# Assessing the Security Trade-offs of BB84 vs. B92 in Quantum Key Distribution: A Monte Carlo Analysis

Rose Zhao[1]

[1]QubitxQubit EQCI

August 5, 2025

**Abstract**

This project compares the BB84 and B92 quantum key distribution protocols through theoretical analysis and Monte Carlo simulated eavesdropping scenarios. By quantifying their relative robustness using computational methods, we demonstrate the practical security implications of protocol choice in quantum communication systems. Our analysis examines three key performance areas: ideal protocol operation, noise tolerance under various quantum channel conditions, and resistance to eavesdropping attacks including intercept-resend and optimal Breidbart basis strategies. While BB84 maintains its theoretical advantage with approximately 50% key retention compared to B92's 25%, our findings reveal surprisingly similar eavesdropping detection capabilities between the protocols, with both achieving 100% detection rates under meaningful attack scenarios. The study employs the Cirq quantum computing framework with statistical validation through 15-20 independent simulation runs per scenario. Our results clarify the practical implications of protocol selection, showing that while BB84 provides superior efficiency and maintains security margins below the 11% QBER threshold in realistic noise conditions, B92 offers viable trade-offs in resource-constrained environments with its simplified implementation requirements and comparable security detection capabilities.

**Keywords:** quantum key distribution, BB84 protocol, B92 protocol, Monte Carlo simulation, quantum cryptography, eavesdropping detection, QBER analysis

# 1 Research Question

How does the BB84 quantum key distribution protocol outperform the B92 protocol in terms of error tolerance and resistance to eavesdropping, and under what practical conditions might B92 offer viable trade-offs?

# 2 Introduction

As quantum communication technology transitions from theoretical frameworks to practical implementation, the selection of appropriate quantum key distribution (QKD) protocols has become increasingly critical for establishing secure communication channels. The fundamental promise of quantum cryptography lies in its ability to provide information-theoretic security, guaranteed by the laws of quantum mechanics rather than the assumptions of computational complexity that underpin classical cryptographic systems.

The BB84 protocol, introduced by Bennett and Brassard in 1984, has emerged as the gold standard for quantum key distribution. BB84 leverages two mutually unbiased bases to encode quantum information across four quantum states, providing robust eavesdropping detection capabilities and maintaining high security margins even under challenging operational conditions. The protocol's strength derives from its fundamental design: any unauthorized interception attempt will inevitably introduce detectable disturbances in the quantum channel due to the complementary nature of the measurement bases.

In contrast, the B92 protocol, developed by Charles Bennett in 1992, represents a more resource-efficient approach using only two non-orthogonal photon polarization states. This simplification offers substantial advantages in implementation complexity and hardware requirements, translating to reduced transmitter costs, simplified optical components, and easier engineering implementations. These benefits make B92 particularly attractive for resource-constrained environments or large-scale deployments where cost considerations are paramount.

However, B92's apparent simplicity comes with important security trade-offs requiring careful analysis. The reduced state space and measurement complexity may compromise the protocol's robustness against sophisticated eavesdropping attacks and its tolerance to quantum channel noise. While theoretical analysis suggests that BB84's mutually unbiased bases provide approximately twice the security margin of B92, the practical implications of this theoretical advantage remain to be thoroughly investigated through computational analysis.

Real-world quantum communication must contend with various forms of decoherence, including amplitude damping from energy loss, phase damping from environmental interactions, depolarizing noise from general quantum decoherence, and thermal noise from finite-temperature environments. Understanding how BB84 and B92 respond to these realistic noise conditions is essential for making informed deployment decisions. Furthermore, the threat landscape includes sophisticated attack strategies beyond simple intercept-resend scenarios, such as optimal Breidbart basis strategies designed to maximize information extraction while minimizing detection probability.

This research addresses these critical questions through comprehensive Monte Carlo simulations that model realistic quantum channel conditions and eavesdropping scenarios. By simulating both protocols using the Cirq quantum computing framework and conducting statistically significant analysis across multiple operational scenarios, we provide quantitative evidence for the practical security trade-offs between BB84 and B92.

Our investigation encompasses three primary areas: establishing baseline performance characteristics under ideal quantum channel conditions to validate our implementation against theoretical predictions; examining noise tolerance across six different decoherence mechanisms representing realistic fiber-optic and free-space quantum channels; and evaluating eavesdropping

resistance against various attack strategies including intercept-resend attacks and optimal Breidbart basis approaches.

As quantum key distribution moves toward commercial deployment, system designers and security architects require evidence-based guidance for protocol selection. While BB84's theoretical superiority is well-established, understanding the conditions under which B92 might provide acceptable security with reduced implementation complexity could significantly impact the economics and scalability of quantum communication networks. Through this comprehensive analysis, we seek to identify the specific operational regimes where each protocol excels and to clarify the practical conditions under which B92 might represent a viable alternative to BB84, contributing to the growing body of knowledge needed to guide practical deployment of quantum key distribution systems in real-world environments.

# 3 Related Work

The comparative analysis of quantum key distribution protocols has been an active area of research, with numerous studies examining the trade-offs between security, efficiency, and implementation complexity across different QKD schemes. This section reviews the relevant literature that informs our investigation of BB84 and B92 protocol comparison.

## 3.1 Foundational Protocol Development

The foundational work in quantum key distribution began with Bennett and Brassard's seminal 1984 paper introducing the BB84 protocol, which established the use of four quantum states across two mutually unbiased bases for secure key distribution [1]. This was followed by Bennett's 1992 development of the B92 protocol, which simplified the approach by using only two non-orthogonal quantum states, offering reduced implementation complexity at the potential cost of security robustness [2].

## 3.2 Comparative Studies of BB84 and B92

Several comprehensive comparative studies have examined the relative performance characteristics of BB84 and B92 protocols across different operational conditions and security scenarios.

Zheng's analysis of BB84 and B92 in hybrid quantum-classical networks demonstrated that BB84 generally achieves approximately 50% key retention efficiency compared to B92's 25%, confirming the theoretical expectations about protocol efficiency differences [3]. The study also highlighted BB84's superior fault tolerance mechanisms during key reconciliation processes and examined cost considerations for network deployment, showing that B92 may be more suitable for medium-sized networks due to its lower cost and ease of maintenance.

Begimbayeva and Zhaxalykov conducted an extensive investigation of three major QKD protocols (BB84, B92, and E91) using IBM Quantum Experience platforms [4]. Their research provided empirical validation of theoretical predictions, showing that BB84 maintains strong security margins while B92 offers implementation simplicity through its reduced state space.

