Convergence
A Journal for Young Researchers

ORIGINAL RESEARCH

Received: 8-28-25; Accepted: 11-22-25;
Managing Editor: Jonas Katona;
Action Editor: Jonas Katona

Comparative Performance Analysis of BB84 and E91 Quantum Key Distribution Protocols Under Real-World Imperfections

Eduardo Lougon Sampaio Lopes

Instituto GayLussac, Niterói, Brazil

Abstract

Quantum key distribution (QKD) has emerged in recent decades as a potential approach to guarantee secure data transmission, especially as conventional cryptographic methods face threats from the rise of quantum computing. While there are numerous studies on security proofs and theoretical analyses, practical implementation and real-world validation of QKD protocols remain limited. Therefore, this research aims to analyze the performance of BB84 and E91 QKD protocols over eavesdropping attacks and imperfect conditions introduced by physical communication channels. We hypothesize that BB84 outperforms E91, demonstrating higher key rates and lower quantum bit error rates (QBER) across all communications channels due to its resilience to noise and independence on entangled pairs. First, a simulation of both QKD protocols in Python is run under eavesdropping attacks and distinct levels of noise and photon loss associated with water, free-space, and optical fiber channels. Then, the performances are evaluated by measuring metrics such as key rates, key length, and QBER. The results show that BB84 was more efficient under real-world imperfections, while E91 was notably sensitive to noise, demonstrating high QBER values. Thus, our hypothesis was proven right, offering valuable insights into the current limitations, effectiveness, and security of the BB84 and E91 protocols for future QKD practical implementations and research.

Keywords: quantum key distribution (QKD), BB84 protocol, E91 protocol, quantum bit error rate (QBER), secure key rate, sifted key rate, quantum communication, photon loss, depolarization

1. Introduction

In a society increasingly dependent on digital financial transactions and communication, information security is vital. To protect sensitive data, modern systems rely heavily on cryptography. However, the development of quantum computers and algorithms has fundamentally threatened the security of many traditional cryptographic methods. Shor's quantum

algorithm (Shor, 1994), for instance, can efficiently factor large integers, thereby rendering RSA and other widely used public-key systems vulnerable (Bernstein, Heninger, Lou, & Valenta, 2017) (Bhatia & Ramkumar, 2020). As a result, the search for reliable and secure solutions has become a key concern. Fortunately, a promising alternative based on the principles of quantum mechanics has been found: quantum key distribution (QKD). In recent decades, many protocols, such as B92 (Bennett, 1992) and SARG04 (Scarani, Acín, Ribordy, & Gisin, 2004), have been proposed to secure communication through the transmission of quantum bits (qubits), usually described by the polarization of photons. However, this paper focuses on two of the most foundational and widely studied quantum key distribution protocols: BB84 and E91.

The BB84 protocol, introduced by Bennet and Brassard in 1984, was the first QKD method and remains the most widely researched and implemented. Its security, only mathematically proven in 2000 (Shor & Preskill, 2000), originates from the uncertainty principle of quantum mechanics and the no-cloning theorem (Nielsen & Chuang, 2010). By using two conjugate bases — typically the rectilinear and diagonal bases — Alice and Bob can send polarized photons whose polarization directions encode binary values (0 and 1). When both communication parties select the same basis, and assuming a noiseless channel, Bob will measure the correct bit. However, if Alice sends a photon encoded in the rectilinear basis and Bob chooses the diagonal basis, quantum uncertainty dictates a 50% probability of obtaining the correct value. Using a classical insecure channel, Alice and Bob go through a process called sifting and generate shared secret keys to later encrypt and decrypt information securely. It is essential to note that an eavesdropper cannot measure the photons without disturbing their quantum states: any interception and remeasurement by Eve inevitably introduces detectable errors in the sifted key, allowing Alice and Bob to infer the presence of eavesdropping (Bennett & Brassard, 2014).

In contrast, the E91 protocol is based on quantum entanglement and the violation of Bell's inequalities (Nielsen & Chuang, 2010). Proposed by Ekert in 1991, the protocol uses pairs of entangled photons shared between Alice and Bob, instead of sending individually prepared qubits. Each party randomly selects bases and performs measurements on their respective photons. When compatible measurement settings are used, the results are strongly correlated — a direct manifestation of entanglement. For certain incompatible basis choices, the correlations deviate from classical predictions, enabling a statistical violation of Bell's inequalities. This sensitivity to measurement settings makes E91 more susceptible to noise and interference, which can increase quantum bit error rate (QBER) in practical channels. However, this same sensitivity underpins its security since any interaction by an eavesdropper disturbs the delicate quantum correlations, producing highly detectable spikes in QBER. To verify the security of the quantum channel, they can compare a subset of their measurement results to check for violations. If Bell's inequalities are satisfied rather than violated, this would imply that the correlations could be explained by local realistic (classical) models, suggesting that entanglement may have been lost due to depolarization or eavesdropping. Finally, if communication is private, they can use bits measured in compatible bases to generate a secret key, just like in the BB84 protocol (Ekert, 1991).

While both protocols offer theoretical security rooted in the laws of quantum mechanics, their performance under realistic and adversarial conditions can differ significantly. In this respect, this research aims to compare the BB84 and E91 protocols in simulated quantum channel scenarios, such as satellite, fiber optic, and underwater communications. The study incorporates factors like photon loss, noise, and active eavesdropping attacks to assess the efficiency of each protocol under stress. After simulation, performance metrics, such as fidelity, quantum bit error rate (QBER), and key rate, are evaluated. We hypothesize that BB84 outperforms E91 in efficiency across all scenarios tested, since E91 requires correlated measurements, which are more susceptible to decoherence and attenuation, particularly in lossy channels. Accordingly, we predict that underwater channels, characterized by strong absorption and scattering, will degrade quickly,

rendering them impractical for real-world implementation.

In recent years, QKD has begun to move beyond theory into the real world. Satellite- and fiber optics-based implementations are rapidly becoming a reality. In 2017, scientists successfully demonstrated the distribution of entangled photon pairs through satellite-based quantum communication links between two separate locations over 1200 kilometers apart (Yin et al., 2017). Similarly, advancements in long-distance fiber optic QKD have enabled secure key exchange over hundreds of kilometers, using techniques like quantum repeaters and low-loss channels to mitigate signal degradation (Briegel, Dür, Cirac, & Zoller, 1998). However, most prior studies focus on idealized conditions that, although extremely valuable, do not account for practical limitations. Thus, this work seeks to connect theory and implementation in order to offer insights into the effectiveness and limitations of the most widely discussed protocols for future QKD real-world applications and research.

This paper is organized as follows: Section 2 sketches the methodology for the performance analysis of BB84 and E91 protocols. In section 3, the results' metrics such as QBER, secure and sifted key generation rate, and key length are presented and discussed. We conclude in Section 4.

2. Methods

This section outlines the simulation methodology used to implement and evaluate quantum key distribution (QKD) protocols — specifically BB84 and E91 — under realistic channel conditions. As access to experimental quantum hardware, like single-photon sources and detectors, was not available for this study, the polarization states, measurements, and channel effects were modeled computationally. Each protocol was implemented with and without eavesdropping, and a series of key performance metrics were used to assess protocol security and reliability over varying distances.

This section is separated into four subsections. Subsection 2.1 presents the main environmental factors — photon loss and depolarization — that affect photon transmission through different channels and explains how these were modeled computationally. Subsections 2.2 and 2.3 describe the implementation of the BB84 and E91 protocols, respectively, including how eavesdropping was simulated. Lastly, subsection 2.4 defines the performance metrics used to evaluate the protocols, such as quantum bit error rate (QBER), sifted and secure key rate, key length, and CHSH S-values.

2.1. Channel Modeling: Photon Loss and Depolarization

In real-world quantum communication, photons traveling through physical media, such as water, optical fibers, or free space, are affected by two key factors — photon loss and depolarization — which can significantly reduce the efficiency and performance of QKD protocols. In the simulation, both phenomena are modeled as functions of the transmission distance and are adapted for each type of communication channel.

Firstly, photon loss refers to the probability that a photon fails to reach the receiver due to absorption or scattering. To quantify this phenomenon, Beer-Lambert's law (Teich & Saleh, 2007) can be employed:

$$I(d) = I_0 10^{-\alpha d}, \tag{1}$$

where I(d) denotes the intensity of light after propagating a distance d (in km) through an absorbing or scattering medium,

I_0 represents the initial power, and α (dB/km) the attenuation coefficient (Czerwinski & Czerwinska, 2022). To obtain the fraction of photons that survive transmission, both sides are divided by I_0, and the factor 1/10 is used to convert the logarithmic decibel scale to the linear power scale:

$$P_{survive}(d) = \frac{I(d)}{I_0} = 10^{-\frac{\alpha d}{10}} \quad (2)$$

Photons are probabilistically dropped according to the loss model defined by Equation 2. For each photon simulated, a random number in [0,1] is generated and compared to Psurvive(d). If the number is greater, the photon is considered lost and excluded from the measurement process.

In order to simulate realistic channel conditions, typical attenuation coefficients of all communication channels' conditions were used. These are shown in Table 1. However, it is important to note that additional loss mechanisms (detection or coupling) are not included in this work, as the focus of this simulation is to quantify the effect of propagation distance and medium-dependent attenuation. These effects are experimentally compensated and therefore omitted to isolate the impact of transmission loss across different channels. Furthermore, the present free-space channel model represents an overly simplified description of optical propagation and does not include the effects of atmospheric turbulence. In realistic free-space optical links, turbulence arises from random fluctuations caused by temperature and pressure variations. Therefore, a full-scale treatment of these effects, stochastically inducing changes in the phase and amplitude of transmitted photons, time-varying losses, etc., would require advanced numerical techniques, such as split-step propagation, which lie beyond the scope of this work.

