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

Abstract

Quantum key distribution (QKD) has emerged in recent decades as a hopeful 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 optic 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, Quantum Communication, Communication Protocols, BB84, E91, Realistic Simulation.

I - 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, since the development of quantum computers and algorithms, the security of many traditional cryptographic methods has been fundamentally threatened. 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 quantum mechanics' uncertainty principle and no-cloning theorem (Nielsen & Chuang, 2010). By using two conjugated bases - typically the rectilinear and diagonal bases - Alice and Bob can send polarized photons representing binary values (0 and 1). When both communication parties select the same bases, and assuming a noiseless channel, Bob will measure the correct bit. But, if Alice sends a photon encoded in the rectilinear basis and Bob chooses the diagonal, quantum uncertainty dictates a 50% probability of obtaining the correct value. Then, using a classical insecure channel, Alice and Bob can go through a process called sifting and generate shared secret keys to later encrypt and decrypt information securely. It is essential to note that, because a photon's state collapses upon measurement with the wrong basis, the presence of an eavesdropper is highly detectable (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. This way, both parties can randomly select bases and perform measurements on their respective photons. Since these are entangled, the results are strongly correlated - even when different bases are chosen. Then, to check the integrity of the key exchange, they can compare a subset of their measurements' results to check if it violates Bell's inequalities. With this analysis, Alice and Bob can determine if there was an eavesdropper, because a successful violation confirms the entanglement of the photons. Finally, if communication was 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. Still, we predict that underwater channels are not viable for practical 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 on 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 II sketches the methodology for the performance analysis of BB84 and E91 protocols. In section III, the results' metrics such as QBER, secure and sifting key generation rate and key length are presented and discussed. We conclude in section IV.

II - 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. Due to the absence of real quantum hardware (such as single-photon sources and detectors), 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 **(a)** presents the main environmental factors - photon loss and depolarization - that affect photon transmission through different channels and explains how these were modeled computationally. Subsections **(b)** and **(c)** describe the implementation of the BB84 and E91 protocols, respectively, including how eavesdropping was simulated. Lastly, subsection **(d)** 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..

a) Channel Modeling: Photon Loss and Depolarization

In real-world quantum communication, photons travelling 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 law (Teich & Saleh, 2007) can be used:

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

where $I(d)$ denotes the intensity of light after propagating a distance d through an absorbing or scattering medium, I_0 represents the initial power and α the attenuation coefficient (Czerwinski & Czerwinska, 2022). Then, to get the fraction of photons that survive transmission, both sides are divided by I_0:

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

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

In order to simulate realistic conditions, typical attenuation coefficients of all channel communication conditions were used. These are shown in Table 1.

Table 1 : Attenuation Coefficient (α), measured in dB per kilometers, 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:

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

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:

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

where λ is defined as the depolarization length, with units dependent on the distance *d*. For this simulation typical values of λ for each channel (underwater, fiber optic and free-space) were used. These are shown in Table 2.

Table 2 : Depolarization length (λ), measured 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)
Free-space	63 (Buttler et al., 1998)

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

b) 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 has 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,

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

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

Then, these photons travel through noisy and lossy channels before reaching Bob's randomly chosen polarization bases and single-photon detectors. After, 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 are 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 $\{ai\}$ with $ai \in \{0, 1\}$ 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 BB84 protocol

Polarization	**Basis**	**Bit Representation**
0	Z (Rectilinear)	0

π/2 (90°)	Z (Rectilinear)	1
π/4 (45°)	X (Diagonal)	0
3π/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 as described in Table 4, if k is smaller than the depolarization probability.

Table 4. 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.*

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 ϕi to perform his measurement. For example, if Bob detects a photon polarized in the rectilinear basis (horizontal $|H\rangle$ (0) or vertical $|V\rangle$ (π/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):

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

The probabilities of obtaining bit 0 or 1 when measured in the Z (rectilinear) or X (diagonal) basis, for each of the four polarization states of a photon, are shown in Table 5.

Table 5. Measurement outcome probabilities for BB84 states in the Z and X bases.

Prepared State	**Z Basis: *P*(0), *P*(1)**	**X Basis: *P*(0), *P*(1)**
|H⟩ (0)	1.0, 0.0	0.5, 0.5
|V⟩ (π/2)	0.0, 1.0	0.5, 0.5
|A⟩ (π/4)	0.5, 0.5	1.0, 0.0
|D⟩ (3π/4)	0.5, 0.5	0.0, 1.0

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 with 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. It is important to note that if the error rate is over a certain threshold - 11% (Shor & Preskill, 2000) - the key is not considered secure and must be discarded rather than used for encryption.

Building on the error-correction stage, eavesdropping is modeled as an intercept-resend attack. In this sense, it is introduced in the communication channel, after all loss and noise is applied, an observer, Eve. 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}, and a new replacement photon is sent to Bob prepared in the state observed. This way, when Eve's basis matches Alice's, her intervention goes undetected; in contrast, whenever she measures in the wrong basis, she introduces an error half of the time. Table 6 and Table 7 show an example of the protocol without and with eavesdropping, respectively.

Table 6. 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 incorrect basis		**1**		**0**	**1**				**0**	**0**

Table 7. 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	X	Z	Z	X	Z	Z	X	Z	X	Z

Detector										
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 6 - when no eavesdropper was present - all matching bases correspond to matching bits. However, in Table 7, after introducing eavesdropping, the bits in positions b4 and b8 (which share the same bases) are corrupted. 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.

c) 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 an entangled pair. 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.

Bell's inequalities (Nielsen & Chuang, 2010) are mathematical expressions that any hidden variable theory - deterministic models that seek to explain that the probabilistic nature of quantum mechanics arises from the existence of hidden unobservable variables that pre-determine measurement outcomes - must satisfy. Quantum mechanics, however, predicts correlations that exceed these classical bounds, providing an interesting functionality. By testing for violations of a specific Bell inequality (CHSH inequality (Clauser, Horne, Shimony, & Holt, 1969)), Alice and Bob can detect the presence of an eavesdropper. When the quantum channel is intercepted, the entanglement of the particle is disturbed, reducing observed correlations below the quantum threshold.

Similarly 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 individual, Victor, equally distant to Alice and Bob sends, to both parties, photons prepared in the maximally entangled singlet state

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

Next, Alice and Bob independently select one of three measurement bases (angles) randomly, with uniform probabilities. Table 8 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 is reserved for key generation. In this simulation, the basis that corresponds to a measurement angle of π/2 is used to generate the final key.

Table 8. Possible Measurement Bases for Alice and Bob

Basis Index	**Alice's bases**	**Bob's bases**
0	π/2	π/2
1	0	π/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 $(k) \in \{0, 1\}$. On the other hand, when the depolarization probability is smaller 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 ($|0\rangle$) or -1 ($|1\rangle$) - 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

$$P(b = -a \mid \theta_A = \theta_B) = 1, \quad (9)$$

where a,b and θA, θB represent Alice and Bob's measurement outcomes and selected angles, respectively. It is also important to mention that the singlet state $|\Psi\rangle$ defines a 50% probability of measuring each outcome for both parties, because the probability of Alice measuring +1 is given by

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

and after this measurement, $|\Psi\rangle$ collapses to just

$$|\Psi^-\rangle = |01\rangle, \quad (11)$$

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):

$$E(\theta_A, \theta_B) = P_{++} + P_{--} - P_{+-} - P_{-+}, \quad (12)$$

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:

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

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

$$E(\theta_A, \theta_B) = -\cos[2(\theta_A - \theta_B)], \quad (14)$$

finally giving the expression in the form:

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

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. Table 9 shows more examples.

Table 9. Equation (15) applied to various measurement angles combinations

Bits	θA (Alice)	θB (Bob)	θA − θB	− cos[2(θA − θB)]	P_{same} **(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

In sum, step three of the simulation starts with Alice measuring the value $a \in \{+1, -1\}$ 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 $(k) \in \{0, 1\}$. If P_{same} is

smaller, 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 behaviour was preserved, ensuring the channel was not disturbed.

Lastly, eavesdropping is implemented for the E91 protocol in the simulation as an intercept-resend attack. For each transmitted photon, Eve has a probability e of intercepting it (the eavesdropper strength). Upon interception, Eve measures on a random basis and resends a random state, completely destroying entanglement. Therefore, when Alice and Bob measure their photons, the results are not correlated.

d) 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 offer 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.

Quantum Bit Error Rate (QBER) is one of the most critical metrics of quantum key distribution protocols. By measuring the fraction of bits of the sifted key that differ between Alice and Bob, the communication's security can be evaluated. Therefore, it is given by

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

where N is the total number of bits in the sifted key; a_i, b_i are the i-th bit from Alice and Bob, respectively; $\delta(a_i \neq b_i)$ is a function that returns 1 if $a_i \neq b_i$ and 0 otherwise. While a low QBER indicates stronger security guarantees, a QBER above a certain threshold points to the presence of malicious interference or excessive noise. In the BB84 protocol, for instance, a measurement of this metric below 11% (Shor & Preskill, 2000) is considered secure. However, since QBER increases drastically with depolarization, it becomes harder to determine whether there was or not an eavesdropper intercepting the channel as the probability of depolarization increases with distance.

The sifted key rate refers to the proportion of raw key bits that remain after Alice and Bob discard all bits for which they used incompatible measurement bases. Thus, it

is an important metric to evaluate the effectiveness of a protocol: a higher sifted rate means more usable bits per transmission - which makes it more practical for real-world implementations.

In contrast, the secure key rate represents the portion of the sifted key that can be securely used. Since some of the bits in the sifted key may be compromised by noise, losses and potential eavesdropping, it is important to discard them to prevent leaking valuable information. Therefore, the secure key rate reflects the protocol's real-world viability by considering just the net amount of safe key material. Its calculation is given by (Shor & Preskill, 2000):

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

where R_{sifted} is the sifted rate and H_2 is a binary entropy function:

$$H_2(p) = -p\, log_2\, p - (1-p) log_2(1-p). \quad (18)$$

The key length refers to the total number of secure bits generated after all post-processing steps. Similarly to the sifted key rate metric, the key length is particularly relevant for assessing the practical usability of the protocol. Since most cryptographic applications require large key lengths to be effective, the protocol's ability to generate long, secure bit strings is a crucial factor for in-the-field quantum communication.

Lastly, the CHSH (Clauser–Horne–Shimony–Holt) S-Value (Clauser, Horne, Shimony, & Holt, 1969) is used to evaluate the security of quantum communication based on the E91 protocol exclusively. It quantifies the strength of the correlations between Alice and Bob's outcomes. By computing four correlation coefficients - described by Equation (12) - for which Alice and Bob used different measurement angles, the S-Value is obtained:

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

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√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).

III - Results

For both protocols, the transmission of 100000 particles 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 10 presents these intervals and their respective amount of sampling points.

Table 10. 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

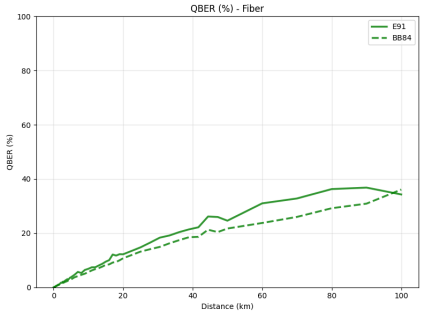
This section is divided into four subsections. Each of the first three subsections is dedicated to describe the results of both protocols under each simulated quantum channel. Subsection **(a)**, **(b)** and **(c)** present, respectively, the results of fiber optic, underwater, and free-space channels. Lastly, subsection **(d)** discusses the results obtained and compares the performance of both protocols.

a) Fiber Optic Channel

Firstly, both protocols were simulated without eavesdropping. Our results show that, expectedly, the efficiency of both protocols decayed slowly as the distance of communication increased.

Specifically, the BB84 protocol, at a distance of approximately 20 km, reached the security threshold of 11% QBER (Shor & Preskill, 2000), meaning that the secure key rate dropped to zero beyond this point. At a distance of 5 km, BB84 has a QBER value of 2.9% - which is more than 20% lower than E91's value (3.7%). As the distance increases, BB84 continues to have a QBER slightly lower than E91's. For instance, at 50 km, there was a difference of 2.9 between both protocols. Interestingly, however, at 100 km the simulation showed a QBER value of 34.3% for E91 and of 36.1% for BB84. Figure 1 illustrates these results.

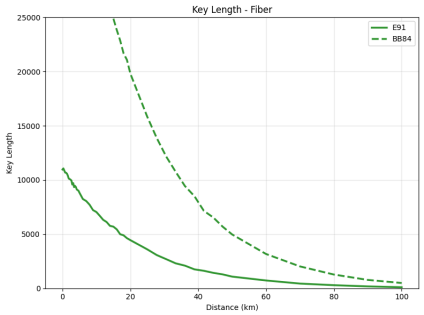
Figure 1. QBER vs. Distance in Fiber Optic Channel Without Eavesdropping



Concerning key lengths, both protocols exhibit a downward trend, approaching 0 at around 100 km. BB84's key length values start close to 50000 bits and, as distance increases, this value steeply declines until a distance of 40 km - where it begins slowly

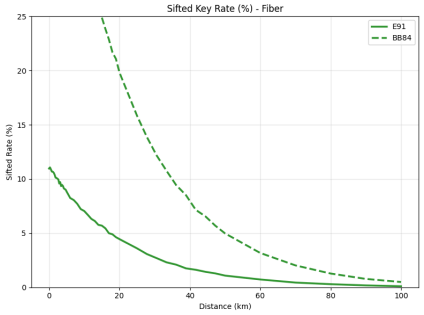
descending to zero. In contrast, E91's key length value begins at around 11000 and decreases following a slightly less steep trajectory. But, across all distances evaluated, BB84 outperforms E91 in this metric, as shown in Figure 2.