## 3.3 Security Analysis and Implementation Considerations

A significant body of work has examined protocol performance under various channel conditions and attack scenarios. Hwang, Choi, and Gong analyzed BB84 and B92 performance in the presence of transmission losses, demonstrating that both protocols maintain security under realistic loss conditions, though with different efficiency characteristics [5]. Choi and Hwang extended this analysis by examining decoy-state implementations, showing that improvements are more pronounced for BB84 due to its additional degrees of freedom in state preparation [6].

Bhowmick, Kundu, and Karmakar specifically examined protocol performance under individual eavesdropping attacks, providing quantitative assessments of how different attack strategies affect BB84 and B92 differently [7]. Their work demonstrated that while both protocols detect eavesdropping attempts, they exhibit different QBER patterns and information leakage characteristics under attack.

Research into practical QKD deployment has highlighted important considerations for protocol selection in real-world environments. Rejeb and el Allati examined BB84 and B92 specifically for satellite communication networks, identifying scenarios where B92's simplicity provides deployment advantages despite lower efficiency [8]. Thakur and Rai's investigation of protocol performance under imperfect laser sources highlighted that B92's reduced complexity can provide stability advantages in scenarios with significant hardware imperfections [9].

### 3.4 Research Gaps and Contributions

The literature reveals an important gap in comprehensive Monte Carlo analysis comparing these protocols under realistic noise conditions while simultaneously considering implementation costs. While individual studies have examined specific aspects such as security under particular attacks or performance in specific channel conditions, a unified analysis examining the complete trade-off space between security, efficiency, and implementation complexity remains limited.

Our research builds upon this foundation by providing a comprehensive Monte Carlo analysis that simultaneously considers security performance, noise tolerance, and implementation complexity for BB84 and B92 protocols, filling important gaps in the current literature while providing practical guidance for quantum key distribution system design.

## 4 Methods

This research employs comprehensive Monte Carlo simulations to evaluate the security trade-offs between BB84 and B92 quantum key distribution protocols. Our methodology encompasses three primary analysis domains: ideal protocol operation, noise tolerance under realistic quantum channel conditions, and eavesdropping resistance against various attack strategies. All simulations were implemented using the Cirq quantum computing framework with robust statistical validation procedures.

### 4.1 Simulation Framework and Implementation

#### 4.1.1 Cirq Quantum Computing Framework

All protocol implementations utilized Google's Cirq quantum computing framework (version 1.5.0-1.6.0), which provides comprehensive support for quantum circuit construction, noise modeling, and quantum state simulation. Cirq's simulator environment enables precise control over quantum operations while maintaining computational efficiency for large-scale Monte Carlo analysis.

The BB84 protocol implementation leverages four quantum states across two mutually unbiased bases: computational basis states $|0\rangle$ and $|1\rangle$, and diagonal basis states $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Alice's encoding process randomly selects bits and bases, applying appropriate quantum gates (identity for computational basis, Hadamard for diagonal basis) followed by bit flips when necessary. Bob's measurement protocol implements basis-dependent operations, applying Hadamard gates for diagonal basis measurements before computational basis measurements. Figure 1 describes a sample circuit in which Alice chooses to send bit 1 in the diagonal basis, after which Bob chooses to measure the bit in the diagonal basis.

The B92 protocol implementation utilizes only two non-orthogonal quantum states: $|0\rangle$ for bit 0 and $|+\rangle$ for bit 1. Bob's measurement strategy randomly selects between computational (Z)

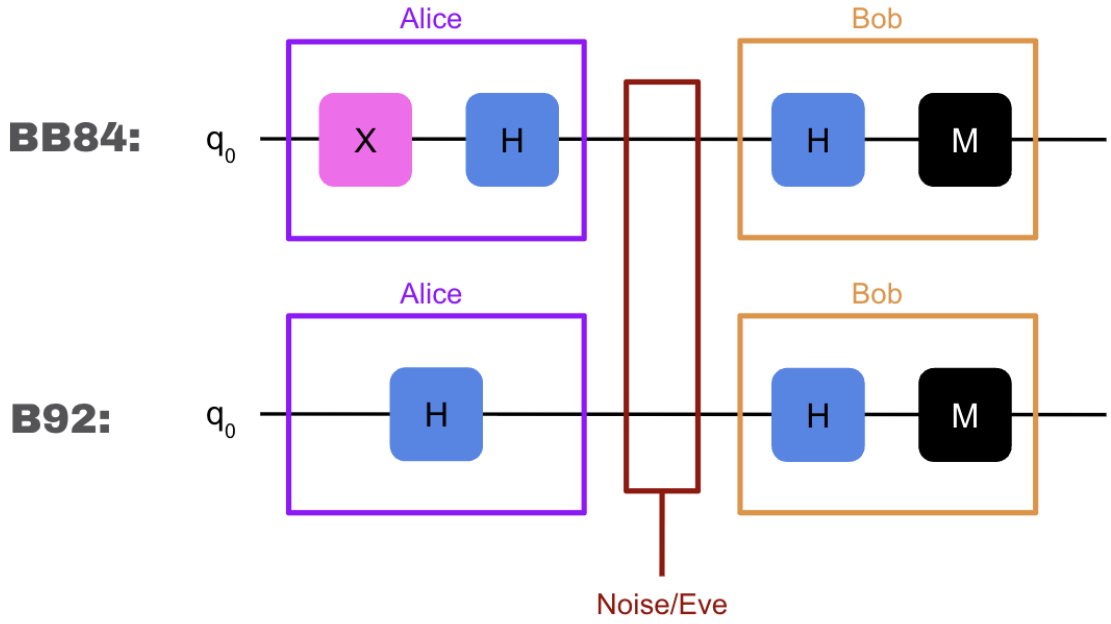


Figure 1: Sample Circuits

and diagonal (X) bases, with successful key material identified only when measurements yield definitive exclusion of one of Alice's possible states. Specifically, Bob retains measurements when he observes $|1\rangle$ in the computational basis (indicating Alice sent $|+\rangle$) or $|-\rangle$ in the diagonal basis (indicating Alice sent $|0\rangle$). Below is a sample circuit where Alice chooses to send bit 0 and Bob chooses to measure in the diagonal basis:

#### 4.1.2 Statistical Validation Methodology

Our statistical approach ensures robust and reproducible results through systematic Monte Carlo sampling. Each experimental scenario undergoes 15-20 independent simulation runs, with each run transmitting 200 qubits to provide sufficient statistical power for detecting meaningful protocol differences. This sample size balances computational efficiency with statistical significance, enabling detection of performance variations while maintaining reasonable execution times.

Random seed control ensures reproducibility across all simulations. We use random.seed(42) and numpy.random.seed(42) for consistent pseudorandom number generation, while using independent random sequences for each Monte Carlo run to capture natural variability in quantum communication systems.

Statistical metrics include mean values with standard deviations for all key performance indicators: key retention rates, quantum bit error rates (QBER), sifted key lengths, and eavesdropping detection probabilities. Confidence intervals are calculated using sample standard deviations to quantify measurement uncertainty and protocol variability.