Table 1: Attenuation Coefficient (α), measured in dB per kilometer, for each communication channel evaluated. Higher α corresponds to more lossy environments

Channel	Attenuation Coefficient (dB/km)
Underwater	200 (Zhao et al., 2019)
Fiber optic	0.2 (Agrawal, 2012)
Free-space	1 (Aspelmeyer, Jennewein, Pfennigbauer, Leeb, & Zeilinger, 2003)

Note: These values may vary for different fiber materials, and weather and water conditions.

Secondly, depolarization refers to the degradation of a photon's polarized state due to interaction with the transmission medium. In the simulation, this is implemented by applying a random Pauli error (Nielsen & Chuang, 2010) with a probability that increases with distance. The expression can be formulated from the exponential-in-time form of a Markovian depolarizing channel, corresponding to a single-qubit Pauli channel with equal probabilities for X, Y, and Z errors:

$$P(t) = 1 - e^{-\Gamma t}, \quad (3)$$

where P(t) is the probability that depolarization has occurred by time t and Γ is the decay rate, with units s^{-1} (Xu et al., 2010). However, since the simulation is distance-dependent, the time variable is calculated by distance over speed (v), considering v is constant. This way, a new parameter λ is defined:

$$\Gamma t = \Gamma \frac{d}{v} = \frac{d}{\lambda}, \ where \ \ \lambda = \frac{v}{\Gamma}$$

Then, substituting into Equation 3, the final equation used to model the probability that a random Pauli X, Y, or Z error is applied to a photon polarization is obtained:

$$P_{\text{depol}}(d) = 1 - e^{-d/\lambda}, \tag{4}$$

where λ is defined as the depolarization length, with units dependent on the distance *d*.

For this simulation, typical values of lambda for each channel (underwater, fiber optic, and free-space) were used. These are shown in Table 2. The parameter λ directly maps to the distance-dependent depolarization probability (Equation 4), representing the chance that a photon becomes depolarized after traveling a distance *d*. Once depolarization occurs, a random Pauli X, Y, Z error is applied with equal probability (1/3), assuming isotropic polarization noise with no preferred basis, since in many transmission media polarization disturbances are well approximated as randomizing processes. If future experimental data show bias toward particular error axes, the model can be replaced by a Pauli channel with p_x, p_y, p_u fit from data.

Table 2: Depolarization length (λ), measured in kilometers, for each communication channel evaluated

Channel	Depolarization length λ (km)
Underwater	0.1 (Zhao et al., 2019)
Fiber optic	68 (Zhang et al., 2025 - provisional assumption)
Free-space	63 (Buttler et al., 1998)

Note: These values were estimated by equating Equation 4 to a proportion of QBER from experimental data.

2.2. Protocol Implementation: BB84

In a laboratory or field deployment of BB84 (Bennett & Brassard, 2014), Alice prepares truly single photons and encodes each bit in one of two typical polarization bases: the rectilinear basis (Z), which comprises horizontal |H⟩ (0°) and vertical |V⟩ (π/2), and the diagonal basis (X), which has anti-diagonal |A⟩ (π/4) and diagonal |D⟩ (3π/4) (Maloo, n.d.), where,

$$|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) \tag{5}$$

$$|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \tag{6}$$

These photons then travel through noisy and lossy channels before reaching Bob's randomly chosen polarization bases and single-photon detectors. Afterward, both parties communicate through a classical channel to sift their data and extract a secure key. However, since this process is modeled computationally in the simulation, the physical apparatus is replaced with algorithmic steps that mirror each operation.

The first step of the protocol is generating the random basis and bits. Alice creates two uniformly random sequences of length n: a bit string $\{a_i\}$ with $a_i \in \{0, 1\}$ and a basis string $\{\theta_i\}$ with $\theta_i \in \{Z, X\}$. Then, each bit is encoded as the polarization state of a photon, as shown in Table 3.

Table 3: Bit representation of different states of polarization in the BB84 protocol

Polarization	Basis	Bit Representation
0	Z (Rectilinear)	0
$\pi/2$ (90°)	Z (Rectilinear)	1
$\pi/4$ (45°)	X (Diagonal)	0
$3\pi/4$ (135°)	X (Diagonal)	1

Next, these photons traverse a hypothetical channel characterized by attenuation α (dB/km) and depolarization length λ, where the survival and noise probabilities defined by Equation 2 and Equation 4, respectively, are applied. A photon is considered lost — and its value is set to None — if the survival probability is smaller than a randomly generated number (k) $\in \{0, 1\}$. Similarly, a photon suffers depolarization, represented by the application of random Pauli X, Y, or Z errors with equal probability, if k is smaller than the depolarization probability (see Appendix B).

After channel effects are applied, Bob receives the photons and measures each one in a randomly chosen basis. He generates a basis string $\{\phi_i\}$ with $\phi_i \in \{Z, X\}$ and length n. For each incoming photon, Bob uses the corresponding basis ϕ_i to perform his measurement. For example, if Bob detects a photon polarized in the rectilinear basis (horizontal $|H\rangle$ (0°) or vertical $|V\rangle$ ($\pi/2$)) and measures its value with the Z basis, he deterministically records either 0 for $|H\rangle$ or 1 for $|V\rangle$. In contrast, whenever his measurement basis does not match the photon's polarization basis, the output is completely random, yielding 0 or 1 with equal probability, because the probability that Bob's X measurement returns "0" ($|A\rangle$ — defined by Equation 5) when the photon is actually $|H\rangle$ is given by the squared overlap (Born rule) (Nielsen & Chuang, 2010):

$$P(b = 0 \mid \psi = |H\rangle) = |\langle A \mid H\rangle|^2 = \left|\frac{\langle H| + \langle V|}{\sqrt{2}}|H\rangle\right|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} \tag{7}$$

After measurement, Alice and Bob first identify and discard any rounds in which photons were lost. Then, the sifting

process begins — the stage in which Alice and Bob generate a key with the bits measured on the same basis. However, due to channel noise or potential eavesdropping, some of these bits may not match. Thus, in the final error-correction stage, Alice and Bob reconcile and remove any mismatched bits to arrive at an identical secret key.

Building on the error-correction stage, eavesdropping is modeled as an intercept-resend attack. In this sense, we introduce an eavesdropper, Eve, into the communication channel after all loss and noise are applied. For each transmitted photon, Eve has a probability e of intercepting it (the eavesdropper strength). Upon interception, the photon's polarization is measured in a randomly chosen basis {Z, X} with equal probabilities. The measurement result is then used to prepare and resend a new photon to Bob, encoded in the same basis Eve measured. This way, when Eve's basis matches Alice's, her intervention goes undetected. In contrast, if her basis differs, she introduces a disturbance with a probability of 50%, since the re-prepared state collapses onto a random result in Bob's correct basis (see Appendix B). Thus, by comparing a sample of their generated bits, Alice and Bob can detect an eavesdropper in an ideal loss- and noise-free environment simply by checking for any errors.

2.3. Protocol Implementation: E91

In contrast to BB84, Ekert's E91 protocol (Ekert, 1991) is based on entanglement. In other words, instead of Alice sending individually prepared photons to Bob, both parties share entangled photon pairs. When they perform measurements on their respective particles using appropriately chosen bases, their outcomes are strongly correlated in a way that violates Bell's inequalities (Nielsen & Chuang, 2010).

Similar to the BB84 protocol, the first step of E91 involves preparing the photons and selecting a measurement basis. In this simulation, it is assumed that a third party, Victor, equidistant from Alice and Bob, sends, to both parties, photons prepared in the maximally entangled singlet state

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{8}$$

Next, Alice and Bob independently select one of three measurement bases (angles) randomly, with uniform probabilities. Table 4 presents the possible choices for each party. To test the violation of Bell's inequality — and, by extension, the security of the communication channel — two of the three possible choices are allocated to compute correlations, while the remaining one is reserved for key generation. In this simulation, the basis that corresponds to a measurement angle of $\pi/2$ is used to generate the final key.

Table 4: Possible Measurement Bases for Alice and Bob

Basis Index	Alice's bases	Bob's bases
0	$\pi/2$	$\pi/2$
1	0	$\pi/8$

2	π/4	-π/8

Then, in step two, the photons are sent through two hypothetical quantum communication channels, from Victor to Alice and from Victor to Bob, of distance d/2, where d is the total distance between Alice and Bob. Realistically, the quantum channels are modeled with noise and loss, probabilistically determined by Equation 4 and Equation 2, respectively. A photon is considered lost — and its value is completely ignored — if the survival probability (Equation 2) is smaller than a randomly generated number (k) ∈ {0, 1}. On the other hand, when the depolarization probability is greater than (k), the photon becomes mixed, resulting in completely random measurement outcomes.