Figure 2. Key Length vs. Distance in Fiber Optic Channel Without Eavesdropping



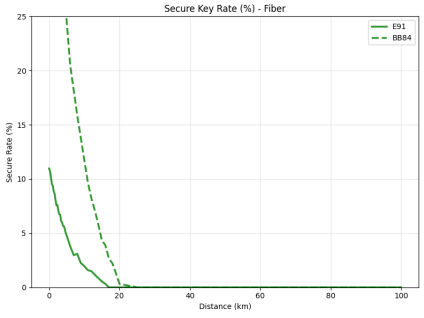
Similarly, the sifted key rate metric performs the same as the key length for both protocols, as shown in Figure 3.

Figure 3. Sifted Key Rate vs. Distance in Fiber Optic Channel Without Eavesdropping



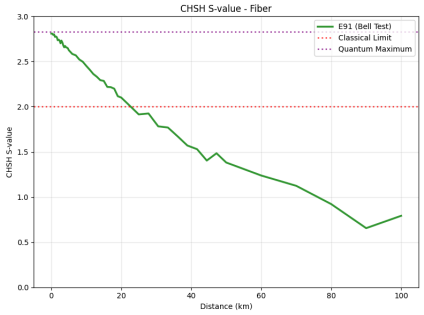
As seen earlier, the secure key rate reaches zero at 20 km as QBER exceeds the 11% threshold. While both protocols present a rapid decline in this metric, BB84's values exceed E91's in smaller communication distances by a huge margin, as shown in Figure 4. In fact, at 10 km, BB84's secure key rate value is 11.7%, while E91 presents a value lower than 2%.

Figure 4. Secure Key Rate vs. Distance in Fiber Optic Channel Without Eavesdropping



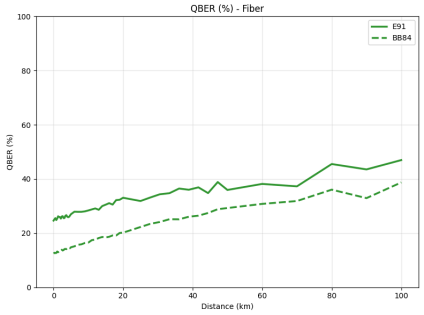
Exclusively to E91, the CHSH S-value begins at the quantum threshold and declines almost linearly. This trend continues until it crosses the classical limit of 2 at around 22 km, indicating a transition from quantum to classical behavior as distance increases, as illustrated in Figure 5.

Figure 5. CHSH S-Value vs. Distance in Fiber Optic Channel Without Eavesdropping



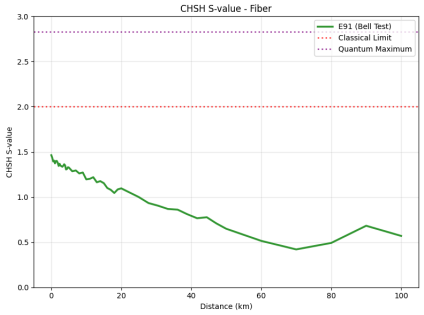
On the other hand, when eavesdropping was implemented in the simulation with a strength of 0.5, the quantum bit error rate for both BB84 and E91 protocols increased noticeably with distance, as shown in Figure 6. In this scenario, E91 maintained considerably higher QBER compared to BB84, depicting its greater sensitivity to eavesdropping.

Figure 6. QBER vs. Distance in Fiber Optic Channel With Partial Eavesdropping (e = 0.5)



Likewise, other security metrics were intensively affected. Secure key rates, for instance, dropped to zero across all distances for both protocols. Furthermore, CHSH S-values, exclusive to E91, were never above the classical threshold, as seen in Figure 7, indicating no quantum behaviour.

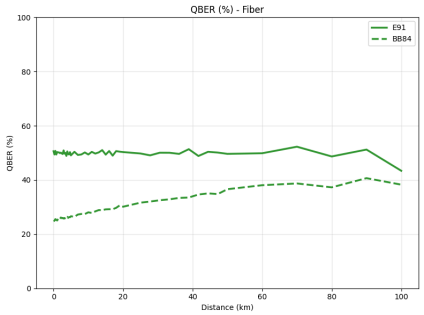
Figure 7. CHSH S-value vs. Distance in Fiber Optic Channel With Partial Eavesdropping (e = 0.5)



With the increase of eavesdropping strength to 1.0, QBER values for both protocols increased, as expected. Still, E91 was more sensitive to eavesdropping behaviour, depicting a QBER of more than 40% for all distances measured. BB84's values

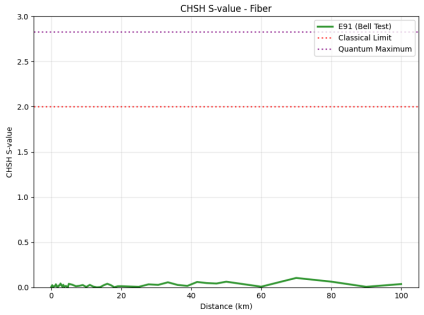
were twice as low for shorter distances, but approached E91's as the distances increased. This data is shown in Figure 8.

Figure 8. QBER vs. Distance in Fiber Optic Channel With Eavesdropping (e = 1)



CHSH S-values, illustrated in Figure 9, also suffered great impact. In fact, these values were close to zero for all distances experimented.

Figure 9. CHSH S-value vs. Distance in Fiber Optic Channel With Eavesdropping (e = 1)



b) Underwater Channel

Again, we started by simulating a channel with no eavesdroppers. But, for this channel, the efficiency of both protocols decayed extremely fast as the distance between Alice and Bob increased.

In fact, at just 250 meters, the QBER for both protocols reached 100%. Figure 10 depicts this scenario. As a result, all other metrics, including key rate and CHSH S-value for E91, also crashed, rendering the protocols unusable beyond this short distance. However, at distances under 0.3 km, BB84 had greater key length, sifted and secure key rate values. This trend can be seen in the analysis of the secure key rate in Figure 11.

Figure 10. QBER vs. Distance in Underwater Channel Without Eavesdropping

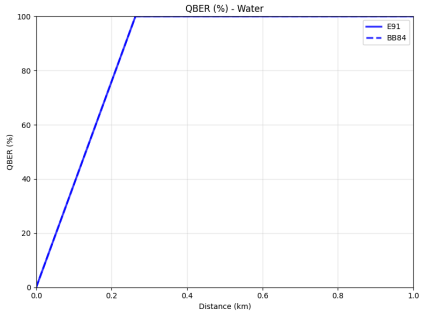
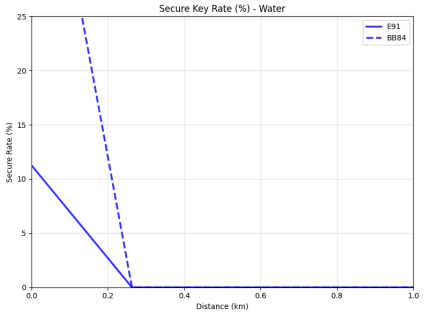
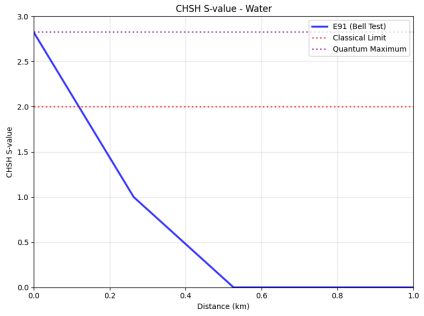


Figure 11. Secure Key Rate vs. Distance in Underwater Channel Without Eavesdropping



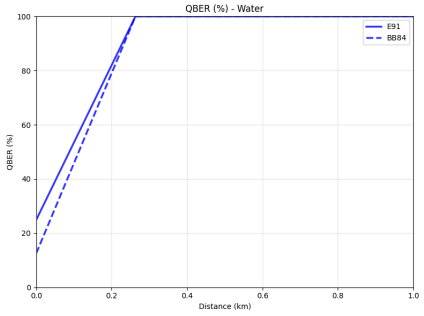
Moreover, the CHSH S-value crossed the classical threshold at less than 200 meters, as shown in Figure 12.

Figure 12. CHSH S-value vs. Distance in Underwater Channel Without Eavesdropping



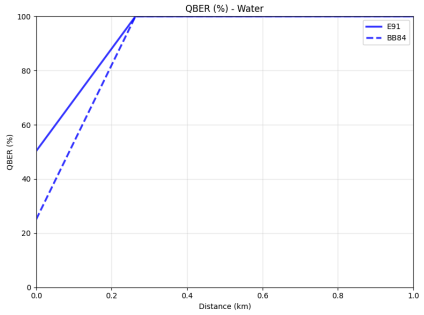
Under partial eavesdropping, QBER was greater than 40% for both protocols at the 100 meter mark. However, at distances shorter than 200 meters, BB84 maintained a slightly smaller value, since E91's QBER was almost twice that of the BB84 protocol, as depicted in Figure 13. As a result, all other security metrics were impacted. The secure key rates were zero for all distances tested and the CHSH S-Values were never greater than 1.5.

Figure 13. QBER vs. Distance in Underwater Channel With Partial Eavesdropping (e = 0.5)



For an eavesdropping strength of 1.0, QBER values increased, beginning at 50.3% for E91 and 25.1% for BB84, as shown in Figure 14. Moreover, CHSH S-values were zero across all distances.

Figure 14. QBER vs. Distance in Underwater Channel With Eavesdropping (e = 1.0)

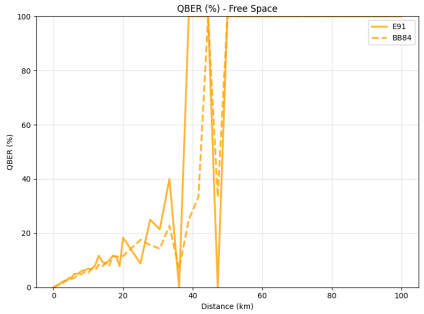


c) Free-space Channel

As usual both protocols were first simulated with no eavesdropping. Although having a depolarization length similar to the fiber optic channel, the simulation on the free-space channel underperformed considerably. However it was still functional over medium distances, in contrast to the underwater channel.

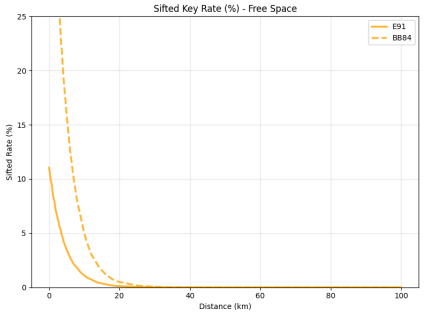
This time, QBER values for both protocols did not increase smoothly. At distances between 30 and 50 km, QBER oscillated, even - unexpectedly - reaching zero. Overall, though, BB84 values were slightly lower and suffered smaller oscillations compared to E91 values. More specifically, at 5 km QBER was 3.2% and 3.1% for E91 and BB84, respectively. But at 25 km, due to the random oscillations, BB84's QBER (17.6%) was twice that of the E91 (8.8%). Still, both protocols reached 100% QBER after the 50 km mark, as seen in Figure 15.

Figure 15. QBER vs. Distance in Free-space Channel Without Eavesdropping



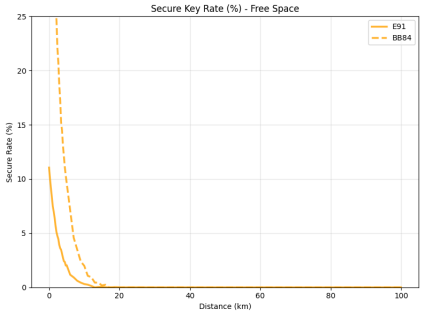
Regarding key lengths, in both protocols a steep decline until the 25km mark was measured. The same trend can be seen in the analysis of the sifted key rate. At 10 km, as shown in Figure 16, the sifted key rate was close to 5% for BB84 and less than 3% for the E91 protocol, meaning that only 2000 of the 100000 bits that were sent were being used to generate the secret key.

Figure 16. Sifted Key Rate vs. Distance in Free-space Channel Without Eavesdropping



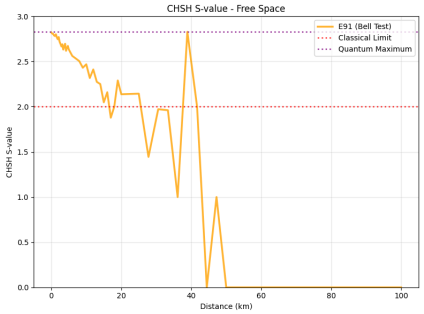
Likewise, the secure key rates followed a steeper decline. At just 10 km these values were close to zero. Specifically, while BB84 presented a rate of 1.99%, E91 value was at just 0.31%. Beyond this point, communication through this channel was made impossible. This is illustrated in Figure 17.