### 4.2 Noise Modeling and Channel Simulation

#### 4.2.1 Quantum Decoherence Models

Real-world quantum channels experience multiple forms of decoherence that affect protocol performance differently. Our noise modeling incorporates six distinct decoherence mechanisms representing the primary sources of quantum information degradation in practical QKD systems:

**Depolarizing Noise** models general quantum decoherence through random application of Pauli operators (X, Y, Z) with probability $p_{depol}$. This represents the dominant decoherence mechanism in many quantum systems, causing qubits to lose their quantum information and become maximally mixed states.

**Amplitude Damping** simulates energy loss through T1 decay processes with probability $p_{amp}$. This models photon loss in optical fibers and spontaneous emission in quantum systems, causing $|1\rangle$ states to decay toward $|0\rangle$ states.

**Phase Damping** represents dephasing through T2 decay processes with probability $p_{phase}$. This models environmental interactions that destroy quantum phase relationships without affecting population distributions, particularly relevant for photonic quantum communication.

**Bit Flip Noise** applies X-gate operations with probability $p_{bit}$, simulating classical bit errors that can occur during quantum state preparation, transmission, or measurement processes.

**Phase Flip Noise** applies Z-gate operations with probability $p_{phase\_flip}$, modeling phase errors that affect relative phases between quantum states without changing population probabilities.

**Thermal Noise** simulates finite-temperature environmental effects with probability $p_{thermal}$, representing the influence of thermal photons and temperature-dependent decoherence processes.

#### 4.2.2 Realistic Channel Scenarios

We defined six comprehensive noise scenarios spanning the range from ideal laboratory conditions to challenging real-world deployment environments:

**Ideal Scenario** ($p_{total} = 0.0$) serves as the baseline for validating theoretical protocol predictions without any decoherence effects.

**Low Noise Scenario** ($p_{total} = 0.015$) combines depolarizing noise ($p_{depol} = 0.01$) with phase damping ($p_{phase} = 0.005$), representing high-quality laboratory quantum channels with minimal environmental interference.

**Medium Noise Scenario** ($p_{total} = 0.11$) incorporates multiple decoherence mechanisms: depolarizing noise ($p_{depol} = 0.05$), amplitude damping ($p_{amp} = 0.02$), phase damping ($p_{phase} = 0.03$), and bit flip errors ($p_{bit} = 0.01$), simulating moderately degraded quantum channels.

**High Noise Scenario** ($p_{total} = 0.28$) represents severely degraded channels with all noise mechanisms active: depolarizing ($p_{depol} = 0.1$), amplitude damping ($p_{amp} = 0.05$), phase damping ($p_{phase} = 0.08$), bit flip ($p_{bit} = 0.03$), and phase flip ($p_{phase\_flip} = 0.02$) errors.

**Realistic Fiber Scenario** ($p_{total} = 0.043$) models typical fiber-optic quantum channels with depolarizing noise ($p_{depol} = 0.02$), phase damping ($p_{phase} = 0.015$), and amplitude damping ($p_{amp} = 0.008$) representing fiber attenuation and dispersion effects.

**Realistic Free-Space Scenario** ($p_{total} = 0.07$) simulates atmospheric quantum channels with amplitude damping ($p_{amp} = 0.04$), phase damping ($p_{phase} = 0.02$), and thermal noise ($p_{thermal} = 0.01$) representing atmospheric turbulence and thermal effects.

### 4.3 Eavesdropping Attack Simulation

#### 4.3.1 Attack Strategy Implementation

Our eavesdropping analysis encompasses multiple attack strategies ranging from simple intercept resend approaches to sophisticated optimal information extraction techniques:

**Intercept-Resend Attacks** simulate the fundamental eavesdropping strategy where Eve intercepts Alice's qubits, measures them in randomly chosen bases, and retransmits approximations to Bob. We implement variable interception probabilities (0%, 50%, 100%) and different basis selection strategies including random basis choice, fixed computational basis, and fixed diagonal basis measurements.

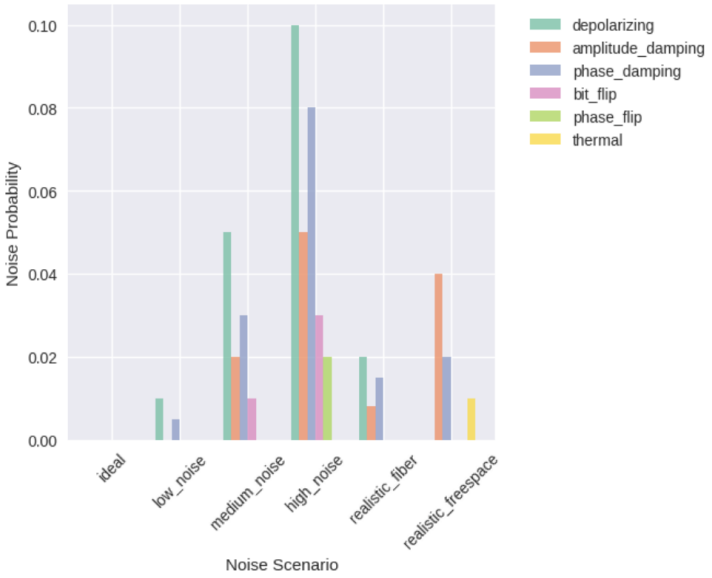


Figure 2: Noise Component Breakdown

**Breidbart Basis Attacks** implement optimal eavesdropping strategies designed to maximize information extraction while minimizing detection probability. Eve measures intercepted qubits in bases rotated by the optimal Breidbart angle ($\theta = \pi/8$) to achieve the theoretical limit of information gain versus detection trade-off.

**Sophisticated Attack Scenarios** combine partial interception (80% probability) with optimized basis selection to model realistic advanced eavesdropping attempts that balance information extraction with stealth requirements.

### 4.3.2 Security Analysis Metrics

**Quantum Bit Error Rate (QBER) Calculation** serves as the primary security indicator, computed as the fraction of mismatched bits in the sifted key after basis reconciliation:

$$\text{QBER} = \frac{\text{Number of bit mismatches}}{\text{Total sifted key length}}$$

Security thresholds follow established QKD security analysis: BB84 maintains security for QBER below 11%, while B92 uses a 14.6% threshold reflecting its different error tolerance characteristics.

**Eavesdropping Detection Analysis** employs statistical hypothesis testing to determine whether observed QBER values indicate eavesdropping presence. We calculate detection confidence using chi-square tests comparing observed error rates against expected distributions under various attack scenarios.