Upon receiving the particles, Alice and Bob measure their respective photons in their chosen bases, initiating step three. For this protocol, the results of the measurement can be either +1 (|0⟩) or -1 (|1⟩), which represent the spin of the particle. Since the photons are entangled, as described in Equation 8, quantum mechanics predicts perfect anticorrelation of the results obtained by Alice and Bob (Ekert, 1991) whenever they measure in the same basis. This means that

$$P\left(b = -a \mid \theta_A = \theta_B\right) = 1, \tag{9}$$

where a, b, and θ_a, θ_β represent Alice and Bob's measurement outcomes and selected angles, respectively. It is also important to mention that the singlet state |Ψ⟩ defines a 50% probability of measuring each outcome for both parties, because the probability of Alice measuring +1 is given by:

$$\left|\left|\Psi^{-}\right\rangle\right|^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}, \tag{10}$$

and after this measurement, |Ψ⟩ collapses to just

$$\left|\Psi^{-}\right\rangle = |01\rangle, \tag{11}$$

where Bob has a 100% chance of measuring -1. Thus, Bob also has a 50% total probability of obtaining one of the results, as his outcome is dependent on Alice's 0.5 probability.

Building on this, the correlation between both parties' outcomes can be expressed by (Ekert, 1991):

$$E\left(\theta_A, \theta_B\right) = P_{++} + P_{--} - P_{+-} - P_{-+}, \tag{12}$$

where, for instance, P_{+-} is the probability that Alice obtains +1 and Bob -1. Therefore,

$$P_{same} = P_{++} + P_{--}, \quad P_{opp} = P_{+-} + P_{-+},$$

meaning that the probability of Alice and Bob measuring the same outcomes can be calculated by:

$$E\left(\theta_A,\ \theta_B\right) = P_{same} - P_{opp} \ \Rightarrow\ P_{same} = \frac{1 + E\left(\theta_A, \theta_B\right)}{2}. \tag{13}$$

Moreover, the expected correlation coefficient can be written as (Díaz & Lenin, 2014):

$$E(\theta_A, \theta_B) = -\cos[2(\theta_A - \theta_B)], \tag{14}$$

finally giving the expression in the form:

$$P_{same} = \frac{1 - \cos[2(\theta_A - \theta_B)]}{2}. \tag{15}$$

In the simulation, Equation 15 is used to calculate the probability that Bob's outcome matches Alice's based solely on the measurement bases (angles) selected. For example, if Alice chooses to measure her photon at an angle of π/2, as Bob also does, Equation 15 will return a value of 0, meaning that, as seen in Equation 9, the results of measurements in the same bases are anti-correlated (see Appendix B).

In sum, step three of the simulation starts with Alice measuring the value a ∈ {+1, -1} with equal probability. Then, the expected correlation, defined by Equation 14, is calculated and used in Equation 15 to determine the probability that Bob measures b to be equal to a. Subsequently, this probability is compared to a randomly generated number (k) ∈ {0, 1}. If Psame is greater, Bob's outcome matches Alice's. On the other hand, if the opposite is true, the results are anti-correlated.

Finally, both parties communicate in a classical channel to share the orientations of the detectors used and divide the measurements into two separate groups (Ekert, 1991). While the group in which the measurement angles matched and were equal to π/2 is allocated to generate the secret key, the other is used to evaluate if the channel was disturbed by an eavesdropper. To achieve this, both parties publicly reveal the results obtained within the second group of measurements and calculate if the CHSH inequality (Clauser, Horne, Shimony, & Holt, 1969) is violated. A violation of the inequality would mean that quantum behavior was preserved, ensuring the channel was not disturbed.

Lastly, eavesdropping is implemented for the E91 protocol as an intercept-resend attack. For each transmitted photon pair, Eve has a probability e (the eavesdropping strength) of intercepting it. In the simulation, the attack is modeled as a complete loss of entanglement: when an interception happens, both photons are replaced by randomly generated polarization outcomes, independent of each other and of Alice's and Bob's chosen bases. This represents the effect of Eve measuring and resending photons in a fully random manner, eliminating quantum correlations entirely. As a result, correlations are notably disturbed, and the CHSH-S value decreases toward the classical limit as e increases.

2.4. Performance Metrics

To compare the performance of both protocols under limiting realistic conditions, a series of performance metrics is evaluated. These include QBER, sifted key rate, secure key rate, key length, and CHSH S-Values. Each of the metrics offers insights into different aspects of the BB84 and E91 protocols, from efficiency to security guarantees. Together, they will be used to determine how viable and secure each protocol is under varying levels of noise, loss, and eavesdropping — factors that any QKD protocol should withstand in a practical implementation.

QBER measures the fraction of mismatched bits in the sifted key and serves as an indicator of noise and potential eavesdropping. The sifted key rate corresponds to the fraction of detected bits retained after basis reconciliation, while the secure key rate estimates the amount of final usable key material after accounting for information leakage and error

correction. Similarly to the sifted key rate metric, the key length is particularly relevant for assessing the practical usability of the protocol. For E91, the CHSH S-value quantifies non-classical correlations between Alice and Bob's measurement outcomes.

In the BB84 protocol, an asymptotic security analysis under idealized conditions, assuming infinite key lengths and one-way error correction and privacy amplification, establishes a theoretical threshold around 11%, beyond which secure key generation is no longer possible (Shor & Preskill, 2000). However, this value should be interpreted as a guideline rather than a strict limit, since real implementations operate under finite-key constraints and may tolerate slightly different error levels. In this work, we follow a conventional assumption for simplicity: set the secure key rate to zero once the QBER exceeds this threshold. Therefore, it is important to note that practical systems would require a more detailed finite-key security analysis to determine the exact limits.

Full mathematical definitions for these metrics, along with the derivations of the formulas used in the simulations, are provided in Appendix C.

3. Results

For both protocols, the transmission of 100,000 photons across three types of channels — fiber, underwater, free-space — was simulated over varying distances and eavesdropping strengths. Specifically, to evaluate the performance of the BB84 and E91 protocols, four distance intervals with varying sampling densities are defined. Table 5 presents these intervals and their respective number of sampling points.

Table 5: Distance intervals with uniformly spaced sampling points.

Distance Intervals	Number of Sampling Points
0–5 km	20 points
6–20 km	15 points
25–50 km	10 points
60–100 km	5 points

This section is divided into four subsections. Each of the first three subsections is dedicated to describing the results of both protocols under each simulated quantum channel. Subsection (3.1) presents the results for the generated key length across all channels. Subsection (3.2) shows the secure and sifted key rates for each protocol separately. Finally, subsection (3.3) reports the quantum bit error rate (QBER) and the CHSH S-values, highlighting the Bell inequality violation for the E91 protocol. Lastly, subsection (3.4) discusses the results obtained and compares the performance of both protocols.

For all subsections, the analysis follows the same structure: first, the results are presented under no eavesdropping to establish a performance baseline. Then, the impact of partial (e = 0.5) and full eavesdropping is examined to assess how

attacks affect the protocols' performance.

3.1. Key Length

In this subsection, we present the results for the key length across the different communication channels. Figure 1 shows the key length as a function of distance for both protocols, under ideal, fiber-optic (fiber), underwater (water), and free-space transmission.

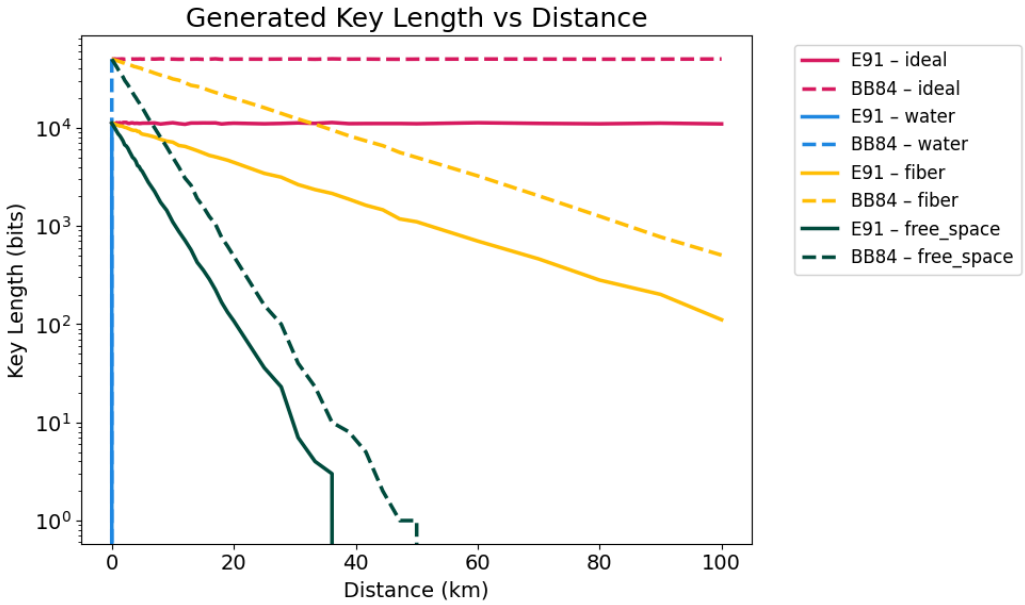

Figure 1: Key Length vs. Distance (Without Eavesdropping)

Under no eavesdropping, both protocols exhibit a monotonic decrease, as expected from channel attenuation and depolarization. Among the three channels tested, the fiber-optic link yielded the highest key length, while the underwater channel experienced the steepest decay, reaching zero bits beyond 300 meters. Furthermore, across all transmission media, BB84 consistently achieved longer key lengths than E91.

When partial (e = 0.5) and full eavesdropping were introduced, the key length trends remained unchanged for both BB84 and E91, which was expected since the raw key length is not a sensitive diagnostic of interceptions.

3.2. Secure and Sifted Key Rate

In this subsection, we present the results for the secure and sifted key rate across the different communication channels for each protocol separately. Figure 2 shows the secure and sifted key rate as a function of distance for the BB84 protocol, under ideal, fiber-optic (fiber), underwater (water), and free-space transmission. Figure 3 depicts the same metrics but for the E91 protocol.