Figure 17. Secure Key Rate vs. Distance in Free-space Channel Without Eavesdropping



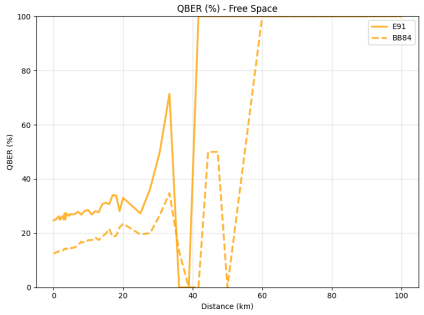
In contrast to all other channels, the CHSH S-value did not follow an almost linear decline as distance increased. After crossing the classical threshold at around 20 km, it oscillated intensely until it finally reached zero at the 50 km mark, as shown in Figure 18.

Figure 18. CHSH S-value vs. Distance in Free-space Channel Without Eavesdropping



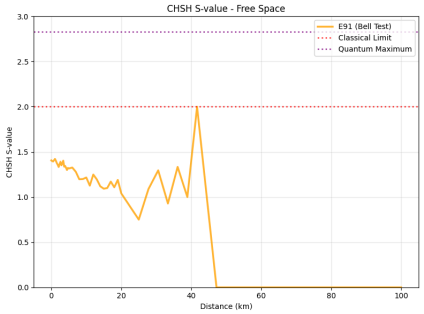
As other channels, partial eavesdropping simulation reveals a significant impact on QBER. Again, both protocols exhibited a bumpy increase as the distance between Alice and Bob overtook the 30 km mark. Now, though, E91' values were considerably higher than BB84's across all distances measured, as illustrated in Figure 19

Figure 19. QBER vs. Distance in Free-space Channel With Partial Eavesdropping (e = 0.5)



CHSH S-values, seen in Figure 20, were also never above the classical limit and equalled zero beyond 50 km. Moreover, due to the high QBER, the secure key rates for both protocols remained zero for all distances simulated.

Figure 20. CHSH S-value vs. Distance in Free-space Channel With Partial Eavesdropping (e = 0.5)



In a scenario where eavesdropping was maximized at 1.0, shorter distances' QBER values were substantially increased. At 25 km the QBER for BB84 and E91 in a simulated free-space channel was 64.3% and 36.5% respectively. Figure 21 depicts this situation. Moreover, CHSH S-Values were minimum for most distances. However, between the 35 to 50 km interval, anomalous spikes were measured over the classical limit, as shown in Figure 22.

Figure 21. QBER vs. Distance in Free-space Channel With Eavesdropping (e = 1)

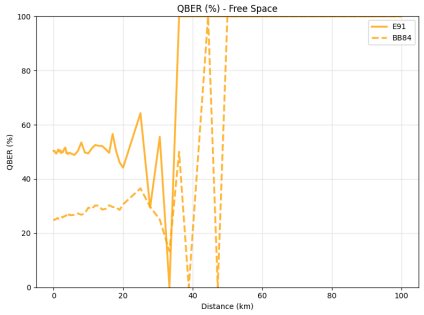
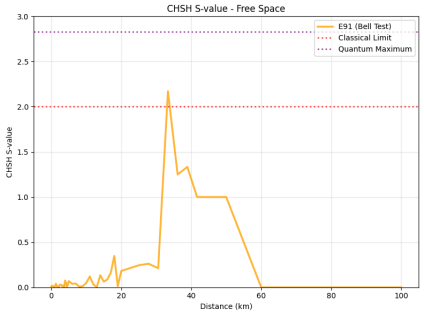


Figure 22. CHSH S-value vs. Distance in Free-space Channel With Eavesdropping (e = 1)



d) Discussion

In the absence of eavesdropping, BB84 consistently demonstrated greater performance in terms of efficiency metrics over E91. Specially 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 to be less susceptible to drastic QBER escalation under eavesdropping attacks. While E91 provided an additional metric - CHSH S-values - these values quickly degraded and fell below the classical threshold, even when no eavesdropper was implemented.

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 partially correct. Under short distances below 200 meters, communication is in fact possible. However, experiments over this threshold showed that the high attenuation and depolarization length of this type of channel imposes intense challenges for particle transmission.

In sum, although E91 is more sensitive to eavesdropping, allowing for easier detection, the protocol is too vulnerable to mild environmental noise compared to BB84. This means that its efficiency is drastically reduced, making it less practical over real-world noisy channels, even without eavesdroppers.

IV - Conclusion

Quantum Key Distribution (QKD) is the next step to secure communication. Thus, practical implementation needs to take place in the near future to protect secret information from the threats that quantum computers' algorithms impose. 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. However, we noted that, as E91 was more sensitive to eavesdropping, demonstrating higher values of QBER overall, it presented better detection capabilities.

With these insights, we believe that future research and practical implementations have valuable information 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, like quantum repeaters (Briegel, Dür, Cirac, & Zoller, 1998) and advanced quantum correction methods. So, bridging the gap between theoretical and practical quantum communication is essential to unveil the full potential of this technology.

VII - Bibliography

1. Agrawal, G. P. (2012). *Fiber-Optic Communication Systems*. John Wiley & Sons.
2. 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
3. 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
4. Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560, 7–11. https://doi.org/10.1016/j.tcs.2014.05.025
5. Bernstein, D. J., Heninger, N., Lou, P., & Valenta, L. (2017, June 4). Post-quantum RSA. https://doi.org/10.1007/978-3-319-59879-6_18
6. Bhatia, V., & Ramkumar, K. R. (2020). An Efficient Quantum Computing technique for cracking RSA using Shor's Algorithm. *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*, 89–94. https://doi.org/10.1109/ICCCA49541.2020.9250806
7. 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

8. 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
9. 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
10. Czerwinski, A., & Czerwinska, K. (2022). Statistical Analysis of the Photon Loss in Fiber-Optic Communication. *Photonics*, 9(8), Article 8. https://doi.org/10.3390/photonics9080568
11. Díaz, F., & Lenin, J. (2014, March 28). *Geração de emaranhamento de polarização entre pares de fótons no regime de fentossegundos* [Master's thesis]. Universidade Federal de Pernambuco. https://repositorio.ufpe.br/handle/123456789/18296
12. 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
13. Maloo, S. (n.d.). *Quantum Cryptography and Communication: Protocols, Limitations, and Solutions*.
14. Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information* (10th anniversary ed.). Cambridge University Press.
15. 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), 057901. https://doi.org/10.1103/PhysRevLett.92.057901
16. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134. https://doi.org/10.1109/SFCS.1994.365700
17. 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
18. Teich, M. C., & Saleh, B. (2007). *Fundamentals of photonics* (Vol. 2). Wiley.
19. 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), 7. https://doi.org/10.1038/ncomms1005
20. 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
21. 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), nwaf147. https://doi.org/10.1093/nsr/nwaf147

22. 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

VI - 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 which participated in the IRIS Computer Science sessions. All the support and inspiration was fundamental for both the writing and the empirical process. Therefore, we are extremely grateful to everyone involved.

Referee Report — Convergence

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

Overview. This student manuscript compares BB84 and E91 across fiber, free-space, and underwater channels using simulation. It reports QBER, sifted and secure key rates, and—for E91—CHSH S-values, both with and without an intercept–resend eavesdropper. The topic is timely and well-suited to *Convergence*'s audience. With a focused round of revisions—mainly clarifications, consistency checks, and presentation polish—the paper will make a strong pedagogical contribution.

Comments

1) **Channel models and units.**

   Loss. You cite Beer–Lambert with attenuation α in dB/km but do not show the exact conversion from dB/km to linear transmittance per distance used to compute $P_{\text{survive}}(d)$. Please write the explicit formula used in the simulator (e.g.,

   $$P_{\text{survive}}(d) \;=\; 10^{-\alpha d/10},$$

   include units for α and d, and state any additional loss terms (coupling/detection).

   Depolarization. The model applies a distance-dependent random Pauli error with equal $X/Y/Z$ probabilities. Specify the underlying quantum channel (e.g., depolarizing channel $\mathcal{E}(\rho) = (1-p)\rho + p\,I/2$, or a Pauli channel with (p_X, p_Y, p_Z)), explain how λ maps to the error probability $p(d)$, and justify equal weighting. Replace the future-dated citation ("Zhang et al., 2025") with a published estimate or clearly mark it as a provisional assumption.

2) **Security thresholds and claims.** Treat the $\sim 11\%$ BB84 QBER threshold carefully: it assumes idealized, asymptotic conditions and one-way error correction/privacy amplification. You currently zero the secure key rate beyond ~ 20 km based on this cutoff. At minimum, state these assumptions explicitly and soften the language from "hard limit" to "guideline under our assumptions." If feasible, add a brief note on finite-key sensitivity.

3) **Eavesdropping models.** For E91 you describe intercept–resend where Eve "measures on a random basis and resends a random state," which destroys entanglement; however, different intercept strategies affect correlations differently. Define Eve's behavior precisely for both protocols (basis choice, measurement rule, resend rule). For E91, briefly state the expected change in correlations and in S under your attack model before presenting simulation results.

4) **Numerical stability and anomalies.** The free-space results show QBER oscillations (including unexpected zeros) and CHSH spikes above the classical limit under full eavesdropping at 35–50 km. These suggest inadequate averaging or an implementation issue. Increase runs, vary seeds, report means with uncertainty (error bars or shaded bands), and comment on any residual anomalies rather than over-interpreting single points.

5) **Sifting details.** Report the expected and observed sifting fraction ($\approx 50\%$ for BB84 with random bases) at short distance and no attack, and confirm that your observed fraction matches expectation within statistical error. This serves as a simple end-to-end sanity check.

6) **Figures and captions.** A couple of figure references don't seem to resolve cleanly (the numbering appears to skip), and some axes are hard to read. Please ensure every referenced figure is present, bump font sizes, put units on axes, and keep comparable axis limits across media so side-by-side comparisons are fair.

7) **Reproducibility basics.** Because the conclusions rest on a simulator, include either a minimal code link or an appendix with pseudo-code, random seeds, and a compact parameter table (e.g., α, λ, distance grid, trials per point). Without this, readers can't sanity-check the pipeline.

Verdict

Accept after the revisions.

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

Overview: In this manuscript, the author explores the performance of two well-known quantum key distribution protocols, BB84 and E91, under realistic conditions of physical noise. The author models the effects of both photon loss and depolarization in different media and defines a number of metrics against which these algorithms are tested and compared.

The paper is very thorough and targets a timely topic. However, it could be better written and illustrated in certain places; in particular, to be most valuable to many audiences, much of the text should be written for concision and many figures should be combined. It should also be thoroughly checked for grammar since there were grammatical errors in many places. I thus suggest that this paper be accepted with major revisions (acceptance conditional on satisfactory major revisions). A thorough set of comments follow below.

Substantive Edits

1. I would strongly recommend making the paper more concise by condensing the Methods section. Too long of a Methods section conceals your more important original results. I would suggest citing certain discussions away to the original papers. This may also be facilitated by using equations, which are naturally more direct, as opposed to text to explain many things. Your discussion of Bell's inequality is repeated, for example.
2. All figures should be enlarged. In particular, all figure fonts should be relatively large and clear to facilitate interpretation, including axis labels and legend fonts. Moreover, curves that represent different data types should be plotted both in different colors AND using different types of lines (solid, dash, dotted, etc.) to facilitate interpretation by a range of people, including those with color-blindness. There are color-blind palettes available.
3. Moreover, in many cases, it would make more sense to condensed the multiple figures into one where figures that study the same phenomena in slightly different ways are made into a single panel.
4. The meaning of this sentence isn't quite correct: "Due to the absence of real quantum hardware (such as single-photon sources and detectors), polarization states, measurements, and channel effects were modeled computationally." Quantum hardware is very real, including single-photon sources. I believe what you mean is that you did not have access to such hardware. If so, the sentence should be rewritten.
5. Papers typically number sections, as opposed to letter them.
6. The methods section would be improved if the key equations underlying both methods were stated.

Minor Edits

1. In the abstract, "Quantum key distribution (QKD) has emerged in recent decades as a hopeful approach to guarantee secure data transmission, …" should replace the word hopeful with potential, prospective, or possible.

2. In the abstract, “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.” should replace the word independence with dependence since BB84 depends upon entangled pairs.
3. The key word “Realistic Simulation” should be removed since it is not clear what that means technically (many things can map to that phrase that have nothing to do with your paper).
4. Still isn’t the right transition word for this sentence since you are not making a contrast: “Still, we predict that underwater channels are not viable for practical implementation.”
5. “For both protocols, the transmission of 100000 particles” should replace particles with photons.

Review of: "Comparative Performance Analysis of BB84 and E91 Quantum Key Distribution Protocols Under Real-World Imperfections"
Author 100061, Submission 100056
Date: October 19, 2025

To the Author,

Recommendation: **Accept with major revisions**

This recommendation reflects the paper's strong research premise and sound methodology. The identified issues, while significant, are well-defined and achievable to address through revision. The core of the research is strong, and a revised version that incorporates these suggestions will meet the high academic standards of the journal.

I am confident that by incorporating the suggestions below, this paper will be an excellent candidate for publication. You have done a wonderful job on a challenging topic, and I strongly encourage you to incorporate the revisions below. I look forward to reading the next version of your manuscript.

Review Summary

Strengths:

- Ambitious and well-executed simulation project.
- Exceptional clarity and pedagogical value in explaining complex quantum protocols.
- Strong, logical structure and excellent use of figures and tables.
- Thorough engagement with foundational and contemporary literature.