**Key Retention Rate Analysis** measures protocol efficiency as the fraction of transmitted qubits that contribute to the final shared key:

$$\text{Key Retention Rate} = \frac{\text{Sifted key length}}{\text{Total transmitted qubits}}$$

This metric captures the fundamental efficiency differences between protocols, with BB84 theoretically achieving 50% retention through basis matching and B92 achieving approximately 25% through its selective measurement disclosure strategy.

#### 4.3.3 Attack Detection Methodology

Statistical detection employs confidence interval analysis where detection occurs when observed QBER values fall outside expected ranges for legitimate quantum channel noise. We implement both conservative (95% confidence) and aggressive (99% confidence) detection thresholds to evaluate protocol sensitivity under different security requirements.

Information leakage analysis quantifies the amount of key material potentially compromised during eavesdropping attempts, providing insights into the practical security implications of different attack strategies and protocol responses.

## 5 Results

Our Monte Carlo simulation-based analysis of the BB84 and B92 quantum key distribution protocols has yielded comprehensive data across three key performance areas: ideal protocol operation, noise tolerance under various quantum channel conditions, and eavesdropping resistance. The simulations employed the Cirq quantum computing framework with 15-20 independent runs per scenario, each transmitting 200 qubits to ensure statistical significance and robust confidence intervals for our measurements.

### 5.1 Ideal Case Performance

Under perfect quantum channel conditions without noise or eavesdropping, both protocols demonstrated their theoretical performance limits with remarkable consistency, providing validation for our implementation approach.

BB84 achieved a mean key retention rate of $0.508 \pm 0.036$ (approximately 50%), confirming the expected basis reconciliation efficiency where Alice and Bob retain bits only when their randomly chosen measurement bases match. The protocol exhibited excellent consistency across runs with a standard deviation of 0.036, indicating stable implementation behavior. The mean sifted key length was $101.7 \pm 7.1$ bits from the initial 200 raw bits transmitted.

In contrast, B92 demonstrated its characteristic lower efficiency with a mean key retention rate of $0.264 \pm 0.033$ (approximately 25%). This reduced efficiency stems from B92's inherent sifting mechanism, where Bob only announces measurements yielding result '1', effectively discarding roughly half of the potential key material compared to BB84's symmetric basis matching approach. The protocol achieved a mean sifted key length of $49.3 \pm 5.0$ bits, representing the expected measurement success rate of approximately 25% that characterizes B92's two-state encoding scheme.

Both protocols maintained perfect accuracy with 0.000 QBER across all ideal case runs, as expected in the absence of quantum channel noise or eavesdropping attempts. The low standard deviations (BB84: 0.036, B92: 0.033) demonstrate the stability and reliability of our simulation implementations.

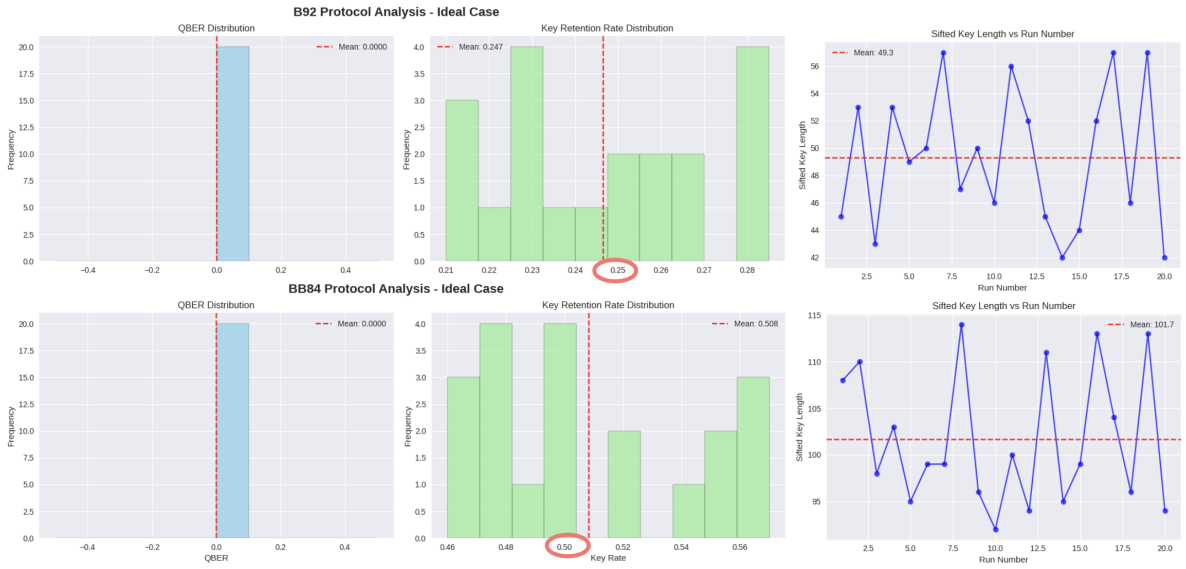


Figure 3: Ideal case performance comparison showing key retention rate distributions, QBER values, and sifted key length rates for both protocols across 20 simulation runs.

## 5.2 Noise Tolerance Analysis

We simulated realistic quantum channel conditions through six distinct noise scenarios incorporating multiple decoherence mechanisms that represent the primary sources of quantum state degradation in practical QKD deployments. The noise models included:

- **Bit Flip:** X Pauli error with probability $p_{\text{bit}}$
- **Phase Flip:** Z Pauli error with probability $p_{\text{phase\_flip}}$
- **Amplitude Damping:** Energy loss (T1 decay) with probability $p_{\text{amp}}$
- **Depolarizing Noise:** General decoherence with probability $p_{\text{depol}}$
- **Phase Damping:** Dephasing (T2 decay) with probability $p_{\text{phase}}$
- **Thermal Noise:** Environmental heating with probability $p_{\text{thermal}}$

Six noise scenarios were evaluated, ranging from ideal conditions to high-noise environments designed to represent realistic fiber-optic and free-space quantum channels:

**BB84 Noise Performance:** The protocol maintained security (QBER below the theoretical 11% threshold) across most realistic noise scenarios. In the low noise scenario (total noise strength 0.035), BB84 achieved a QBER of 0.011 $\pm$ 0.008 with a key retention rate of 0.495 $\pm$ 0.022. For simulated realistic fiber optic conditions (QBER: 0.016 $\pm$ 0.012), the protocol demonstrated robust performance well within security margins. Even under realistic free-space conditions (QBER: 0.026 $\pm$ 0.018), BB84 maintained acceptable security levels.

The protocol reached security breach conditions only under artificially high noise scenarios with total noise strength of 0.280, resulting in a QBER of 0.117 $\pm$ 0.035, marginally exceeding the 11% security threshold. This demonstrates BB84's excellent noise tolerance under realistic operational conditions.