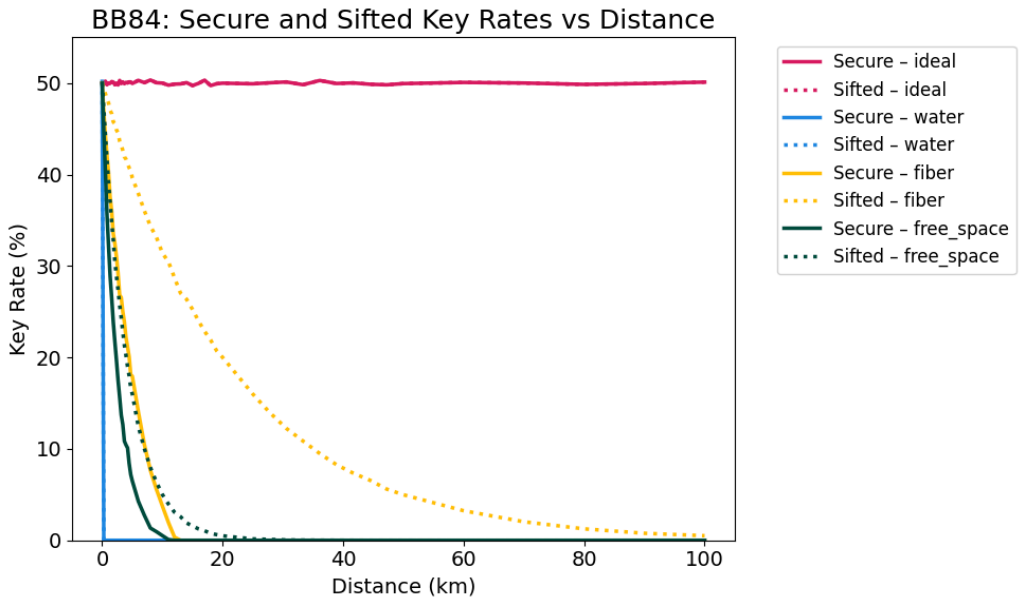

Figure 2: BB84 — Secure and Sifted Key Rate vs. Distance (Without Eavesdropping)

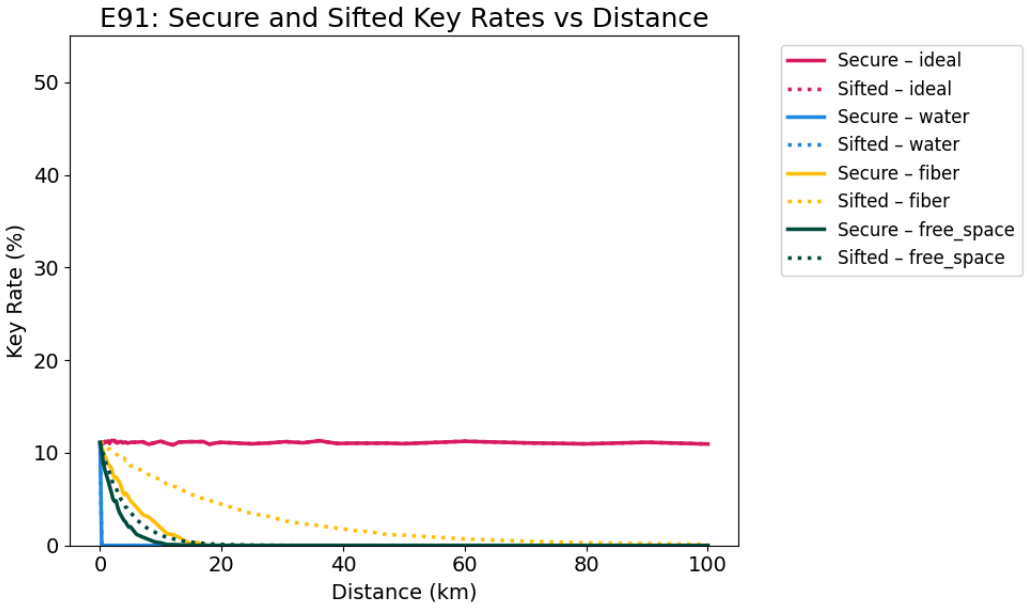

Figure 3: E91 — Secure and Sifted Key Rate vs. Distance (Without Eavesdropping)

For both protocols, the sifted and secure key rates display a decrease with distance, reflecting the effects of photon loss and depolarization in all imperfect channels. Comparatively, BB84 outperforms E91 in both sifted and secure key rates. At short distances, the difference between the two protocols is substantial. In fact, at 5 km, under a fiber-optic channel, BB84's secure key rate value is approximately 30%, while E91 presents a value lower than 5%. However, it is important to note that this performance gap is due to E91's reliance on coincident-pair detections, which are naturally less efficient than BB84's single-photon detections.

As a consistency check, the observed sifting fraction for BB84 at short distances was around 50%, closely matching the theoretical expectation for randomly chosen measurement bases. For E91, where basis reconciliation follows an entanglement-based procedure, the effective sifting fraction was inherently lower.

Under partial eavesdropping (e = 0.5), the sifted key rates were not impacted, as expected, since the metric does not reflect the effects of eavesdropping. On the other hand, security key rates suffered an extreme reduction, as seen in Figures 4–5. Specifically, this metric dropped to zero across all channels and distances. This occurs because, in the simulation, a key is assumed secure if the QBER remains below the 11% threshold established in Section 2. It is crucial to note, however, that this limit is not a strict boundary and may change in practical implementations.

In addition, a similar behavior was analysed under full eavesdropping (e = 1.0). Figures 6–7 depict, respectively, BB84 and E91's secure and sifted key rate in this condition.

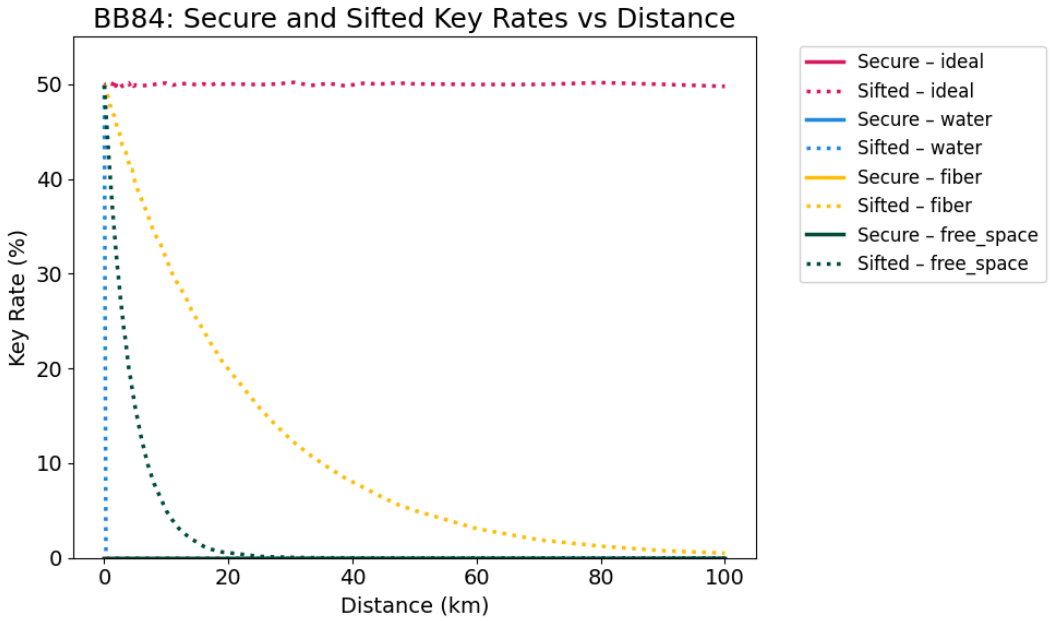

Figure 4: BB84— Secure and Sifted Key Rate vs. Distance (Partial Eavesdropping — e = 0.5)

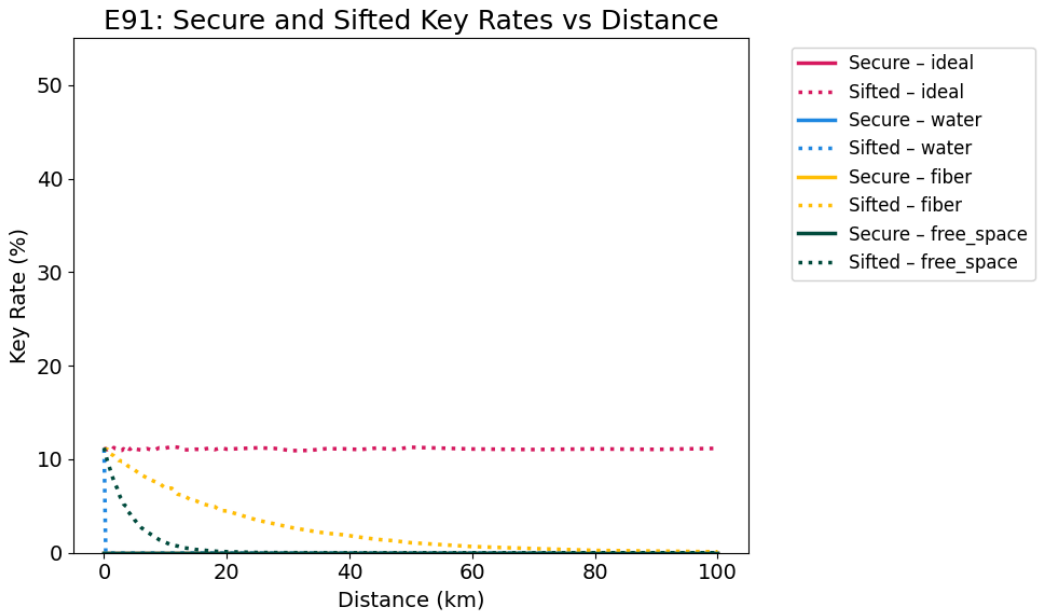

Figure 5: E91 — Secure and Sifted Key Rate vs. Distance (Partial Eavesdropping — e = 0.5)