Limitations:

- The primary limitations are the unaddressed statistical anomalies in the free-space simulation results and the inconsistencies in explaining how probabilities were dealt with in the methodology section, which currently detract from the paper's rigor.

This is a high-quality manuscript with the potential to be an outstanding contribution to the journal. The identified limitations are significant but correctable with relatively minor revisions.

General Assessment

Thank you for submitting your work to Convergence Journal! It was a pleasure to read such a well-structured and ambitious paper from an early-career researcher. You have undertaken a significant computational project and presented the results with remarkable clarity. The work is well-suited for the journal's audience and provides an excellent, accessible bridge between the theory of quantum communication and the practical challenges of implementation. My review is structured according to the journal's key evaluation criteria,

followed by a summary and final recommendations. You have tackled a difficult and highly relevant topic with clarity and academic rigor. The feedback below is offered in the spirit of mentorship, with the goal of helping you refine this already impressive manuscript into an even stronger publication. Some of the recommendations start from errors and should be definitely addressed in order to prepare the manuscript for publication. By contrast, the remaining feedback is aimed at helping the author improve the paper even more and the author is the one to decide whether they believe it is worth the effort to address these recommendations.

This is a very strong manuscript that demonstrates a solid understanding of quantum key distribution principles and a commendable proficiency in computational simulation. You clearly present the research question, develop a sound methodology for modeling the quantum channels and protocols, and present the results in a logical fashion. The paper's greatest strength is its pedagogical value; the explanations of the BB84 and E91 protocols, channel effects like photon loss and depolarization, and the relevant performance metrics are exceptionally clear and would be highly beneficial for high school and undergraduate readers. While the overall quality is high, there are specific areas, particularly concerning the interpretation of some simulation results, that require revision to enhance the paper's scientific rigor.

Detailed Feedback Based on Evaluation Criteria

1. Originality & Significance:
While a comparative study of BB84 and E91 is not novel in the broader field of quantum physics, this paper's contribution is significant and original within the context of student research and for the journal's target audience. The direct comparison of the protocols across three distinct and physically motivated channels (fiber optic, underwater, and free-space), complete with simulated eavesdropping, provides a comprehensive and insightful analysis. It is a creative and well-executed project that synthesizes complex theoretical concepts into a tangible computational experiment, which is a valuable contribution.

2. Clarity & Structure:
The paper's structure and clarity are exemplary. The manuscript is organized logically, beginning with a well-motivated introduction, followed by a detailed methodology, a systematic presentation of results, and a concluding discussion. The use of subsections for each channel and eavesdropping scenario makes the results section easy to navigate. Furthermore, the inclusion of tables to summarize parameters (e.g., Table 1 for attenuation coefficients) and illustrate protocol steps (e.g., Table 6 for a BB84 example) significantly enhances readability and understanding. You have done an excellent job of making a complex topic accessible.

One important remark is that the figures should be slightly larger, maybe even double in size to ensure clarity. The axes labels and figure title are difficult to read without zooming into the page.

3. Use of Evidence & Research Methods:
The methodology is generally sound and well-explained. You correctly employ standard physical models, such as the Beer-Lambert law for photon loss and a Markovian model for depolarization, and ground the simulation parameters in cited literature. The implementation of the protocols and the eavesdropping attack models are appropriate.

However, a significant concern arises from the results of the free-space channel simulation. The paper reports that the Quantum Bit Error Rate (QBER) "oscillated, even unexpectedly reaching zero" at intermediate distances (Figure 15) and that the CHSH S-value showed "anomalous spikes" under eavesdropping (Figure 22). These results are highly irregular and suggest statistical artifacts rather than physical phenomena. They are likely caused by a very low number of photons surviving transmission at those distances, making the calculated metrics unreliable.

Specific Recommendation: To address this, I recommend the author perform one of the following:

- Increase simulation trials: Re-run the free-space simulation with a much larger number of initial photons (e.g., 1,000,000 instead of 100,000) if computationally possible. This will improve the statistical significance of the results at longer distances and likely smooth out the anomalous oscillations.
- Acknowledge and discuss uncertainty: If re-running the simulation is not feasible, the author must add a discussion of this anomaly. It should be explicitly stated in the Results and Discussion sections that the oscillations are likely statistical noise due to a low count of surviving photons.

Addressing this point is crucial for the paper's scientific integrity.

4. Engagement with Literature:
You demonstrate a strong engagement with the relevant scientific literature. The paper correctly cites the foundational works of Bennett & Brassard (BB84) , Ekert (E91) , and Shor & Preskill (for the BB84 security proof). Furthermore, the use of a standard textbook like Nielsen & Chuang and references to experimental papers for channel parameters shows that the author has conducted thorough background research. The work is well-situated within the established knowledge of the field. I encountered one case where you did not cite the original paper, but a more recent one, which I highlighted below in the feedback for the corresponding section.

5. Grammar & Language:
The quality of the writing is suitable for a research journal. The language is clear, professional, and precise. You explain complex concepts without resorting to unnecessary jargon, making the paper highly accessible to its intended audience. The manuscript is polished and free of any significant grammatical errors.

Additional specific recommendations

A. Abstract and Introduction

- This is a tiny typographic advice but it is applicable for the entire manuscript: you should replace the hyphens (-) with em (—) or en (–) dashes. Check when each one should be used and please use them accordingly in your manuscript.
- Some recommendations on the paragraph where you explain the BB84 protocol:
    - Clarify what is meant by "representing binary values": "Alice and Bob can send polarized photons representing binary values (0 and 1)"
    - Refine the explanation of eavesdropping detection: The photon's state doesn't just "collapse with the wrong basis", rather, *Eve's measurement disturbs the quantum state*, leading to observable error rates in the sifted key.
    - Cite Bennett & Brassard correctly**:** "Bennett & Brassard, 2014" likely refers to a *reprint* or *retrospective publication*. I believe the **original** paper is *Bennett & Brassard (1984)* You could clarify this.
    - Add one line to complete the flow (optional): It might help to close by mentioning that after sifting, error correction and privacy amplification are performed to finalize a secure key.
- Some recommendations on the paragraph where you explain the E91 protocol:
    - Clarify the correlation behavior: The correlations are strongly correlated only when compatible measurement settings are used, not "even when different bases are chosen." In fact, for certain non-compatible basis choices, quantum correlations deviate from classical predictions, allowing the Bell test, but the measurement results themselves are not deterministic.
    - Bell test interpretation: It's not that "violation confirms entanglement" per se, but that it rules out local realistic (classical) explanations, which is evidence of entanglement and no eavesdropping.
    - Terminology tweak: "Check the integrity of the key exchange" → better phrased as "verify the security of the quantum channel."
    - Minor stylistic polish: Replace some dashes with commas or semicolons for smoother academic flow.
- Consider reframing the hypothesis to explain why this performance difference is expected. This reframing elevates the hypothesis from a simple prediction to a more sophisticated physical argument, demonstrating a deeper level of understanding.
- The introduction could also benefit from acknowledging the dual nature of E91's sensitivity to noise and interference. The manuscript correctly identifies this sensitivity as a practical drawback leading to higher QBER. However, this sensitivity is also the very foundation of its security model. An eavesdropper's interaction with the entangled pair inevitably disturbs the delicate quantum correlations, causing a detectable drop in the CHSH S-value and a spike in the QBER. In this sense, E91's "fragility" is also its strength, as it makes eavesdropping attempts more conspicuous.

B. Methodology

It is not expected that you implement a full-scale atmospheric turbulence simulation, as these often require complex numerical methods like split-step propagation and the generation of random phase screens. However, acknowledging this limitation is a crucial part of rigorous scientific reporting. It is recommended that you:

1. Acknowledge the limitation**:** In subsection II-a) on Channel Modeling, add a paragraph explicitly stating that the current free-space model is a simplification that does not account for the effects of atmospheric turbulence.
2. Describe the physics**:** Briefly explain what turbulence is and its primary effects (e.g., Atmospheric turbulence causes random fluctuations in signal strength and phase, leading to bursty errors and time-varying channel loss, rather than a smooth degradation with distance).
3. Contextualize the results**:** In the Results and Discussion sections, explicitly connect the observed oscillations in the free-space data to this model limitation. This demonstrates a mature understanding of both the underlying physics and the boundaries of the simulation.

I am afraid section II-a) contains a critical error which I hope is just a typo and not the actual way in which the photon loss was modelled. In a per-photon Monte Carlo, you keep the photon if the random number you draw from [0,1] is <= P_survive(d) and drop it otherwise. Your text says “If the number is lower, the photon is considered lost,” which is the opposite of what “survival probability” means. At the beginning of the channel, P_survive(0) = 1, so by the method you describe we would drop all the photons…The same description with the inverted logic repeats in section II-b) so please check this aspect thoroughly (“A photon is considered lost - and its value is set to None - if the survival probability is smaller than a randomly generated number (k) ∈ {0, 1}. “)...In section II-c), your logic is the correct one (“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}.”) so I hope this is how the algorithm worked in your simulation.

Please also correct the descriptions of how the depolarization is applied in section II-b) and II-c) since the two descriptions are not consistent (they represent the two opposite cases). For example, the logic in section II-c) is backwards (“On the other hand, when the depolarization probability is smaller than (k), the photon becomes mixed, resulting in completely random measurement outcomes.”) and not correct. Think about the starting location, where P_depol = 0. By your description, all photons would depolarize from the start no matter the value of k in (0, 1].

Please also correct and double check the part of the algorithm described by “Subsequently, this probability is compared to a randomly generated number (k) ∈ {0, 1}. If P_same is smaller, Bob’s outcome matches Alice’s.”. The logic here is also inverted compared to the correct one. If P_same = 1, and you compare it to any k, you will always conclude that Bob’s outcome does not match Alice’s even though we started with a 100% probability for the outcomes to be the same….

C. Results and Analysis

You should re-interpret these anomalous results by discussing the potential high effect of statistical artifacts in the results presented in your figures. At longer distances in a highly lossy channel, the number of photons that survive to be measured by Bob becomes very small. For instance, out of 100,000 initial particles, only a tiny fraction might reach the detector at 40 km or 50 km. When performance metrics like QBER or correlation coefficients are calculated from a very small statistical sample, they are subject to large random fluctuations. A few "unlucky" random errors can cause a large swing in the calculated QBER. This effect explains the jagged, non-monotonic behavior seen in the graphs.

A particularly telling example is Figure 22, which shows spikes in the CHSH S-value that appear to violate the classical limit of $|S| \leq 2$ even with a strong eavesdropper present. This is an unphysical result. The CHSH test requires calculating four separate correlation coefficients from the measurement outcomes. When the number of surviving photon pairs available for this calculation becomes statistically insignificant, the resulting S-value is essentially random noise and can fluctuate into these unphysical regimes.

You should explicitly discuss this in the analysis. For example, when discussing Figure 22, you should highlight some of the following aspects. The anomalous spikes observed in the CHSH S-value at longer distances, particularly under eavesdropping, are likely statistical artifacts. At these distances, high photon loss drastically reduces the number of correlated pairs available for the CHSH calculation. When the sample size is very small, the calculated correlation values are not statistically significant and can fluctuate randomly. This highlights a practical challenge in implementing the E91 protocol: a sufficient number of transmitted particles is required to perform a statistically meaningful security check.

For figures showing key rate or key length versus distance (e.g., Figure 2, Figure 3, Figure 4), consider using a logarithmic scale for the y-axis. This is standard practice in QKD literature as it allows the performance at longer distances to be visualized more clearly, rather than appearing to crash to zero immediately.

Additional specific recommendations:

- The underwater channel claims are plausible but contextual. Stating “<200 m works; >200 m is impractical” is site- and spectrum-dependent (water type, turbidity, wavelength (blue-green window ~450–550 nm, beam divergence, background light, polarization scrambling). It’s fine to say your data shows feasibility below ~200 m for your water type and hardware, but avoid universalizing it.
- CHSH S-values “below classical even with no eavesdropper”
    - This is a red flag about the link, not proof E91 is weaker.
    - CHSH S is exquisitely sensitive to visibility, alignment, depolarization, detector noise, and loss. If S<2 without an eavesdropper, your state visibility V was too low (misalignment/depolarization/multi-pair, or accidental coincidences). The rough mapping S < 2 implies QBER > approx. 14.6%, i.e. already beyond BB84’s one-way security threshold. So the “quick S degradation” is consistent with channel/device noise, not a protocol flaw.
    - When an article says “CHSH S-values were below the classical threshold even without eavesdropping in the water channel,” that likely means:

- The channel noise (not eavesdropping) destroyed entanglement,
- The measured correlations were too weak to show a Bell violation, and
- Therefore, secure entanglement-based QKD was not achievable under those physical conditions.
- That’s a scientifically valid observation, not an error, but it should be clearly explained as environmental decoherence, not as a classical limit of quantum theory or a weakness of the protocol itself.

D. Discussion and Conclusion

The conclusion that BB84 is more "practical" is fair based on the simulation results. However, it is important to acknowledge the unique theoretical advantages of E91 that are not fully captured by these performance metrics. The E91 protocol is the conceptual foundation for Device-Independent QKD (DI-QKD), an advanced form of quantum security where a secure key can be established even if the quantum devices used by Alice and Bob are untrusted or have been tampered with by an adversary. This provides a level of security that prepare-and-measure protocols like BB84 cannot achieve.