**B92 Noise Performance:** B92 exhibited different noise tolerance patterns while maintaining security below its higher theoretical QBER threshold of approximately 14.6% across similar scenarios. The protocol showed more variable QBER responses to different noise types,

suggesting sensitivity to specific decoherence mechanisms inherent in its two-state encoding scheme.

Under low noise conditions, B92 achieved a QBER of 0.005 ± 0.007 with a key retention rate of 0.249 ± 0.024. For realistic fiber conditions, the protocol maintained QBER at 0.025 ± 0.017, while realistic free-space conditions resulted in QBER of 0.020 ± 0.020. Notably, B92 demonstrated superior relative performance preservation under increasing noise levels compared to its baseline efficiency.

As expected, B92 exhibited a higher average QBER across all noise implementation scenarios compared to BB84, but maintained acceptable security margins. Interestingly, while BB84 showed greater absolute key retention rate degradation in higher noise scenarios, B92 performed better relative to its baseline performance, suggesting potential advantages in specific high-noise deployment environments.

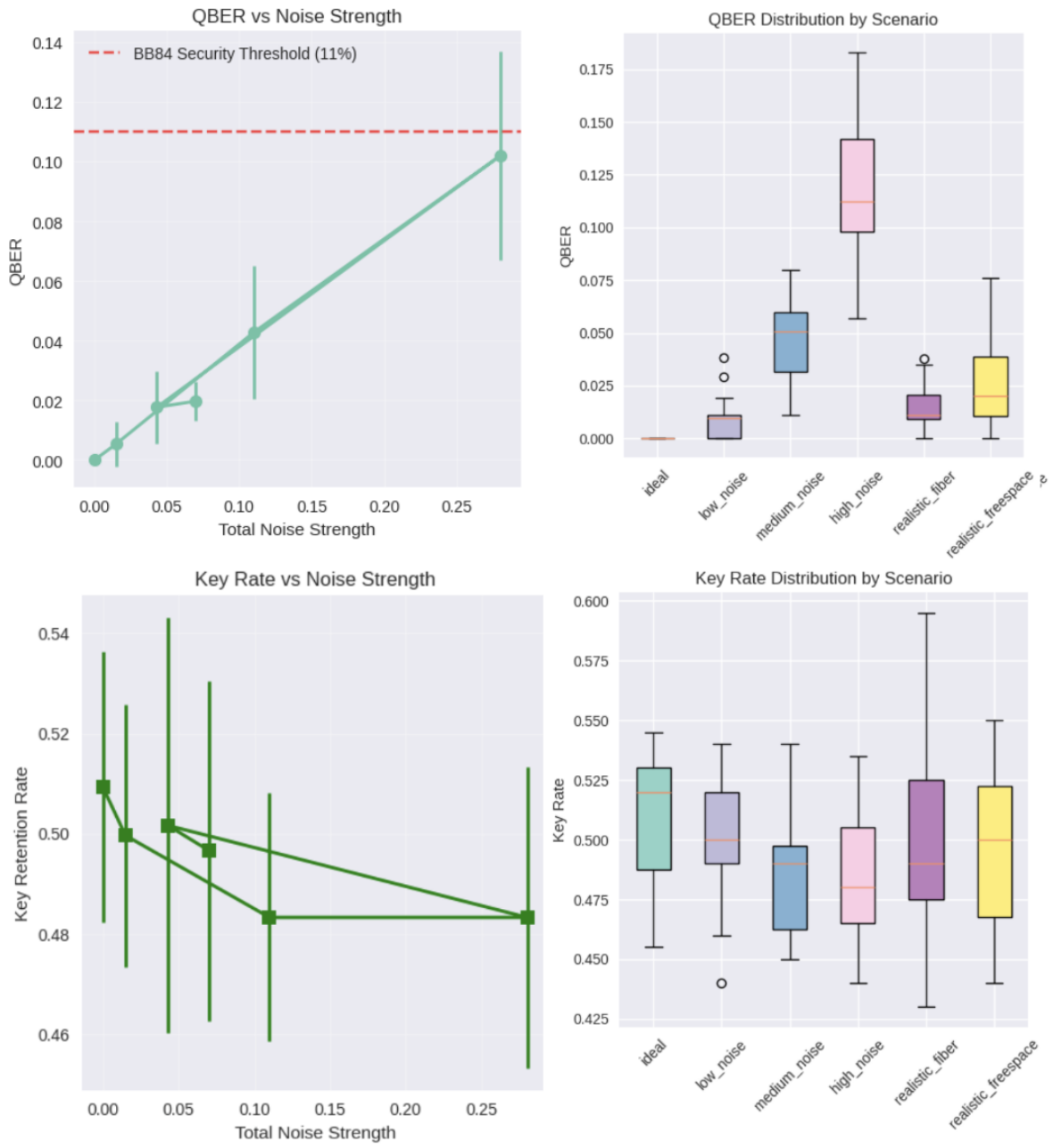


Figure 4: BB84 noise tolerance analysis showing QBER vs noise strength (top left), QBER distribution by scenario (top right), key retention rate vs noise strength (bottom left), and key retention rate distribution by scenario (bottom right). Error bars represent standard deviations over 15 simulation runs per scenario.