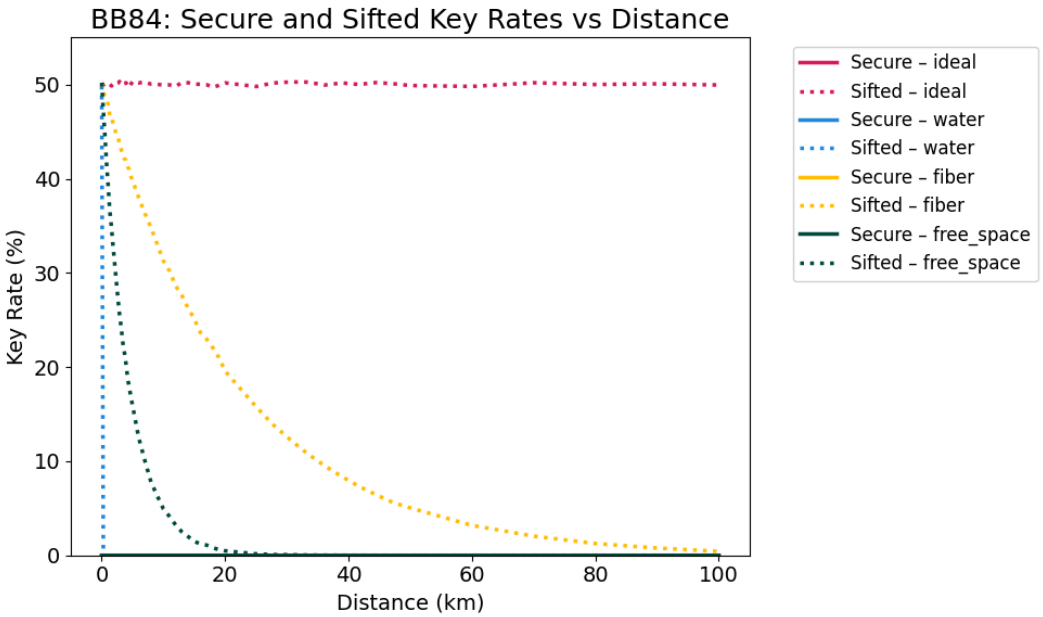

Figure 6: BB84 — Secure and Sifted Key Rate vs. Distance (Full Eavesdropping — e = 1.0)

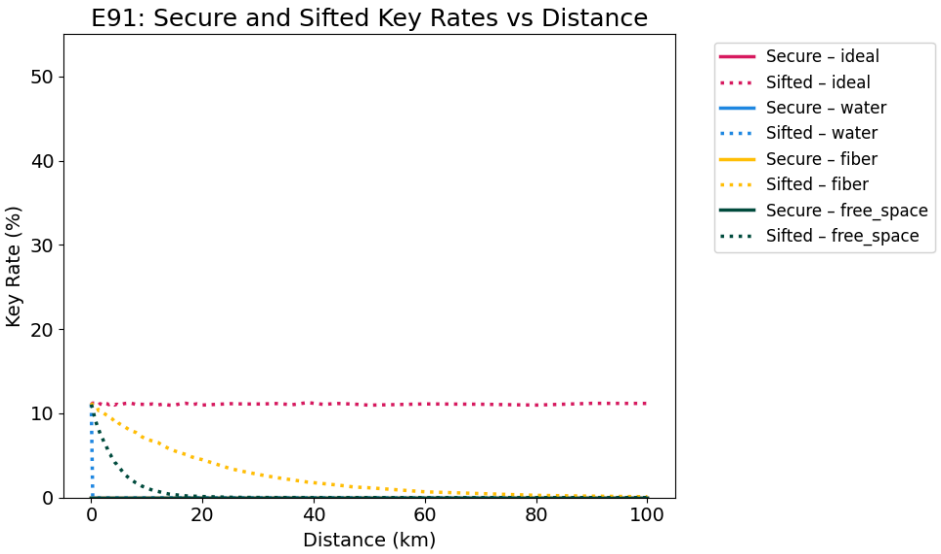

Figure 7: E91 — Secure and Sifted Key Rate vs. Distance (Full Eavesdropping — e = 1.0)

3.3. QBER and CHSH S-value

The simulation analysed the QBER of both protocols under different levels of eavesdropping and channel imperfections. Moreover, we also measure CHSH S-values specifically for E91. Firstly, Figures 8–9 depict simulations of both protocols under no attack.

In a scenario with no eavesdroppers, both protocols displayed low QBER values at short distances. While QBER climbed steeply to 100% for the underwater channel, due to its highly imperfect conditions, the metric increased slowly and approximately at the same rate for both free-space and fiber-optic transmission before the 20km mark. Overall, though, the fiber channel maintained the lowest QBER growth, never reaching 100% in contrast to the free-space link that reached this value between 40 and 60km. It is important to note that the QBER value of 0% reached by the BB84 protocol under a free-space channel is likely a statistical artifact and does not represent a realistic physical phenomenon. In fact, Figure 1 shows that, at the distance this event occurred, an extremely small number of photons were used to generate a key.

Comparatively, at short distances, both protocols displayed similar QBER values, indicating equivalent stability under minimal channel noise. However, as the distance increased, communication under the fiber-optic channel demonstrated higher values for BB84. For the free-space channel simulation, though, QBER reached its peak earlier for the E91 protocol.

In addition to QBER, the CHSH S-value for the E91 protocol was assessed, demonstrating a gradual decrease as transmission distance increased. At short distances and in the absence of attacks, S values consistently exceeded the classical limit. However, beyond 20km, S-values were limited for all channels, except for one occurrence when the metric reached the quantum maximum under a free-space link at approximately 40km. Nonetheless, this represents a statistical noise generated by the low amount of photons measured at this distance.

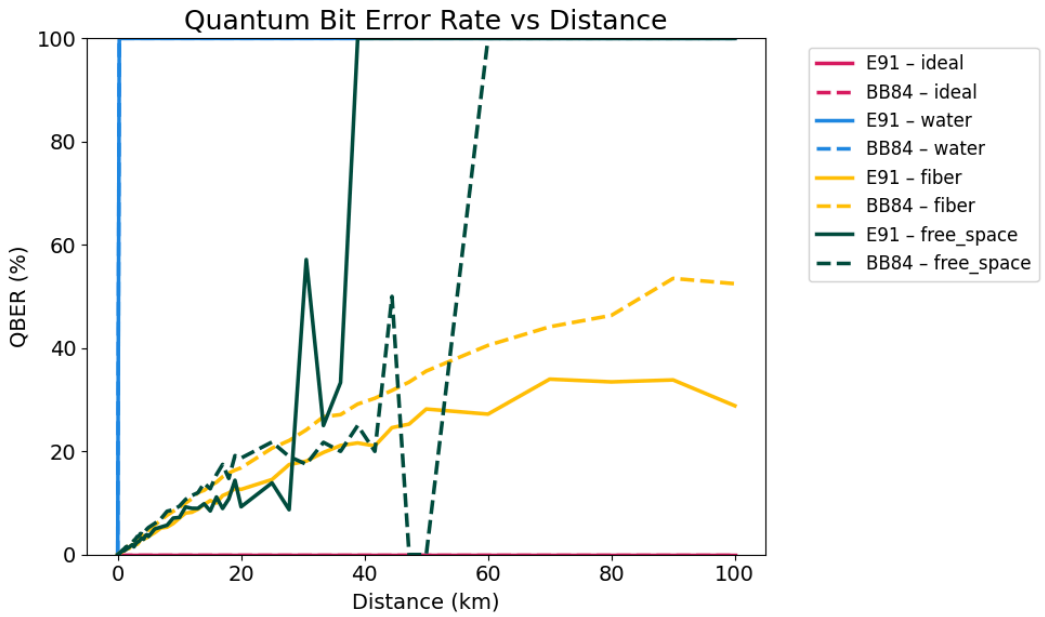

Figure 8: QBER vs. Distance (Without Eavesdropping)