In addition, you can demonstrate a more profound understanding of the field's trajectory by discussing this. A paragraph could be added to the discussion or conclusion. While your results indicate BB84's superior performance in the presence of channel noise, it is important to note the distinct theoretical advantages of the E91 protocol. E91's reliance on Bell's inequality paves the way for Device-Independent QKD, which aims to provide security without having to trust the internal workings of the communication hardware. Therefore, while BB84 may be more suitable for near-term practical implementations, research into overcoming the fragility of entanglement in protocols like E91 is crucial for developing next-generation quantum networks with even stronger security guarantees.

The conclusion rightly mentions quantum repeaters as a key technology for extending the range of QKD. To further showcase the breadth of the author's knowledge, this point could be briefly expanded to include other mitigation techniques being actively researched. These include adaptive optics, which use deformable mirrors to correct for atmospheric turbulence in real-time in free-space links, and advanced classical error correction codes tailored for the low signal regimes of QKD. Mentioning these would add further depth to the outlook on future research.

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

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 optic 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, Quantum Communication, Communication Protocols, BB84, E91.

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, since the development of quantum computers and algorithms, the security of many traditional cryptographic methods has been fundamentally threatened. 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 quantum mechanics' uncertainty principle and no-cloning theorem (Nielsen & Chuang, 2010). By using two conjugated 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 bases, and assuming a noiseless channel, Bob will measure the correct bit. But, if Alice sends a photon encoded in the rectilinear basis and Bob chooses the diagonal, quantum uncertainty dictates a 50% probability of obtaining the correct value. Then, using a classical insecure channel, Alice and Bob can 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 non-compatible 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. Then, to verify the security of the quantum channel, they can compare a subset of their measurements' results to check for violations. If Bell's inequalities are satisfied rather than violated, it implies 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 was 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 on 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 sifting 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 travelling 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 law (Teich & Saleh, 2007) can be employed:

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

where $I(d)$ denotes the intensity of light after propagating a distance d (km) through an absorbing or scattering medium, I_0 represents the initial power and α (dB/km) the attenuation coefficient (Czerwinski & Czerwinska, 2022). Then, to get 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 decibels 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 on the loss model defined by Equation (2). For each photon simulated, a random number in [0,1] is generated and compared to $P_{survive}(d)$. 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 kilometers, 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:

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

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

For this simulation typical values of λ 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 approximate as randomizing processes. If future experimental data shows bias toward particular error axes, the model can be replaced by a Pauli channel with pX, pY, pZ fit from data.

Table 2 : Depolarization length (λ), measured 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 has 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,

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

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

Then, these photons travel through noisy and lossy channels before reaching Bob's randomly chosen polarization bases and single-photon detectors. After, 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 are 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 $\{ai\}$ with $ai \in \{0, 1\}$ 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 BB84 protocol

Polarization	Basis	Bit Representation
0	Z (Rectilinear)	0
π/2 (90°)	Z (Rectilinear)	1
π/4 (45°)	X (Diagonal)	0
3π/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) ∈ {0, 1}. Similarly, a photon suffers depolarization, represented by the application of random Pauli X, Y, or Z errors with equal probability as described in Table 4, if k is smaller than the depolarization probability.

Table 4. 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.*

After channel effects are applied, Bob receives the photons and measures each one in a randomly chosen basis. He generates a basis string {ϕi} with ϕi ∈ {Z, X} and length n. For each incoming photon, Bob uses the corresponding basis ϕi to perform his measurement. For example, if Bob detects a photon polarized in the rectilinear basis (horizontal |H⟩ (0) or vertical |V⟩ (π/2)) and measures its value with the Z basis, he deterministically records either 0 for |H⟩ or 1 for |V⟩. 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⟩ — defined by Equation (5)) when the photon is actually |H⟩ is given by the squared overlap (Born rule) (Nielsen & Chuang, 2010):

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

The probabilities of obtaining bit 0 or 1 when measured in the Z (rectilinear) or X (diagonal) basis, for each of the four polarization states of a photon, are shown in Table 5.

Table 5. Measurement outcome probabilities for BB84 states in the Z and X bases.

Prepared State	**Z Basis: *P*(0), *P*(1)**	**X Basis: *P*(0), *P*(1)**
$\|H\rangle$ (0)	1.0, 0.0	0.5, 0.5
$\|V\rangle$ ($\pi/2$)	0.0, 1.0	0.5, 0.5
$\|A\rangle$ ($\pi/4$)	0.5, 0.5	1.0, 0.0
$\|D\rangle$ ($3\pi/4$)	0.5, 0.5	0.0, 1.0

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 with 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, it is introduced in the communication channel, after all loss and noise is applied, an observer, Eve. 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. Table 6 and Table 7 show an example of the protocol without and with eavesdropping, respectively.

Table 6. 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	$\pi/2$	$\pi/4$	$\pi/4$	$\pi/2$	$3\pi/4$	$\pi/2$	$3\pi/4$	$\pi/4$	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 incorrect basis		**1**		**0**	**1**				**0**	**0**

Table 7. 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		**1**		**0 or**	**1**				**0 or**	**0**

discarding incorrect basis				**1**					**1**	

Notice that in Table 6 — when no eavesdropper was present — all matching bases correspond to matching bits. However, in Table 7, after introducing eavesdropping, the bits in positions b4 and b8 (which share the same bases) are corrupted. 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 an entangled pair. 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).

Similarly 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 individual, Victor, equally distant to Alice and Bob sends, to both parties, photons prepared in the maximally entangled singlet state

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

Next, Alice and Bob independently select one of three measurement bases (angles) randomly, with uniform probabilities. Table 8 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 is reserved for key generation. In this simulation, the basis that corresponds to a measurement angle of π/2 is used to generate the final key.

Table 8. Possible Measurement Bases for Alice and Bob

Basis Index	**Alice's bases**	**Bob's bases**
0	π/2	π/2
1	0	π/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 $(k) \in \{0, 1\}$. 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 ($|0\rangle$) or -1 ($|1\rangle$), 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

$$P(b = -a \mid \theta_A = \theta_B) = 1, \quad (9)$$

where a,b and θA, θB represent Alice and Bob's measurement outcomes and selected angles, respectively. It is also important to mention that the singlet state $|\Psi\rangle$ defines a 50% probability of measuring each outcome for both parties, because the probability of Alice measuring +1 is given by

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

and after this measurement, $|\Psi\rangle$ collapses to just

$$\left|\Psi^-\right\rangle = |01\rangle, \quad (11)$$

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):

$$E(\theta_A, \theta_B) = P_{++} + P_{--} - P_{+-} - P_{-+}, \quad (12)$$

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:

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

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

$$E(\theta_A, \theta_B) = -\cos[2(\theta_A - \theta_B)], \quad (14)$$

finally giving the expression in the form:

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

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. Table 9 shows more examples.

Table 9. Equation (15) applied to various measurement angles combinations

Bits	θA (Alice)	θB (Bob)	θA − θB	− cos[2(θA − θB)]	P_{same} **(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

In sum, step three of the simulation starts with Alice measuring the value $a \in \{+1, -1\}$ 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 $(k) \in \{0, 1\}$. If P_{same} 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 offer 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.

Quantum Bit Error Rate (QBER) is one of the most critical metrics of quantum key distribution protocols. By measuring the fraction of bits of the sifted key that differ between Alice and Bob, the communication's security can be evaluated. Therefore, it is given by

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

where N is the total number of bits in the sifted key; a_i, b_i are the i-th bit from Alice and Bob, respectively; $\delta(a_i \neq b_i)$ is a function that returns 1 if $a_i \neq b_i$ and 0 otherwise. While a low QBER indicates stronger security guarantees, a QBER above a certain threshold points to the presence of malicious interference or excessive noise.

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: 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.

The sifted key rate refers to the proportion of raw key bits that remain after Alice and Bob discard all bits for which they used incompatible measurement bases. Thus, it is an important metric to evaluate the effectiveness of a protocol: a higher sifted rate means more usable bits per transmission — which makes it more practical for real-world implementations.

In contrast, the secure key rate represents the portion of the sifted key that can be securely used. Since some of the bits in the sifted key may be compromised by noise, losses and potential eavesdropping, it is important to discard them to prevent leaking

valuable information. Therefore, the secure key rate reflects the protocol's real-world viability by considering just the net amount of safe key material. Its calculation is given by (Shor & Preskill, 2000):

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

where R_{sifted} is the sifted rate and H_2 is a binary entropy function:

$$H_2(p) = -p\, log_2\, p - (1-p) log_2(1-p). \quad (18)$$

The key length refers to the total number of secure bits generated after all post-processing steps. Similarly to the sifted key rate metric, the key length is particularly relevant for assessing the practical usability of the protocol. Since most cryptographic applications require large key lengths to be effective, the protocol's ability to generate long, secure bit strings is a crucial factor for in-the-field quantum communication.

Lastly, the CHSH (Clauser–Horne–Shimony–Holt) S-Value (Clauser, Horne, Shimony, & Holt, 1969) is used to evaluate the security of quantum communication based on the E91 protocol exclusively. It quantifies the strength of the correlations between Alice and Bob's outcomes. By computing four correlation coefficients — described by Equation (12) — for which Alice and Bob used different measurement angles, the S-Value is obtained:

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

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√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).

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 10 presents these intervals and their respective amount of sampling points.

Table 10. 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

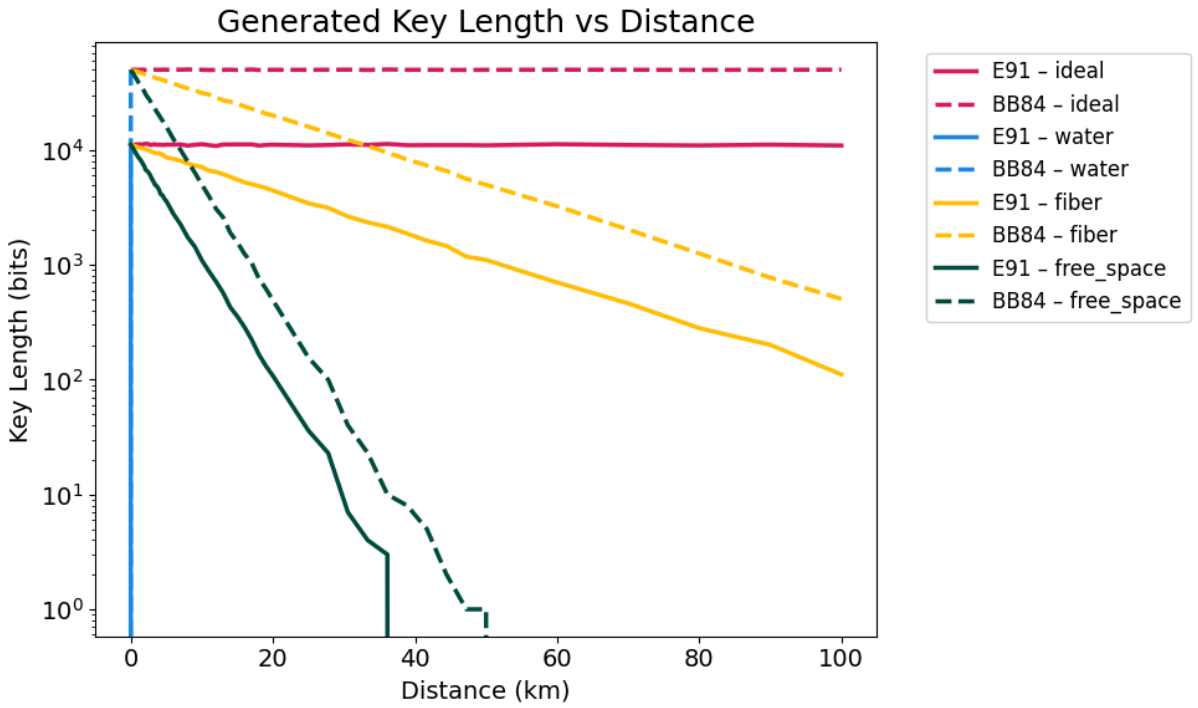
This section is divided into four subsections. Each of the first three subsections is dedicated to describe the results of both protocols under each simulated quantum channel. Subsection **(3.1)** presents the results for the generated key length across all channels. Subsection **(3.2)** shows the secure 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), 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 achieved 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 was 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. Nonetheless, for completeness, the results for 50% and 100% eavesdropping are presented, respectively, in Figures 2–3.