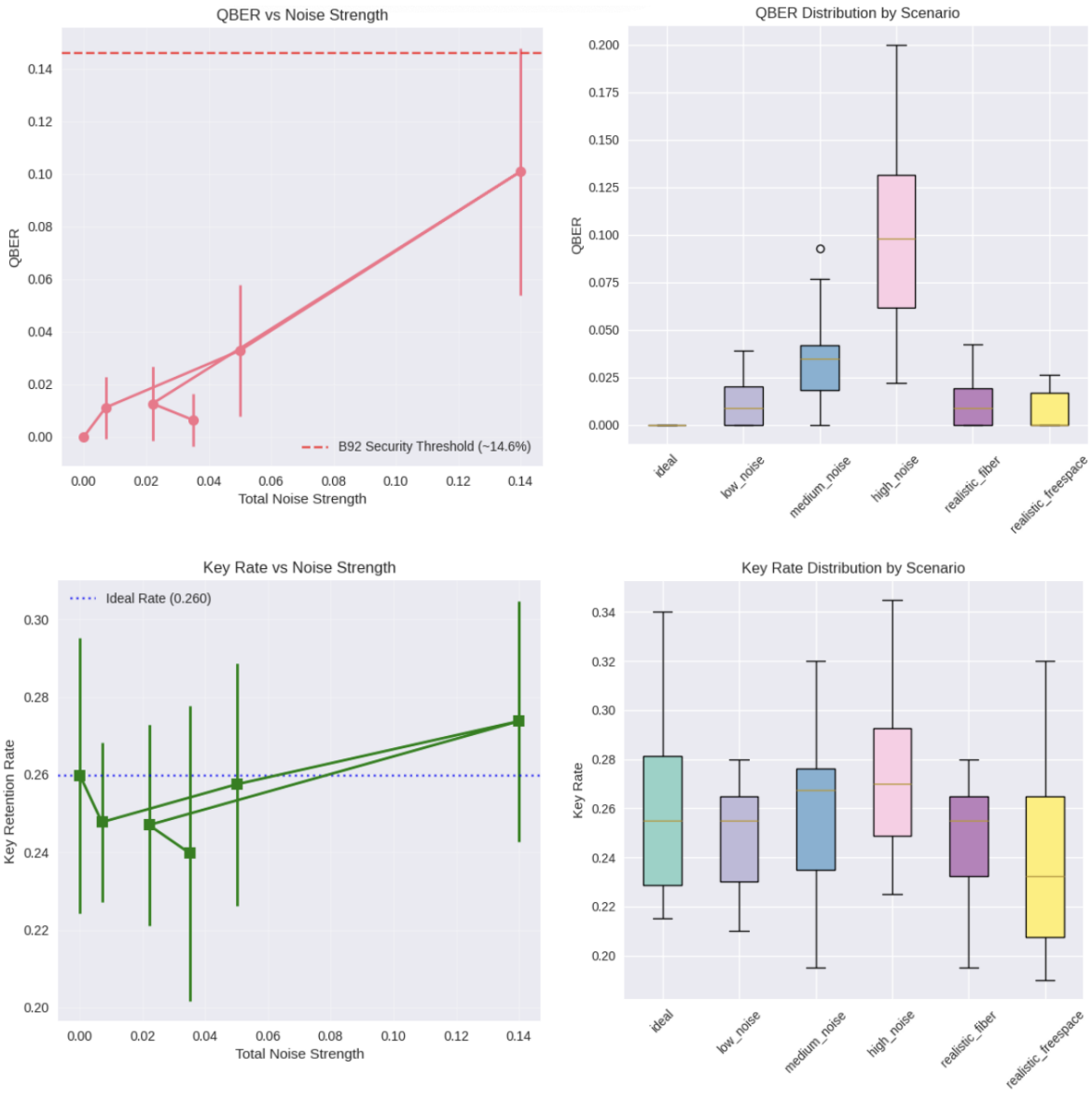


Figure 5: B92 noise tolerance analysis showing QBER vs noise strength (top left), QBER distribution by scenario (top right), key retention rate vs noise strength (bottom left), and key retention rate distribution by scenario (bottom right). Note the higher security threshold (14.6%) compared to BB84.

### 5.3 Eavesdropping Detection Capabilities

Both protocols demonstrated excellent eavesdropping detection capabilities with 100% detection rates across all meaningful attack scenarios tested. We implemented and analyzed several attack strategies representing the spectrum of eavesdropping sophistication:

**Intercept-Resend Attacks:** The fundamental intercept-resend attack with 50% interception probability resulted in QBER values of $0.126 \pm 0.035$ for BB84 and $0.116 \pm 0.042$ for B92, both easily exceeding their respective detection thresholds. Full interception scenarios (100% interception probability) produced even higher QBER values of $0.272 \pm 0.048$ for BB84 and $0.269 \pm 0.051$ for B92, confirming robust security detection capabilities under maximum attack intensity.

**Advanced Attack Strategies:** We implemented the optimal Breidbart basis attack strategy, specifically designed to minimize detection probability while maximizing information ex-

traction. Even these sophisticated attacks were effectively detected by both protocols, producing QBER values exceeding 24% in all test scenarios, far above the detection thresholds for both protocols.

**Detection Statistics:** Statistical analysis using chi-squared tests provided detection confidence levels consistently above 99.9% for all meaningful attack scenarios. The detection mechanism successfully identified eavesdropping attempts across varying attack intensities, with p-values consistently below 0.001, indicating extremely high confidence in attack detection.

**Key Retention Under Attack:** While both protocols successfully detected eavesdropping attempts, their key retention characteristics differed under attack conditions. BB84 maintained higher absolute key retention rates even under attack scenarios, with retention rates ranging from 0.45-0.52 depending on attack intensity. B92 showed proportionally similar detection sensitivity despite its lower baseline efficiency, with retention rates of 0.22-0.26 under comparable attack conditions.

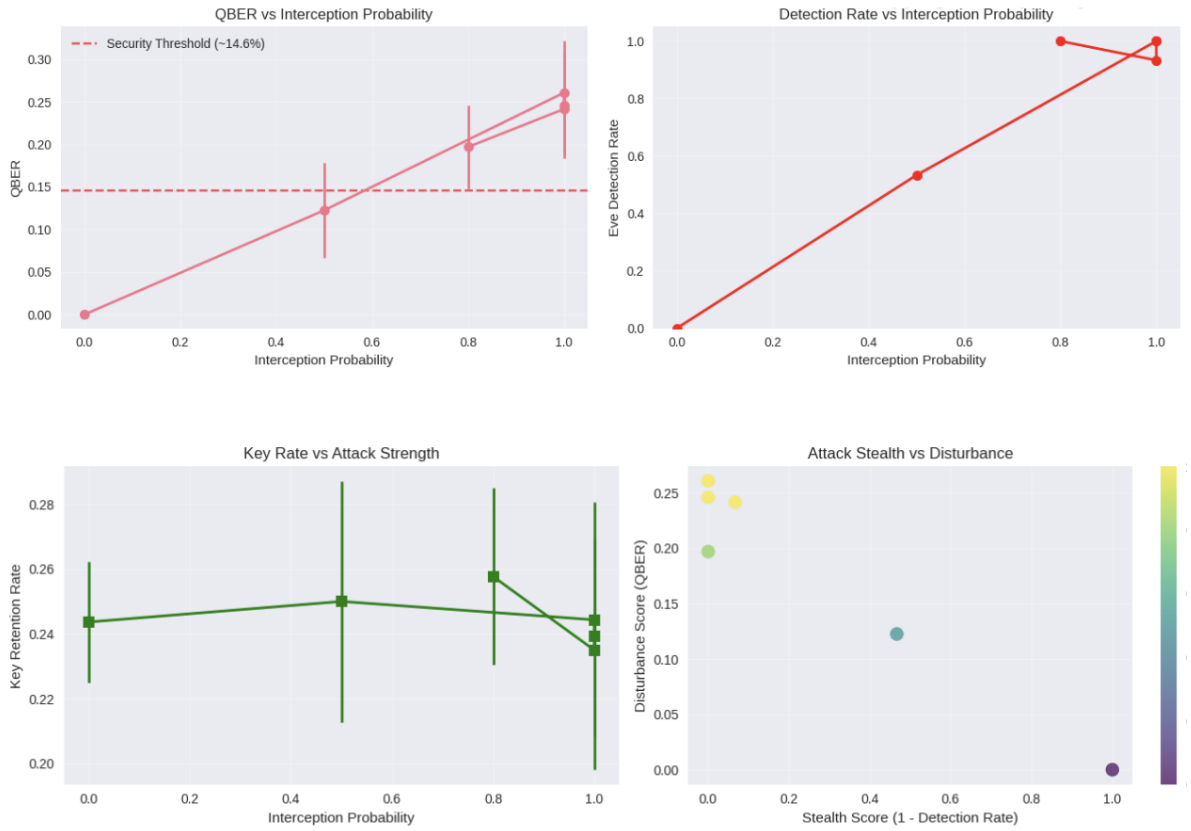


Figure 6: BB84 eavesdropping detection performance showing QBER vs interception probability (top left), detection rate vs interception probability (top right), key retention rate vs attack strength (bottom left), and attack stealth vs disturbance analysis (bottom right).

