryptographic strength, the necessity of discarding bits to detect Eve's presence may reduce the overall key length. This trade-off is particularly evident in scenarios with a higher likelihood of eavesdropping, where a larger portion of the key must be allocated to detection. Strategies to address this trade-off include:

Adaptive Sampling: Dynamically adjusting the sample size based on the perceived threat level could optimize the balance between key length and security.

Error Correction: Incorporating error-correction codes may mitigate the impact of noise and eavesdropping, preserving key length without compromising security.

4.3.2 Practical Implications

The findings have significant implications for real-world applications of the B92 protocol. The ability to detect eavesdropping with high accuracy using moderate sample sizes demonstrates the protocol's suitability for secure communication in resource-constrained environments. However, the variability in key length suggests that additional measures, such as redundancy or pre-shared secrets, may be necessary to ensure consistent performance.

4.4 Comparative Analysis with Existing Literature

4.4.1 Key Length and Variability

The observed average key length of 14.3 bits is consistent with previous studies on the B92 protocol, which report similar ranges under comparable conditions [11]. The relatively narrow standard deviation aligns with findings by [4], indicating that the protocol performs reliably in controlled simulations.

4.4.2 Eavesdropping Detection

The improvement in detection accuracy with larger sample sizes corroborates theoretical models, which predict a direct relationship between sample size and the ability to detect inconsistencies caused by eavesdropping [9]. The results also align with experimental studies demonstrating the efficacy of statistical methods in enhancing QKD security.

5. Conclusion and Future Research

This study examines the Quantum Key Distribution (QKD) B92 protocol, focusing on its performance in generating secure keys and detecting eavesdropping attempts. The research uses Python3 and Qiskit to simulate the protocol, revealing its average key length of 14.3 bits from 100 transmitted qubits, with variability ranging from 3 to 29 bits. The protocol also demonstrates robust eavesdropping detection, achieving 95% accuracy with a sample size of 5 and 100% accuracy with a sample size of 10. However, the study highlights the trade-off between key length and security, suggesting the need for adaptive strategies to optimize protocol performance in different operational scenarios. The results are significant for the development of secure quantum communication systems, as the protocol's ability to detect eavesdropping with high accuracy using moderate sample sizes makes it a practical solution for resource-constrained environments. However, the variability in key length and idealized simulations suggest the need for further research to address real-world factors like noise, decoherence, and hardware imperfections. The study contributes to the existing body of knowledge by providing a detailed performance analysis of the B92 protocol, highlighting its strengths and areas for improvement.

The simulation of the B92 protocol offers valuable insights but does not fully account for real-world factors like noise and decoherence, hardware imperfections, and advanced eavesdropping techniques. The idealized simulation environment excludes these, which are

critical in practical implementations. Variations in quantum state preparation, transmission, and measurement fidelity may also impact the protocol's performance. Future research should focus on real-world noise simulation, hardware optimization, and advanced detection mechanisms to validate the protocol's robustness, investigate the impact of hardware imperfections on key generation and detection accuracy, and develop methods to counter complex eavesdropping techniques like quantum memory or entanglement-based attacks.

References

[1] A. Jimenez-Girela, P. Arteaga-Díaz, D. Merino-Pérez, P. Garcia-Parejo, S. Rodríguez-Bustabad, T. Belenguer-Dávila, V. Fernández-Mármol, A. Álvarez-Herrero. Inflight demonstrator of quantum key distribution between CubeSats of Q-ANSER program.2023, Vol. 12633. p. 126330C. doi:10.1117/12.2672097.

[2] Adu-Kyere A, Nigussie E, Isoaho J. Quantum Key Distribution: Modeling and Simulation through BB84 Protocol Using Python3. Sensors 2022;22:6284.

[3] Amer O, Krawec WO. Finite Key Analysis of the Extended B92 Protocol. 2020. doi:10.48550/arXiv.2001.05940.

[4] Anghel C, Istrate A, Vlase M. A Comparison of Several Implementations of B92 Quantum Key Distribution Protocol. 2022 26th International Conference on System Theory, Control and Computing (ICSTCC). Sinaia, Romania: IEEE, 2022. pp. 374–379. doi:10.1109/ICSTCC55426.2022.9931799.

[5] Bennett CH. Quantum cryptography using any two nonorthogonal states. Phys Rev Lett 1992;68:3121–3124.

[6] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science 2014;560:7–11.

[7] Bin-bin Su, Yuan-yuan Zhou, Xue-jun Zhou. B92 protocol analysis related to the same basis eavesdropping. 2016 IEEE International Conference on Cloud Computing and Big Data Analysis (ICCCBDA). Chengdu, China: IEEE, 2016. pp. 189–192. doi:10.1109/ICCCBDA.2016.7529556.

[8] Bruss D, Erdélyi G, Meyer T, Riege T, Rothe J. Quantum cryptography: A survey. ACM Comput Surv 2007;39:6.

[9] Chatterjee R, Joarder K, Chatterjee S, Sanders BC, Sinha U. qkdSim, a Simulation Toolkit for Quantum Key Distribution Including Imperfections: Performance Analysis and Demonstration of the B92 Protocol Using Heralded Photons. Phys Rev Applied 2020;14:024036.

[10] Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Rev Mod Phys 2002;74:145–195.

[11] Iqbal H, Krawec WO. Analysis of a High-Dimensional Extended B92 Protocol. Quantum Inf Process 2021;20:344.

[12] Mehic M, Niemiec M, Siljak H, Voznak M. Error Reconciliation in Quantum Key Distribution Protocols. In: Ulidowski I, Lanese I, Schultz UP, Ferreira C, editors. Reversible Computation: Extending Horizons of Computing: Selected Results of the COST Action IC1405. Cham: Springer International Publishing, 2020. pp. 222–236. doi:10.1007/978-3-030-47361-7_11.

[13] Rabinovich WS, Mahon R, Ferraro MS, Goetz PG, Bashkansky M, Freeman RE, Reintjes J, Murphy JL. Free space quantum key distribution using modulating retro-reflectors. Opt Express 2018;26:11331.

[14] Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. Rev Mod Phys 2009;81:1301–1350.

[15] Singh PN, Aarthi S. Quantum Circuits – An Application in Qiskit-Python. 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV). Tirunelveli, India: IEEE, 2021. pp. 661–667. doi:10.1109/ICICV50876.2021.9388498.

[16] Zhou T, Shen J, Li X, Wang C, Shen J. Quantum Cryptography for the Future Internet and the Security Analysis. Security and Communication Networks 2018;2018:1–7.

[17] Zhu M, Hu M, Guo B. Free-Space QKD with Modulating Retroreflectors Based on the B92 Protocol. Entropy 2022;24:204.