Figure 2. Key Length vs. Distance (Partial Eavesdropping — e = 0.5)

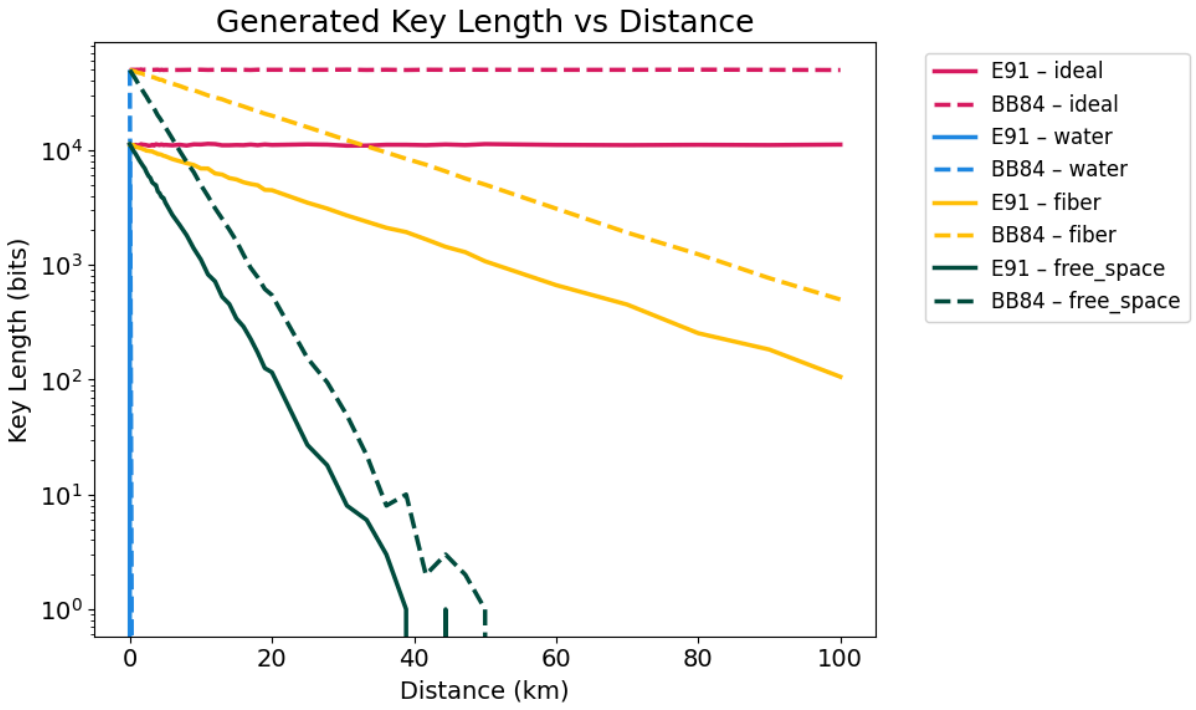
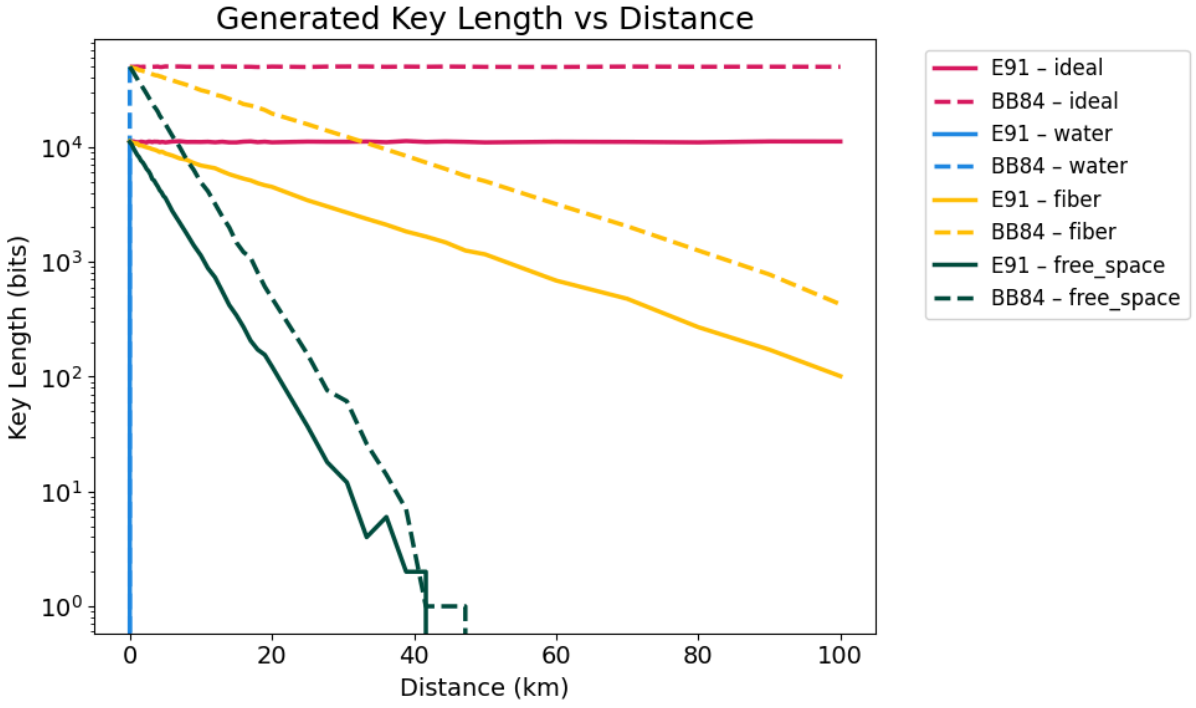


Figure 3. Key Length vs. Distance (Full Eavesdropping — $e = 1.0$)



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 4

shows the secure and sifted key rate as a function of distance for the BB84 protocol, under ideal, fiber-optic (fiber), underwater (water), free-space transmission. Figure 5 depicts the same metrics but for the E91 protocol.

Figure 4. BB84 — Secure and Sifted Key Rate vs. Distance (Without Eavesdropping)

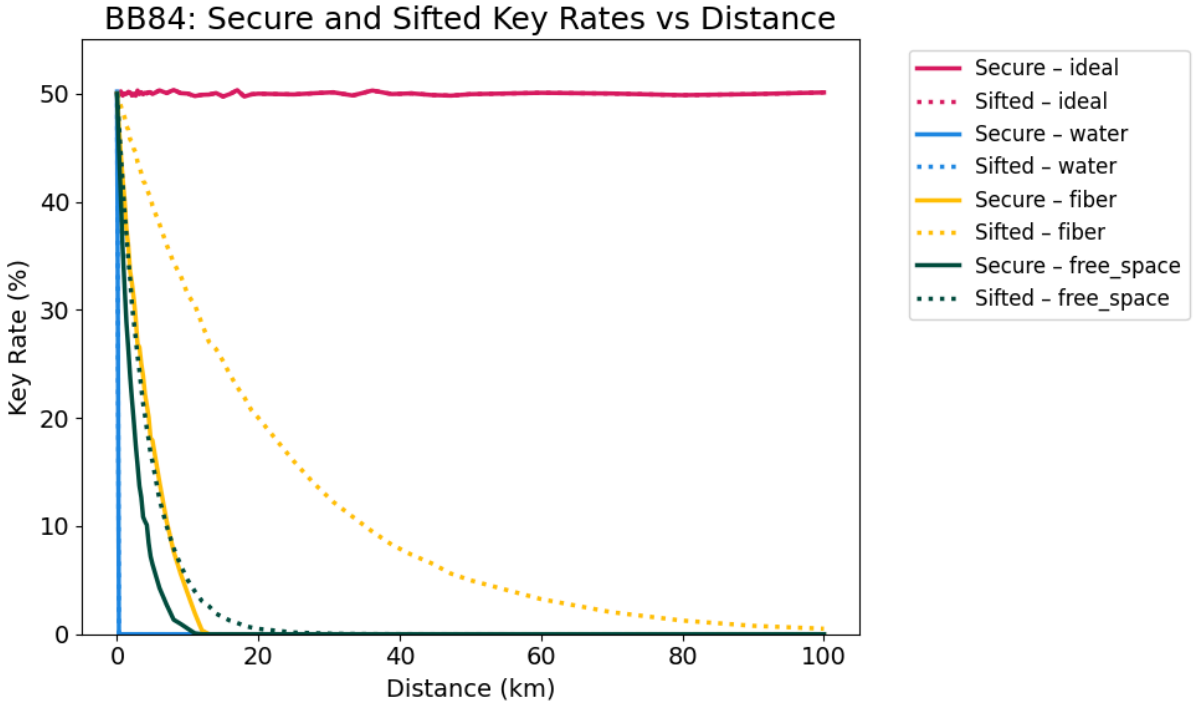
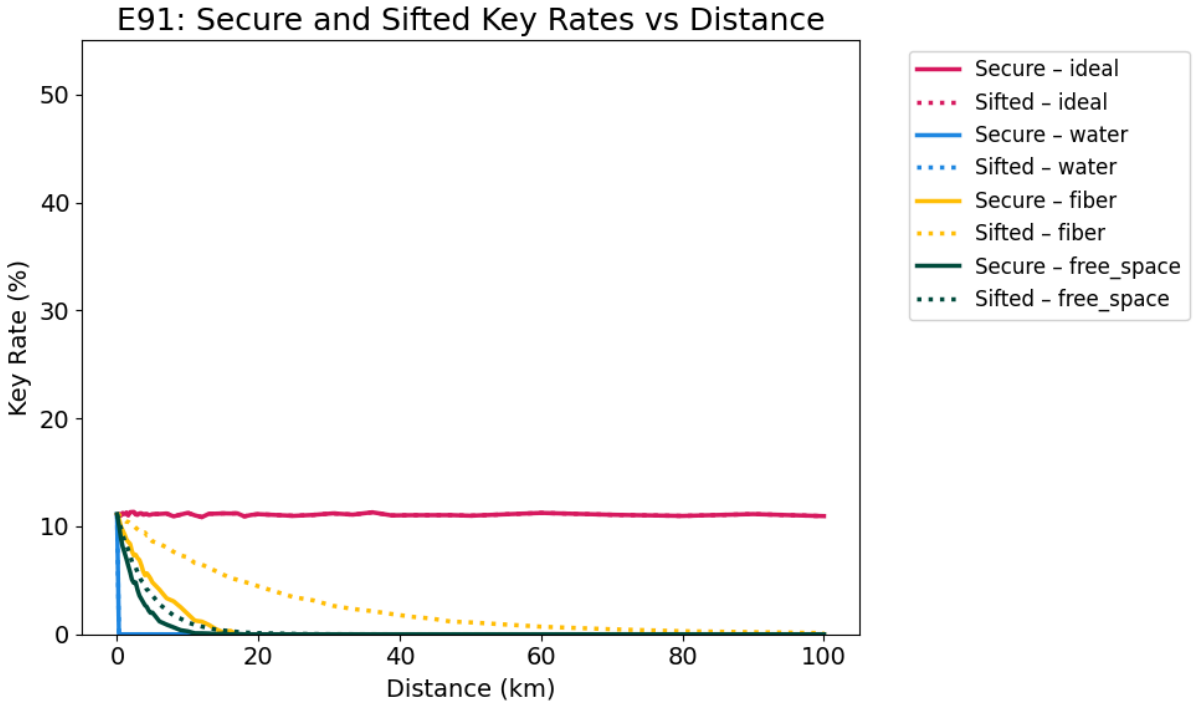


Figure 5. E91 — Secure and Sifted Key Rate vs. Distance (Without Eavesdropping)



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 minimal distances the difference between the two protocols is huge. 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 6-7. 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 remember, though, that this limit is not a strict boundary and may change in practical implementations.

Figure 6. BB84— Secure and Sifted Key Rate vs. Distance (Partial Eavesdropping — e = 0.5)