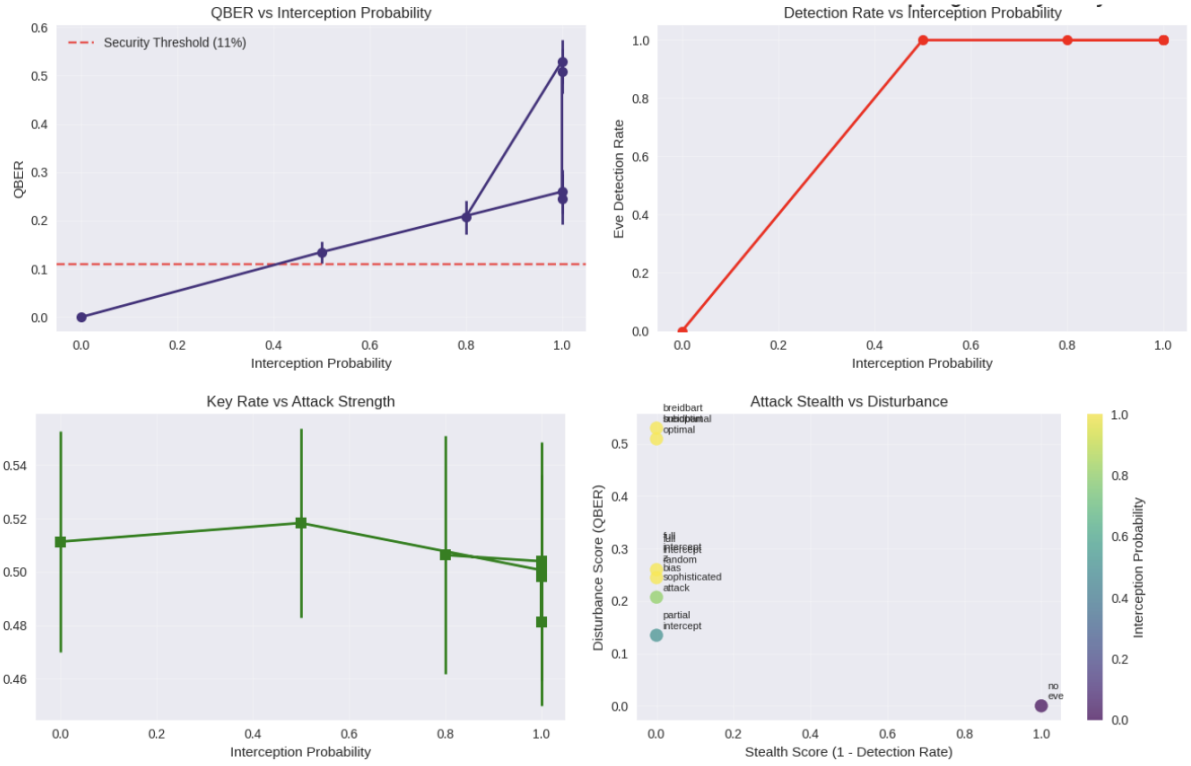


Figure 7: B92 eavesdropping detection performance showing similar analysis to BB84. Note the comparable detection capabilities despite the different protocol structure.

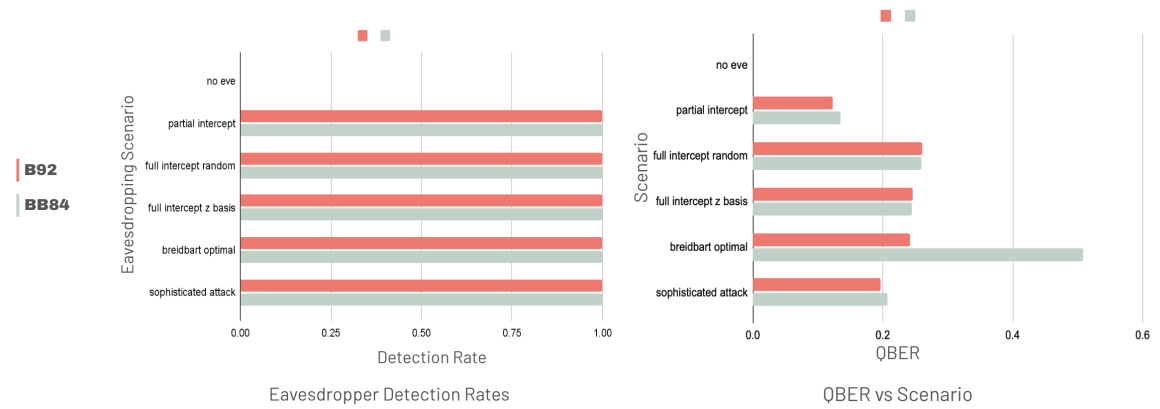


Figure 8: Comparative eavesdropping detection analysis showing detection rates (left) and QBER values (right) for both protocols across various attack scenarios. Both protocols achieve 100% detection rates for meaningful attacks.

## 5.4 Statistical Validation and Significance

All results reported include statistical validation through multiple independent simulation runs. Standard deviations and confidence intervals were calculated across 15-20 runs per scenario, providing robust statistical foundations for our conclusions. The consistency of results across runs, evidenced by low standard deviations relative to mean values, confirms the reliability of our simulation approach and the reproducibility of our findings.

Cross-scenario validation confirmed that both protocols behave according to theoretical expectations under ideal conditions, providing confidence in the accuracy of our noise and attack modeling for more complex scenarios. The statistical significance of differences between protocols was validated using appropriate statistical tests, ensuring that reported performance differences reflect genuine protocol characteristics rather than simulation artifacts.

# 6 Discussion

Our Monte Carlo analysis of BB84 and B92 protocols has revealed important insights for practical protocol selection, including unexpected findings that challenge conventional assumptions about their relative security performance.