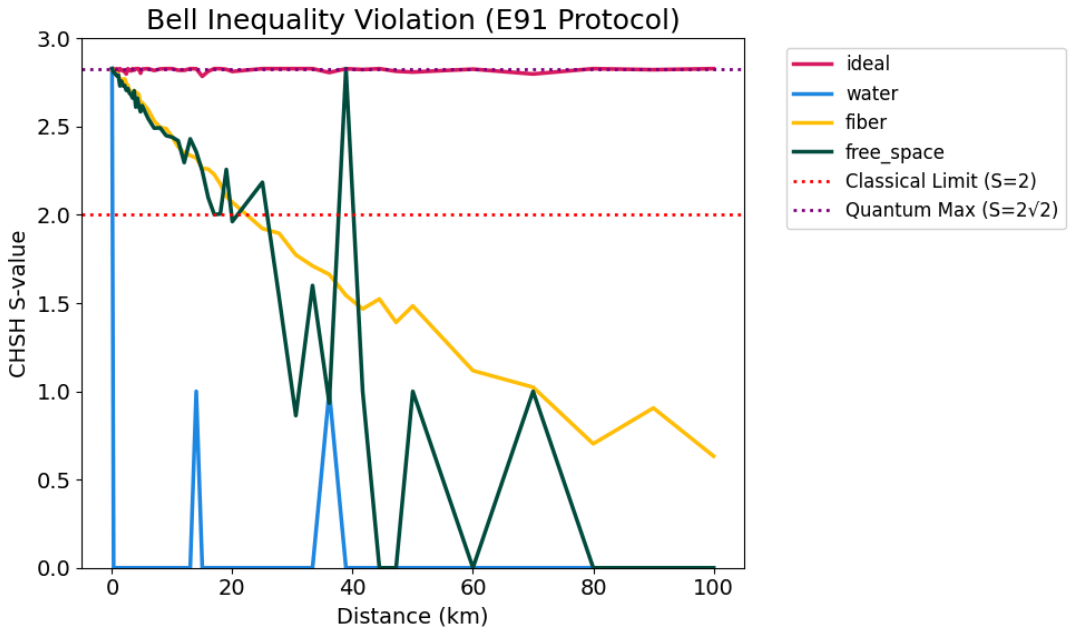

Figure 9: CHSH S-value vs. Distance (Without Eavesdropping)

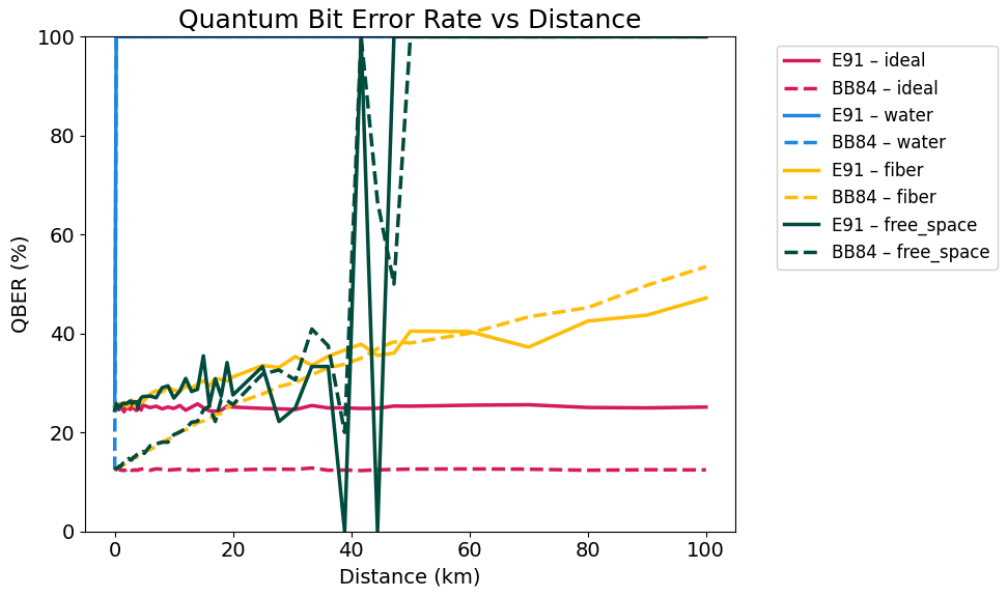

Figure 10: QBER vs. Distance (Partial Eavesdropping — e = 0.5)

Under partial eavesdropping, Figure 10 shows that QBER increased significantly for both protocols. In fact, QBER immediately surpassed the 11% security threshold assumed for all channels. This time, however, BB84 presented lower QBER values under short distances in comparison to E91. But as communication distances increased beyond 40km, the gap between the protocols reduced and maintained an approximately equivalent growth.

Again, the free-space channel simulation for the E91 protocol demonstrated QBER values of 0% that represent statistical anomalies due to the low count of measured photons.

For the CHSH S-values, our simulation demonstrated in Figure 11 that the eavesdropper interceptions dismantled quantum correlations. In fact, for all channels and distances experimented with, this metric never surpassed the classical threshold.

When the eavesdropper activity was increased to full interception (e = 1.0), the observed effects intensified across all metrics. As shown in Figure 12, QBER values exceeded 25% even at short communication distances. Interestingly, BB84 maintained noticeably lower QBER values than the E91 protocol up to approximately 80km, beyond which both protocols converged toward a QBER of 50%. Moreover, the free-space channel simulation continued to display anomalous results.

In contrast to the partial eavesdropping scenario, the CHSH S-values under full attack showed a complete loss of correlations. As illustrated in Figure 13, all recorded values remained below 0.25, with the exception of a few statistical artifacts previously discussed.

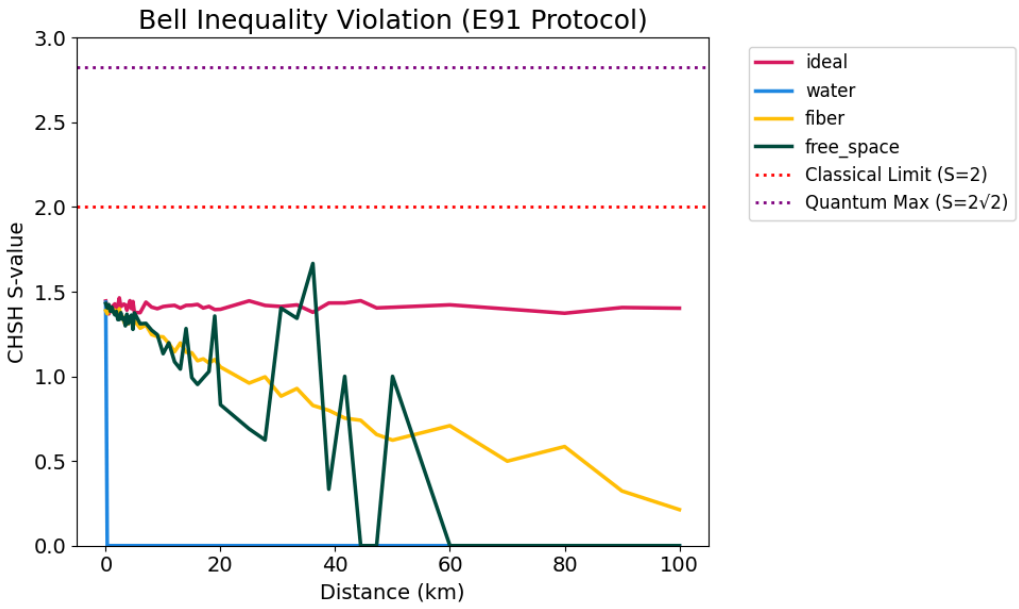

Figure 11: CHSH S-value vs. Distance (Partial Eavesdropping — e = 0.5)

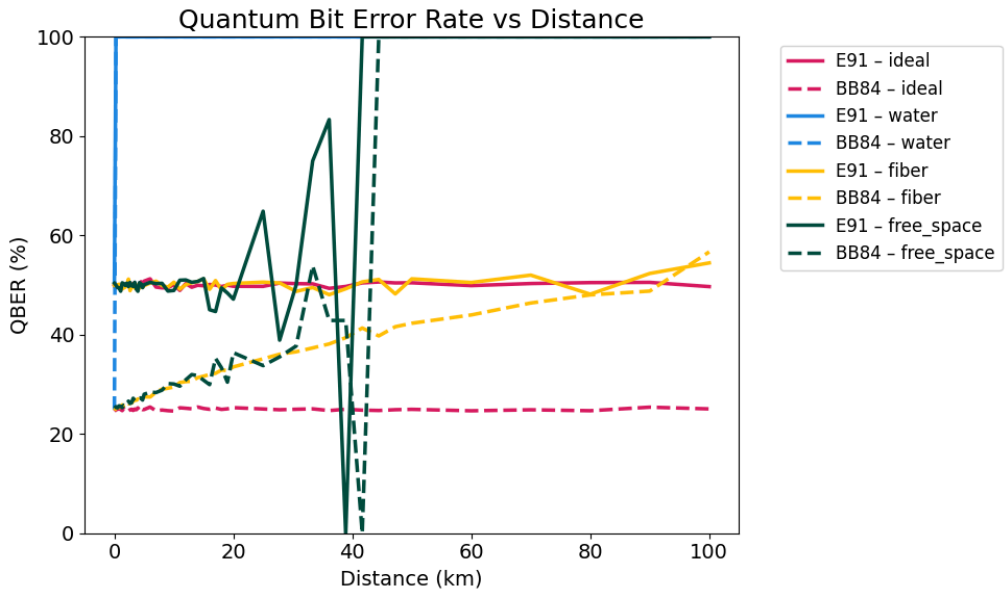

Figure 12: QBER vs. Distance (Full Eavesdropping — e = 1.0)