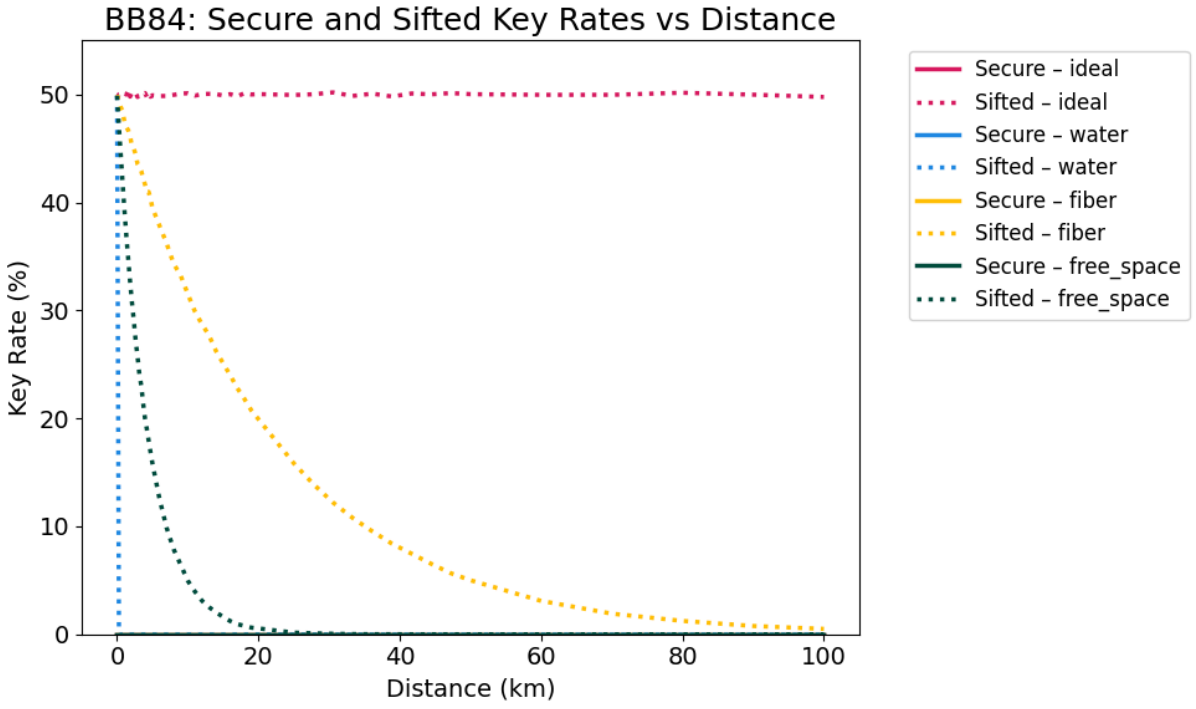
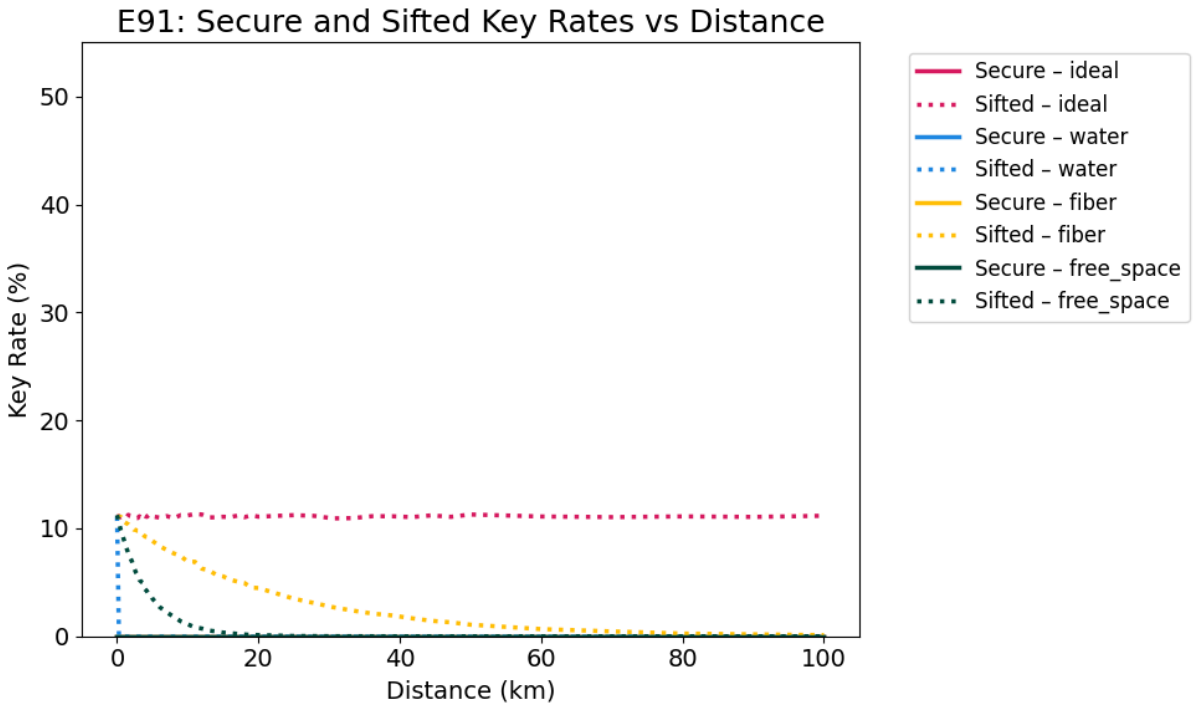


Figure 7. E91 — Secure and Sifted Key Rate vs. Distance (Partial Eavesdropping — e = 0.5)



In addition, a similar behavior was analysed under full eavesdropping (e = 1.0). Figures 8–9 depict, respectively, BB84 and E91's secure and sifted key rate in this condition.

Figure 8. BB84 — Secure and Sifted Key Rate vs. Distance (Full Eavesdropping — e = 1.0)

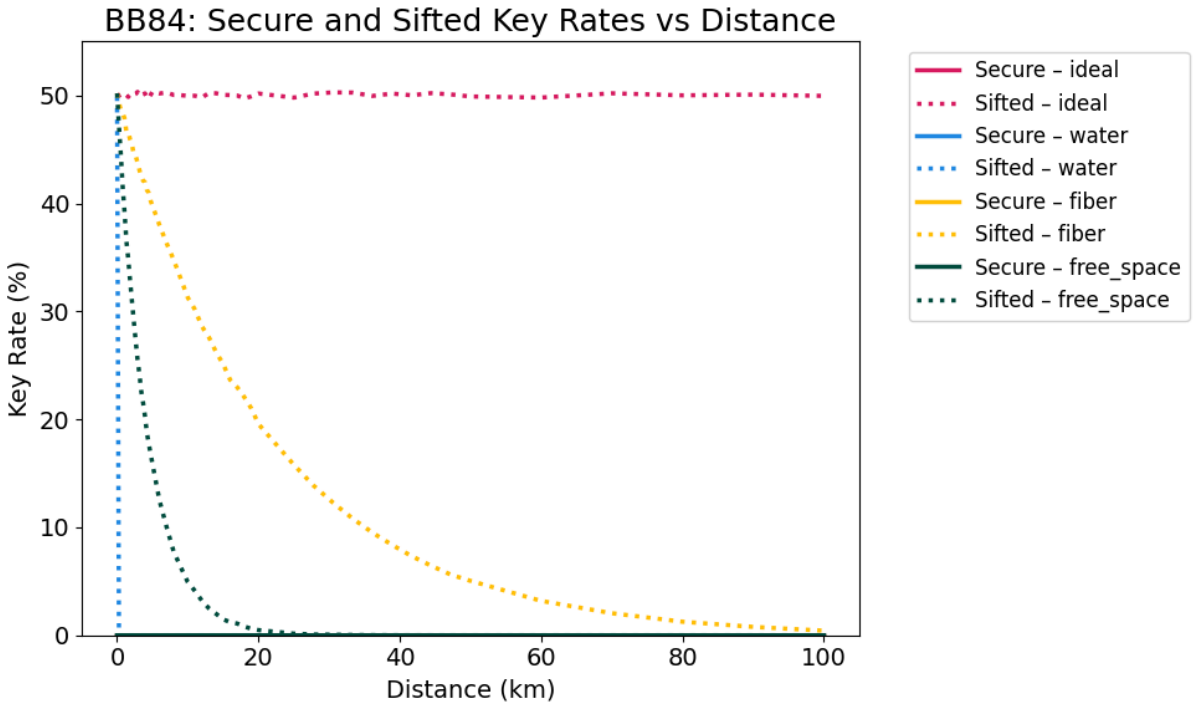
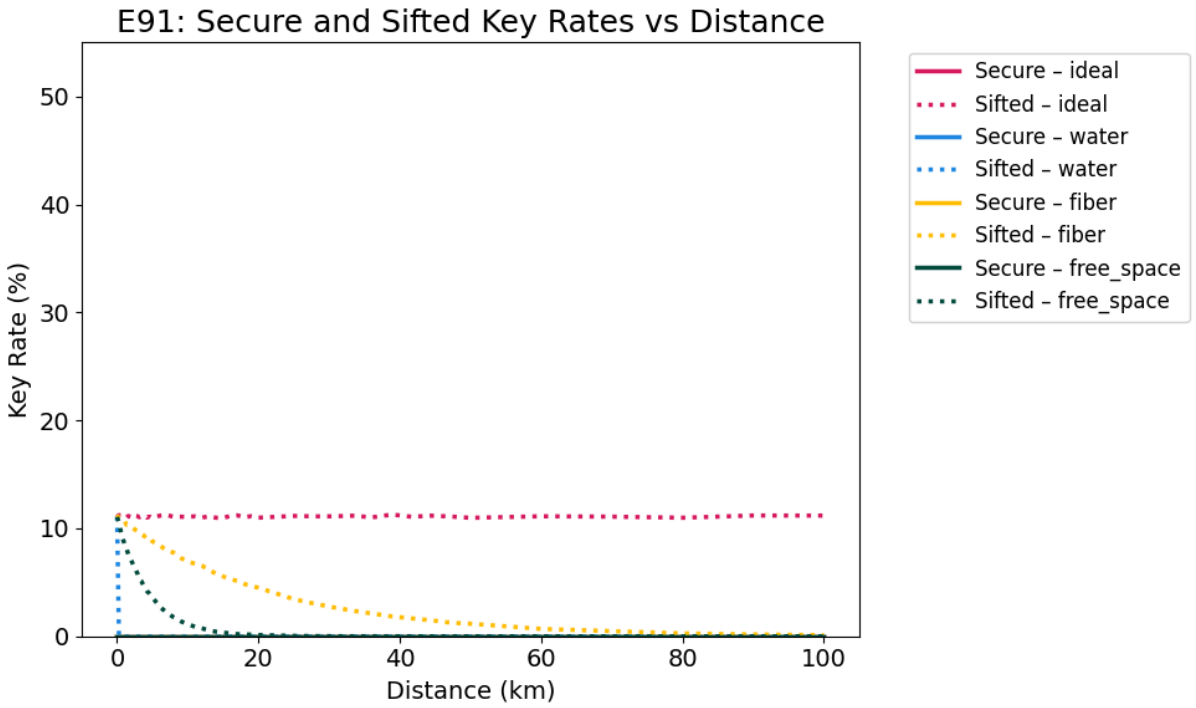


Figure 9. E91 — Secure and Sifted Key Rate vs. Distance (Full Eavesdropping — e = 1.0)



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 10-11 depict simulations of both protocols under no attack.

Figure 10. QBER vs. Distance (Without Eavesdropping)

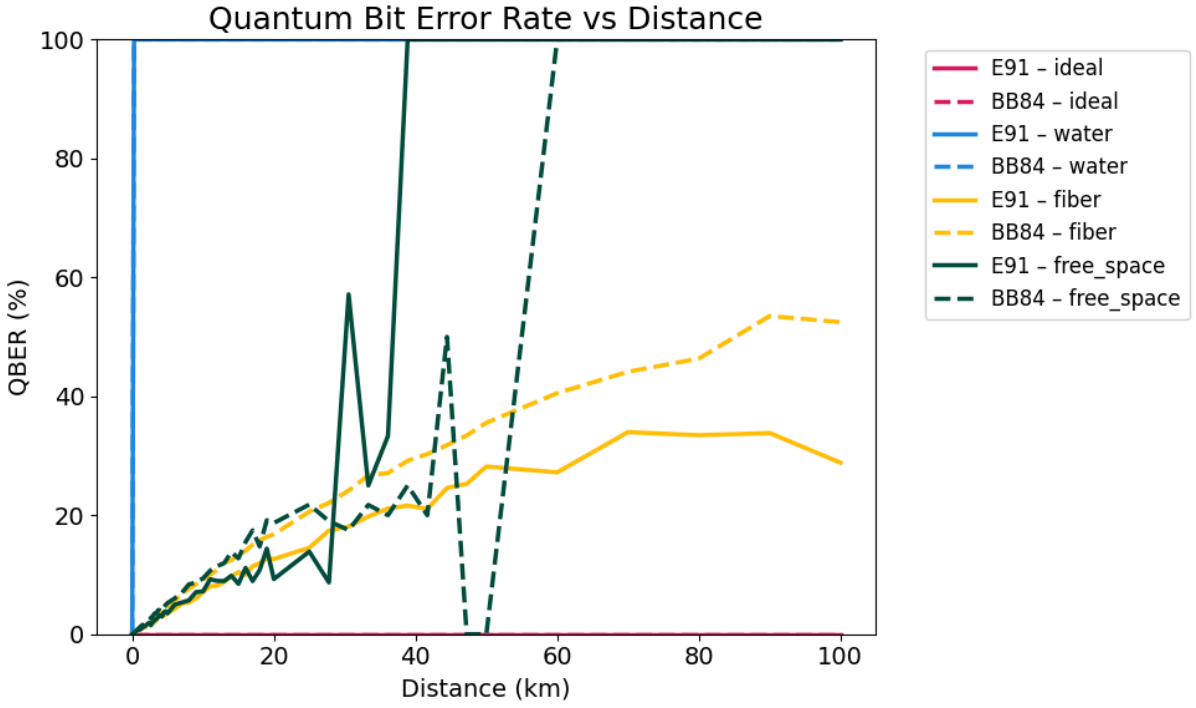
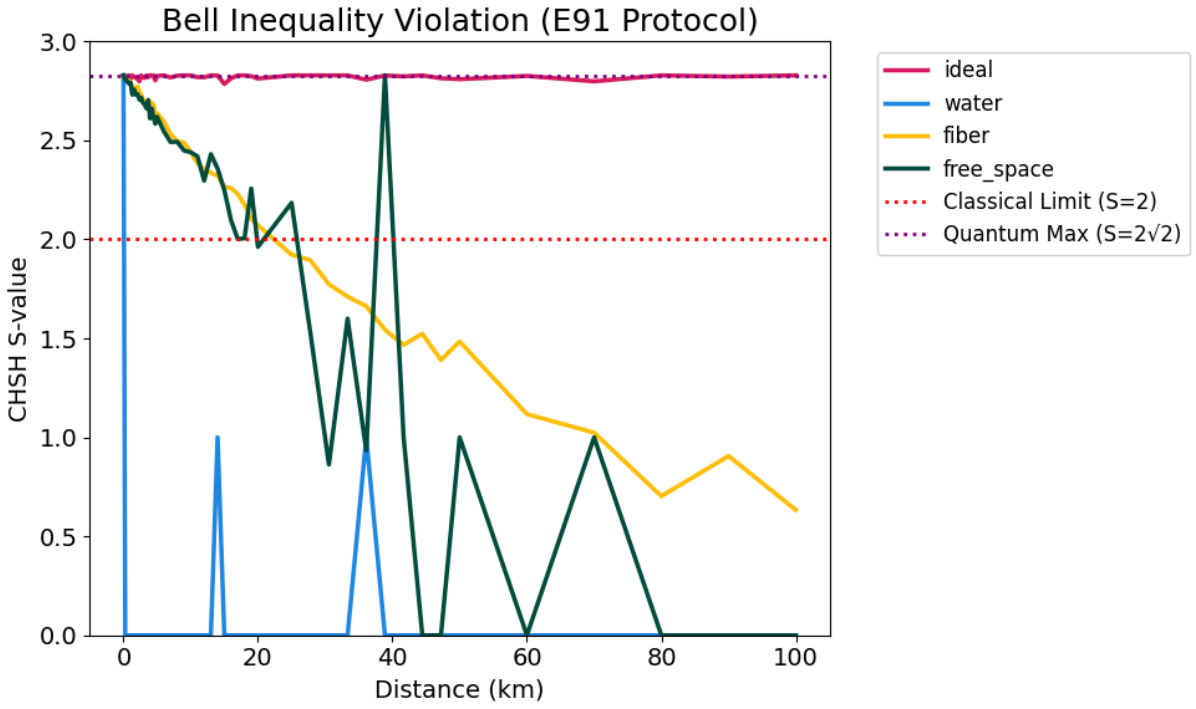