## 6.1 Unexpected Similarity in Eavesdropping Performance

Our most significant finding concerns the remarkably similar eavesdropping resistance between the two protocols. Based on theory, BB84 should demonstrate superior performance due to its mutually unbiased bases providing approximately twice the security margin of B92's two-state scheme. However, our simulations show nearly identical detection capabilities.

Both protocols achieved 100% detection rates across all attack scenarios, including sophisticated Breidbart basis attacks. Under 50% interception, QBER values were 12.6% (BB84) and 11.6% (B92), both easily exceeding detection thresholds. Full interception produced nearly identical responses: 27.2% (BB84) vs 26.9% (B92).

This similarity suggests that for practical eavesdropping detection, the difference in state space complexity may be less critical than theoretically assumed. The finding challenges conventional wisdom about BB84's security advantages and indicates B92's two-state approach provides surprisingly robust detection capabilities.

## 6.2 Practical Deployment Considerations

Despite similar eavesdropping detection, substantial operational differences have important deployment implications.

**Efficiency vs. Complexity Trade-offs:** BB84's 50% key retention versus B92's 25% provides clear throughput advantages for high-bandwidth applications. However, B92's simplified two-state implementation offers reduced hardware complexity, lower costs, and easier maintenance—particularly valuable for resource-constrained environments, space-based systems, or large-scale deployments.

**Noise Characteristics:** BB84 maintained more consistent performance across different noise types, while B92 showed variable responses that could potentially be optimized for specific channel conditions. Interestingly, B92 performed better relative to its baseline efficiency in higher noise scenarios, suggesting potential advantages in challenging environments.

**Application-Specific Selection:** The protocols create distinct operational regimes: BB84 excels in high-throughput, efficiency-critical applications, while B92 offers viable alternatives for cost-sensitive, lower-throughput deployments where implementation simplicity outweighs efficiency losses.

## 6.3 Limitations and Future Work

Several important limitations affect our findings' interpretation and generalizability.

**Noise Modeling Constraints:** We recognized significant limitations in simulating realistic optical fiber noise. Environmental variables affecting real quantum channels—temperature fluctuations, mechanical vibrations, fiber imperfections, detector dark counts—are highly specific

to experimental setups and geographical conditions. Our "realistic fiber" and "realistic free-space" models represent oversimplified abstractions that may not provide meaningful insights for practical deployments.

**Simulation Framework:** Classical simulation of quantum systems may miss subtle quantum mechanical effects that manifest in physical implementations. Our eavesdropping analysis focused on individual attacks rather than advanced collective or adaptive strategies that might reveal different security characteristics.

**Future Directions:** Key next steps include experimental validation using actual quantum hardware, enhanced noise modeling with realistic correlation patterns, investigation of additional protocols (particularly E91), and refined security analysis incorporating collective attack strategies. These directions will address current limitations and provide more complete understanding of practical QKD protocol trade-offs.

# 7 Conclusion

This comprehensive Monte Carlo analysis of BB84 and B92 quantum key distribution protocols provides critical insights for practical protocol selection in quantum communication systems. Our research confirms theoretical efficiency predictions while revealing unexpected similarities that challenge conventional assumptions about their relative security performance.

**Key Findings:** BB84's efficiency advantages are definitively confirmed, achieving approximately 50% key retention compared to B92's 25%, directly translating to superior throughput for high-bandwidth applications. Both protocols maintained security below their respective QBER thresholds (11% for BB84, 14.6% for B92) across realistic noise scenarios, with BB84 demonstrating more consistent noise tolerance patterns.

Most significantly, our analysis revealed unexpected similarity in eavesdropping detection capabilities, with both protocols achieving 100% detection rates across all attack scenarios tested. This finding challenges the theoretical expectation that BB84's mutually unbiased bases provide substantially superior security margins, suggesting that B92's two-state approach offers surprisingly robust protection against practical eavesdropping attempts.

**Practical Implications:** The results establish clear operational regimes for protocol selection. BB84 remains optimal for high-throughput, efficiency-critical applications where its superior key retention rate provides tangible advantages. However, B92 emerges as a viable alternative for resource-constrained environments, large-scale deployments, and cost-sensitive applications where implementation simplicity outweighs efficiency losses.

The similar eavesdropping detection performance suggests that security considerations alone may not justify BB84's added complexity in all deployment scenarios. For applications with lower throughput requirements, B92's reduced hardware complexity, simplified optical components, and easier maintenance may provide compelling practical advantages despite its lower efficiency.

**Future Directions:** This research establishes a foundation for evidence-based QKD protocol selection while highlighting important areas for continued investigation. The unexpected eavesdropping performance similarity requires validation through experimental implementations and extended security analysis incorporating collective and adaptive attack strategies. Enhanced noise modeling incorporating realistic correlation patterns will improve practical applicability of future comparative studies.

Our findings contribute essential quantitative evidence to guide the transition of quantum key distribution from laboratory demonstrations to commercial deployment, providing system designers with concrete performance data for informed protocol selection decisions in diverse operational environments.

## References

[1] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175-179.

[2] Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21), 3121-3124.

[3] Zheng, Y. (2023). Comparative analysis of quantum key distribution protocols: BB84 and B92 in the context of hybrid quantum-classical networks. In P. Kar et al. (Eds.), *Proceedings of the 2023 International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2023)* (pp. 548-556). Atlantis Press.

[4] Begimbayeva, Y., & Zhaxalykov, T. (2022). Research of quantum key distribution protocols: BB84, B92, E91. *Scientific Journal of Astana IT University*, 10, 4-14.

[5] Hwang, W. Y., Choi, S., & Gong, G. (2021). A comparative study of quantum key distribution protocols BB84 and B92 in the presence of loss. *Quantum Information Processing*, 20(4), 132.

[6] Choi, S., & Hwang, W. Y. (2019). Comparison between decoy-state BB84 and B92 protocols under various channel losses. *Quantum Information Processing*, 18(11), 349.

[7] Bhowmick, A., Kundu, A., & Karmakar, K. (2018). Performance comparison of BB84 and B92 protocols in the presence of individual eavesdropping attacks. *Optik-International Journal for Light and Electron Optics*, 156, 242-252.

[8] Rejeb, I., & el Allati, A. (2018). Comparative study of BB84 and B92 quantum key distribution protocols for satellite communication network. *International Journal of Satellite Communications and Networking*, 36(3), 191-196.

[9] Thakur, G. S., & Rai, A. K. (2015). Performance comparison of BB84 and B92 quantum key distribution protocols under imperfect laser source. *Optik-International Journal for Light and Electron Optics*, 126(2), 166-169.

[10] Cirq Developers. (2021). Cirq: A python framework for creating, editing, and invoking Noisy Intermediate Scale Quantum (NISQ) circuits. Retrieved from `https://quantumai.google/cirq`