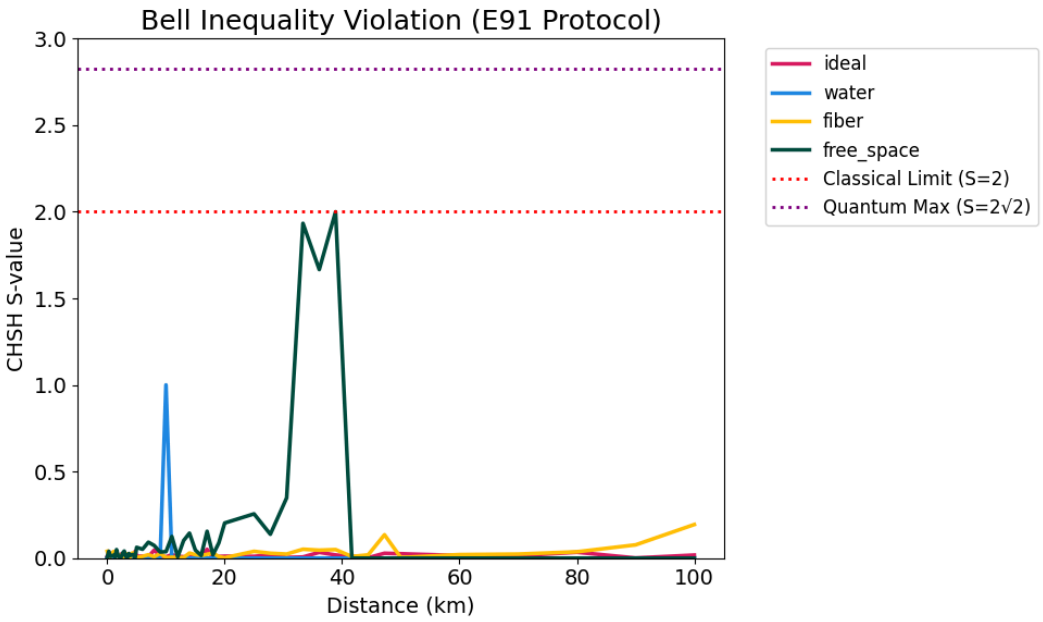

Figure 13: CHSH S-value vs. Distance (Full Eavesdropping — e = 1.0)

3.4. Discussion

In the absence of eavesdropping, BB84 consistently demonstrated greater performance in terms of efficiency metrics over E91. Especially at shorter and medium communication distances, BB84 maintained higher key length, sifted key rate, and secure key rate values, proving to be more efficient. However, under severe levels of photon loss and depolarization, both protocols struggled to sustain high secure key rates, rendering communication impossible in some cases.

From a security standpoint, BB84 proved less susceptible to drastic QBER escalation under eavesdropping attacks. For E91, an additional metric — CHSH S values — served as an indicator of entanglement quality and the presence of non-classical correlations. In our simulations, S-values fell below the classical threshold even without an eavesdropper. This result does not indicate a flaw in the E91 protocol itself, but rather reflects the extreme sensitivity of Bell-inequality measurements to harsh conditions. In such cases, environmental depolarization and photon loss destroyed entanglement to the point where Bell violations could no longer be observed. In other words, channel noise, not the protocol itself, limited secure entanglement-based QKD under those physical conditions.

While our simulations provide comparative insights into BB84 and E91 under different physical channels, several limitations constrain the direct generalization of these findings. The model does not include detector dark counts, basis misalignment, timing jitter, and other realistic effects, all of which can meaningfully impact the QBER and secure key rate in practical applications. Likewise, decoy-state refinements for BB84 or entanglement-purification techniques for E91, which are known to substantially improve performance under low-signal conditions, were not incorporated. Moreover, our environmental assumptions also rely on fixed turbidity, wavelength, and scattering parameters that can vary widely in

real-world deployments. These simplifications were intentional to isolate the comparative behaviour of the protocols, but they limit the applicability of the absolute values obtained.

Thus, our hypothesis that BB84 would outperform E91 in efficiency across all channels tested was proven correct. Furthermore, our prediction that underwater quantum communication was not viable for practical implementation was only partially confirmed. In our simulations, communication was feasible at short distances, approximately below 200 meters, under the specific conditions modeled for our underwater channel. It is important to note that this result is highly dependent on environmental and optical parameters, such as water type, turbidity, wavelength, and polarization effects. Beyond this distance, depolarization and photon loss significantly degraded photon transmission, making key generation impractical in the scenario simulated. Therefore, while our results indicate short-range feasibility, the precise distance limit should not be interpreted as universal but as representative of the modeled conditions.

4. Conclusion

Quantum Key Distribution (QKD) represents the next step toward secure communication. Thus, practical implementation needs to take place in the near future to protect secret information from the threats that quantum computers' algorithms pose. This study analyzed the use of the two most discussed QKD protocols under different realistic conditions determined by underwater, fiber optic, and free-space channels. Through a comparison of efficiency metrics, such as key length, sifted key rate, and secure key rate, we determined that BB84 outperformed E91 across all channels experimented with.

Despite the result, it is crucial to recognize that E91 has theoretical advantages not captured by the performance metrics analyzed here. While our analysis is strictly limited to a simplified intercept–resend scenario, the E91 protocol forms a conceptual foundation for Device-Independent Quantum Key Distribution (DI-QKD), an advanced paradigm that aims to provide security without having to trust the internal workings of the communication hardware. While BB84's robustness makes it more suitable for near-term implementations, progress toward practical E91-like systems depends on improving how entanglement is distributed and preserved in realistic environments. Continued research into enhancing entanglement generation rates, mitigating environmental decoherence, and developing more resilient distribution techniques remains essential for enabling next-generation quantum networks.

These insights provide valuable information for future research and practical implementations to propose novel tools to mitigate the impact of noise and loss on quantum communication channels and to choose the most appropriate protocol for each specific scenario. It is important to point out that these improvements are already taking place, as many research papers propose the use of various techniques such as quantum repeaters (Briegel, Dür, Cirac, & Zoller, 1998) to extend communication range, adaptive optics to correct for atmospheric turbulence in real time in free-space links (Martínez, Rodríguez-Ramos, & Sodnik, 2018), and advanced classical error correction codes designed for the low-signal regimes typical of QKD.

Future work should expand the models to incorporate realistic hardware imperfections, dynamic environment conditions, and advanced protocol enhancements. Additionally, validating the simulations with experimental data from underwater, fiber, and free-space tests would provide a stronger foundation for assessing the practical viability of each protocol. Such developments will help bridge the gap between theoretical design and deployable quantum communication systems, ultimately guiding the choice of protocol for different operational real-world environments.

5. References

Agrawal, G. P. (2012). *Fiber-optic communication systems* (4th ed.). John Wiley & Sons.

Aspelmeyer, M., Jennewein, T., Pfennigbauer, M., Leeb, W. R., & Zeilinger, A. (2003). Long-distance quantum communication with entangled photons using satellites. *IEEE Journal of Selected Topics in Quantum Electronics*, 9(6), 1541–1551. https://doi.org/10.1109/JSTQE.2003.820918

Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21), 3121–3124. https://doi.org/10.1103/PhysRevLett.68.3121

Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560, 7–11. https://doi.org/10.1016/j.tcs.2014.05.025

Bernstein, D. J., Heninger, N., Lou, P., & Valenta, L. (2017). Post-quantum RSA. In T. Takagi & T. Peyrin (Eds.), *Advances in cryptology – ASIACRYPT 2017* (pp. 311–337). Springer. https://doi.org/10.1007/978-3-319-59879-6_18

Bhatia, V., & Ramkumar, K. R. (2020). An efficient quantum computing technique for cracking RSA using Shor's algorithm. In *2020 IEEE 5th International Conference on Computing Communication and Automation* (ICCCA) (pp. 89–94). IEEE. https://doi.org/10.1109/ICCCA49541.2020.9250806

Briegel, H.-J., Dür, W., Cirac, J. I., & Zoller, P. (1998). Quantum repeaters: The role of imperfect local operations in quantum communication. *Physical Review Letters*, 81(26), 5932–5935. https://doi.org/10.1103/PhysRevLett.81.5932

Buttler, W. T., Hughes, R. J., Kwiat, P. G., Lamoreaux, S. K., Luther, G. G., Morgan, G. L., Nordholt, J. E., Peterson, C. G., & Simmons, C. M. (1998). Practical free-space quantum key distribution over 1 km. *Physical Review Letters*, 81(15), 3283–3286. https://doi.org/10.1103/PhysRevLett.81.3283

Clauser, J. F., Horne, M. A., Shimony, A., & Holt, R. A. (1969). Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15), 880–884. https://doi.org/10.1103/PhysRevLett.23.880

Czerwinski, A., & Czerwinska, K. (2022). Statistical analysis of the photon loss in fiber-optic communication. *Photonics*, 9(8), Article 568. https://doi.org/10.3390/photonics9080568

Díaz, F., & Lenin, J. (2014). *Geração de emaranhamento de polarização entre pares de fótons no regime de fentossegundos* [Master's thesis, Universidade Federal de Pernambuco]. Repositório Digital da UFPE. https://repositorio.ufpe.br/handle/123456789/18296

Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6), 661–663. https://doi.org/10.1103/PhysRevLett.67.661

Maloo, S. (n.d.). *Quantum cryptography and communication: Protocols, limitations, and solutions* [Unpublished manuscript].

Martínez, N., Rodríguez-Ramos, L. F., & Sodnik, Z. (2018). Toward the uplink correction: Application of adaptive optics

techniques on free-space optical communications through the atmosphere. *Optical Engineering*, 57(7), Article 076106. https://doi.org/10.1117/1.OE.57.7.076106

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information* (10th anniversary ed.). Cambridge University Press.

Scarani, V., Acín, A., Ribordy, G., & Gisin, N. (2004). Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92(5), Article 057901. https://doi.org/10.1103/PhysRevLett.92.057901

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134). IEEE. https://doi.org/10.1109/SFCS.1994.365700

Shor, P. W., & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2), 441–444. https://doi.org/10.1103/PhysRevLett.85.441

Teich, M. C., & Saleh, B. E. A. (2007). *Fundamentals of photonics* (2nd ed.). Wiley.

Xu, J.-S., Xu, X.-Y., Li, C.-F., Zhang, C.-J., Zou, X.-B., & Guo, G.-C. (2010). Experimental investigation of classical and quantum correlations under decoherence. *Nature Communications*, 1(1), Article 7. https://doi.org/10.1038/ncomms1005

Yin, J., Cao, Y., Li, Y.-H., Liao, S.-K., Zhang, L., Ren, J.-G., Cai, W.-Q., Liu, W.-Y., Li, B., Dai, H., Li, G.-B., Lu, Q.-M., Gong, Y.-H., Xu, Y., Li, S.-L., Li, F.-Z., Yin, Y.-Y., Jiang, Z.-Q., Li, M., … Pan, J.-W. (2017). Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343), 1140–1144. https://doi.org/10.1126/science.aan3211

Zhang, X., Zhang, H., Chua, R. M., Eng, J., Meunier, M., Grieve, J. A., Gao, W.-B., & Ling, A. (2025). Polarization-encoded quantum key distribution with a room-temperature telecom single-photon emitter. *National Science Review*, 12(8), Article nwaf147. https://doi.org/10.1093/nsr/nwaf147

Zhao, S., Li, W., Shen, Y., Yu, Y., Han, X., Zeng, H., Cai, M., Qian, T., Wang, S., Wang, Z., Xiao, Y., & Gu, Y. (2019). Experimental investigation of quantum key distribution over a water channel. *Applied Optics*, 58(14), 3902–3907. https://doi.org/10.1364/AO.58.003902

6. Appendices

Appendix A - Minimal Code

The minimal simulation code used to reproduce the results presented in this paper is available at: Quantum Key Distribution Simulation (Minimal Code).ipynb

Appendix B - Protocols

This appendix provides tables for both the BB84 and the E91 protocols.

Table B1: Application of Pauli errors for different photon polarizations

X Error		**Y Error**		**Z Error**	
Initial Polarization	Final Polarization	Initial Polarization	Final Polarization	Initial Polarization	Final Polarization
0	π/2 (90°)	0	π/2 (90°)	0	0
π/2 (90°)	0	π/2 (90°)	0	π/2 (90°)	π/2 (90°)
π/4 (45°)	π/4 (45°)	π/4 (45°)	3π/4 (135°)	π/4 (45°)	3π/4 (135°)
3π/4 (135°)	3π/4 (135°)	3π/4 (135°)	π/4 (45°)	3π/4 (135°)	π/4 (45°)

Note: X applies a bit-flip to photons polarized in the rectilinear basis. Z also applies a bit-flip, but only for photons polarized in the diagonal basis. Y applies a bit-flip for both polarization bases.

Table B2: BB84 10 Bits Noise- and Loss-free Environment Example Without Eavesdropping (Maloo, n.d.).

Bits	**b0**	**b1**	**b2**	**b3**	**b4**	**b5**	**b6**	**b7**	**b8**	**b9**
Alice's Bits	0	**1**	0	**0**	**1**	1	1	1	**0**	**0**
Angle of Alice's photons	0	π/2	π/4	π/4	π/2	3π/4	π/2	3π/4	π/4	0
Correct Detector	Z	Z	X	X	Z	X	Z	X	X	Z
Bob's Detector	X	Z	Z	X	Z	Z	X	Z	X	Z
P(0)	0.5	0.0	0.5	1.0	0.0	0.5	0.5	0.5	1.0	1.0
P(1)	0.5	1.0	0.5	0.0	1.0	0.5	0.5	0.5	0.0	0.0
Results after discarding the incorrect basis		**1**		**0**	**1**				**0**	**0**

Table B3: BB84 10 Bits Noise- and Loss-free Environment Example With Eavesdropping (e = 1.0) (Maloo, n.d.).

Bits	b0	b1	b2	b3	b4	b5	b6	b7	b8	b9
Alice's Bits	0	**1**	0	**0**	**1**	1	1	1	**0**	**0**
Angle of Alice's photons	0	π/2	π/4	π/4	π/2	3π/4	π/2	3π/4	π/4	0
Correct Detector	Z	Z	X	X	Z	X	Z	X	X	Z
Eve's Detector	Z	Z	X	Z	Z	Z	X	X	Z	Z
Eve's P(0)	1.0	0.0	1.0	0.5	0.0	0.5	0.5	0.0	0.5	1.0
Eve's P(1)	0.0	1.0	0.0	0.5	1.0	0.5	0.5	1.0	0.5	0.0
Bob's Detector	X	Z	Z	X	Z	Z	X	Z	X	Z
Bob's P(0)	0.5	0.0	0.5	0.5	0.0	0.5	0.5	0.5	0.5	1.0
Bob's P(1)	0.5	1.0	0.5	0.5	1.0	0.5	0.5	0.5	0.5	0.0
Results after discarding incorrect basis		**1**		**0 or 1**	**1**				**0 or 1**	**0**

Notice that in Table B1 — when no eavesdropper was present — all matching bases correspond to matching bits. However, in Table B2, after introducing eavesdropping, the bits in positions b4 and b8 (which share the same bases) are corrupted.

Table B4: Equation 15 applied to various measurement angles combinations

Bits	θA (Alice)	θB (Bob)	θA − θB	− cos[2(θA − θB)]	*Psame* (Equation 15)
b1	π/2	π/2	0	-1	0.00 (anti-correlated)
b2	0	π/8	-π/8	-(√2)/2	0.14
b3	π/4	-π/8	3π/8	(√2)/2	0.85

Appendix C – Performance Metrics and Full Definitions

This appendix provides detailed expressions and derivations for the performance metrics used in the simulations.

C.1 Quantum Bit Error Rate (QBER)

The QBER is defined as

$$\text{QBER} = \frac{1}{N}\sum_{i=1}^{N}\delta(a_i \neq b_i), \tag{16}$$

where N is the total number of bits in the sifted key; *ai*, *bi* are the i-th bit from Alice and Bob, respectively; $\delta(a_i \neq b_i)$ is a function that returns 1 if *ai*≠*bi* and 0 otherwise.

C.2 Secure Key Rate

The secure key rate calculation is given by (Shor & Preskill, 2000):

$$R_{secure} = R_{sifted} \times max(0, 1 - 2H_2(QBER)), \tag{17}$$

where Rsifted is the sifted rate, and *H2* is the binary entropy function:

$$H_2(p) = -p\ log_2\ p - (1-p)log_2(1-p). \tag{18}$$

C.3 CHSH S-value (E91)

By computing four correlation coefficients — described by Equation (12) — for which Alice and Bob used different measurement angles, the CHSH S-Value (Clauser, Horne, Shimony, & Holt, 1969) is obtained:

$$S = E(\theta_{A1}, \theta_{B1})\ -\ E(\theta_{A1}, \theta_{B2}) + E(\theta_{A2}, \theta_{B1}) - E(\theta_{A2}, \theta_{B2}), \tag{19}$$

where θAi and θBi correspond to Alice and Bob's measurement angles of index *i*. According to Bell's theorem (Nielsen & Chuang, 2010), any classical system satisfies |S| <= 2. However, quantum mechanics requires that |S| <= $2\sqrt{2}$. This means that, in practice, when the value of |S| is substantially greater than the classical threshold, Alice and Bob can determine that the particles they measured were entangled and not directly or indirectly "disturbed" (Ekert, 1991).

Acknowledgements

We wish to thank Dr. Eric Sakk for monitoring and guiding this work. In fact, this paper would not exist without his key insights on quantum communication and key distribution. Moreover, we acknowledge Ahmed Shaaban and Indigo's research program for providing access to valuable studies mentioned in this article, namely Ekert's E91 paper. We are also thankful for the feedback given by all peers who participated in the IRIS Computer Science sessions. Furthermore, we are grateful to the three anonymous referees who carefully reviewed this paper and provided insightful comments that greatly improved its clarity and rigor. All the support and inspiration were fundamental for both the writing and the empirical process. Therefore, we are extremely grateful to everyone involved.

Author Biography

Eduardo Lougon Sampaio Lopes is a young Brazilian student and aspiring computer scientist and researcher from Rio de Janeiro. As a high-school student at Instituto GayLussac, his work spans artificial intelligence, computer vision, and reinforcement learning, as well as software development in both web and game design. In 2023, Eduardo led and presented a computer vision-based glasses project designed to assist people with visual impairments in national scientific competitions, including FECTI. Furthermore, he was first introduced to computer science research in 2022, when he wrote and presented an article on how AI can save lives. He is also the founder of an online AI-powered platform—O(lympiads)—that helps students and professionals prepare for informatics olympiads and code interviews. Interested in exploring new backgrounds and interdisciplinary subjects, he is currently motivated to learn about cybersecurity and quantum key distribution. Eduardo's long-term goal is to study computer science at the university level and to contribute to advancements in emerging computer systems that benefit society.

Mentor Contribution Statement

Dr. Erik Sakk supervised the development of this paper by providing conceptual guidance, feedback on methodological choices, and suggesting research materials. From the earliest stages of the work, he guided me in identifying a clear research direction, helping to refine the scope of the study and articulate the questions that shaped this manuscript. Moreover, Dr. Sakk offered key explanations that clarified the physics underlying quantum communication. His work was essential to building a rigorous theoretical framework before implementing any simulations. Although he did not participate in coding or the generation of results, he played a crucial role in strengthening the methodological foundation of the paper. Lastly, throughout the writing process, he reviewed multiple drafts and provided constructive feedback on structure and technical accuracy while also motivating the author.