Figure 11. CHSH S-value vs. Distance (Without Eavesdropping)

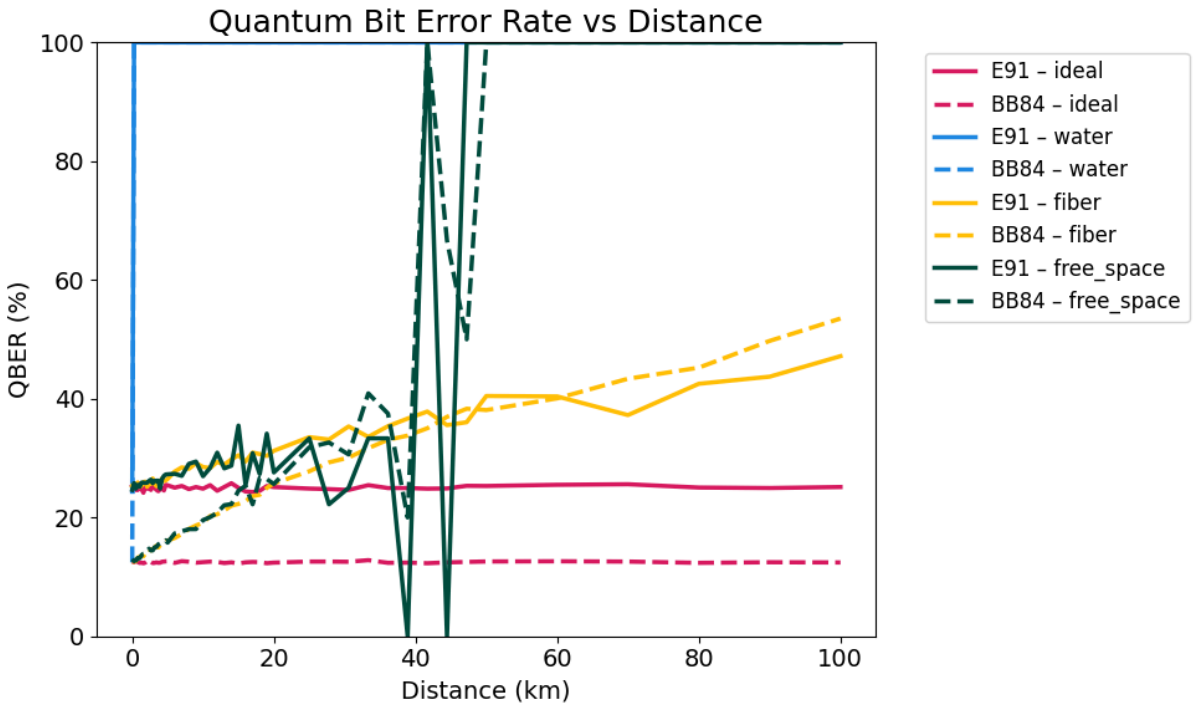


In a scenario with no eavesdroppers, both protocols displayed low QBER values at short distances. While QBER climbed steeply to 100% for the underwater channel, due to its highly imperfect conditions, the metric increased slowly and approximately at the same rate for both free-space and fiber-optic transmission 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 phenomena. 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.

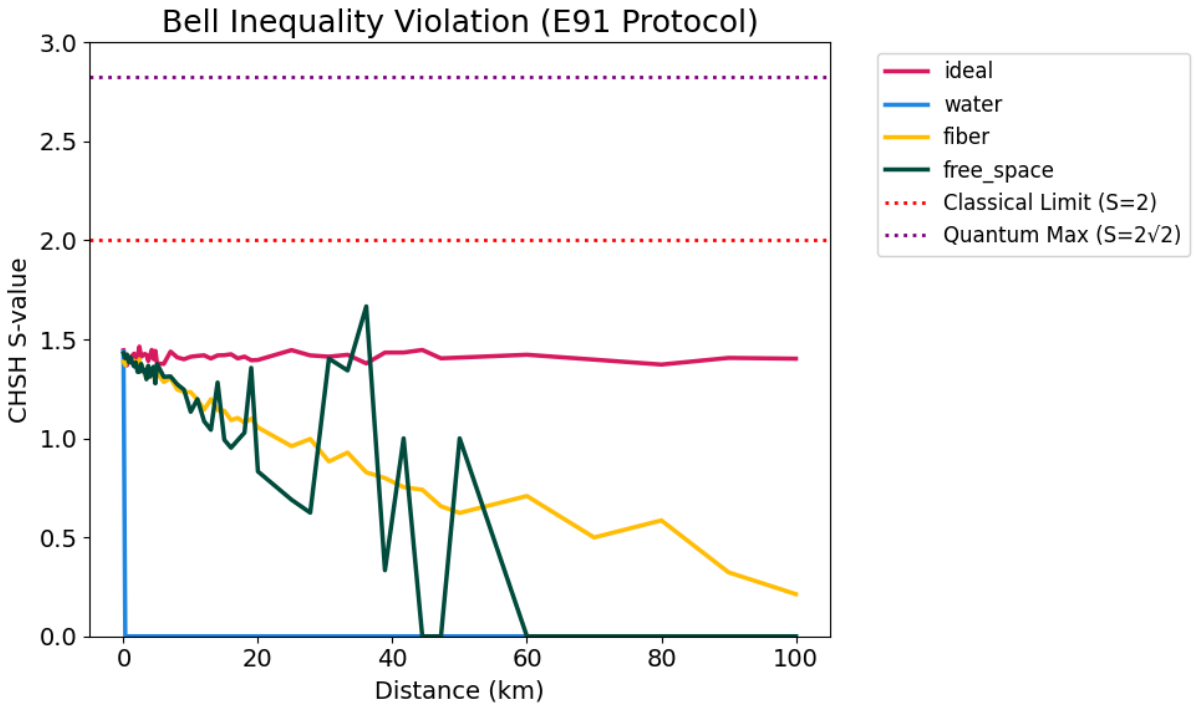
Figure 12. QBER vs. Distance (Partial Eavesdropping — e = 0.5)



Under partial eavesdropping, Figure 12 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, shown in Figure 2.

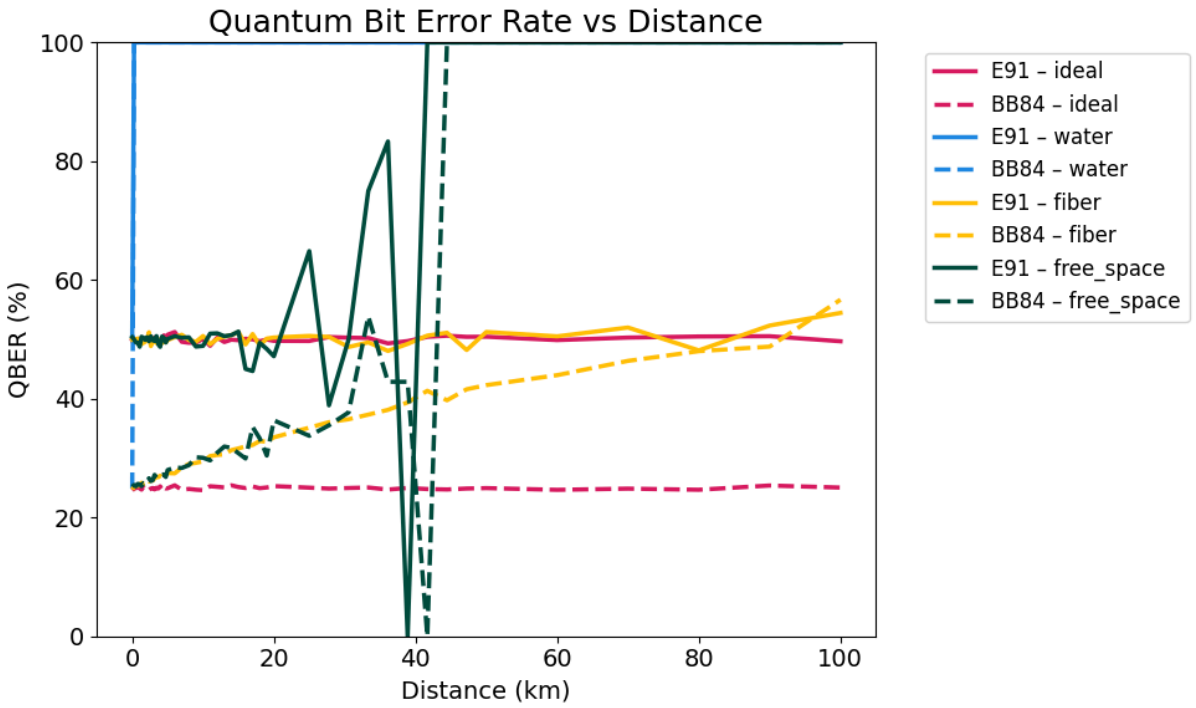
Figure 13. CHSH S-value vs. Distance (Partial Eavesdropping — e = 0.5)



For the CHSH S-values, our simulation demonstrated in Figure 13 that the eavesdropper interceptions dismantled quantum correlations. In fact, for all channels and distances experimented, this metric never surpassed the classical threshold.

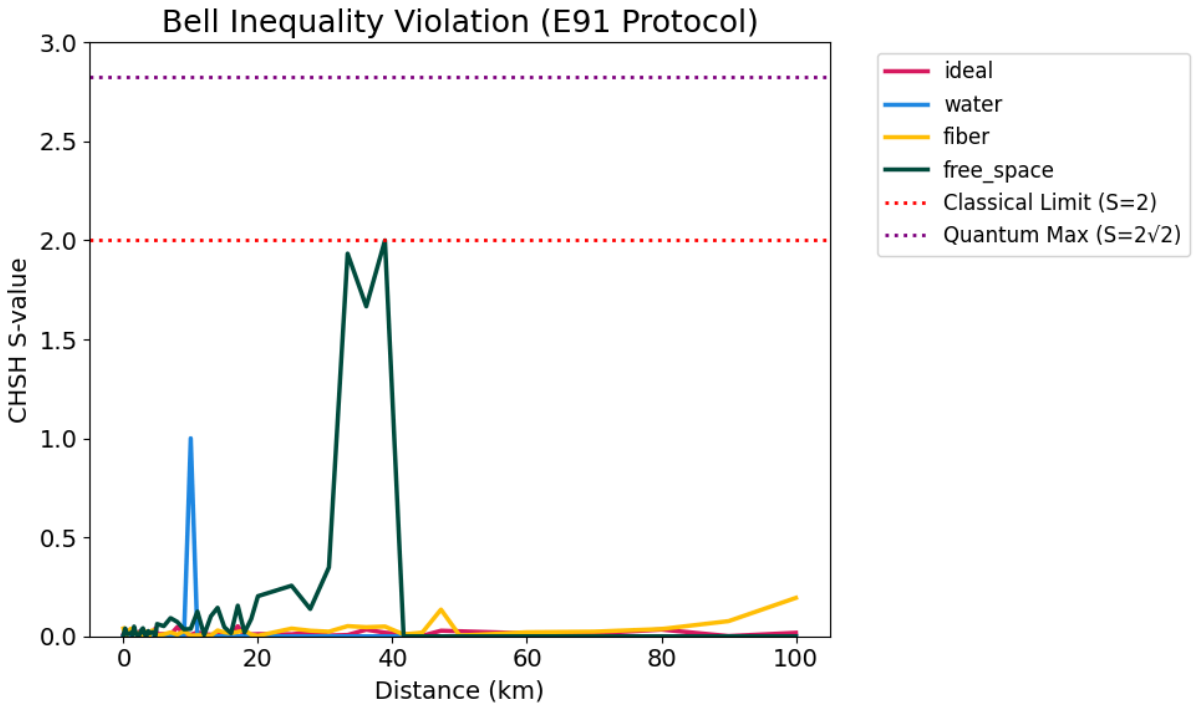
When the eavesdropper activity was increased to full interception (e = 1.0), the observed effects intensified across all metrics. As shown in Figure 14, QBER values exceeded 25% even at short communication distances. Interestingly, BB84 maintained noticeably lower QBER values than the E91 protocol up to approximately 80km, beyond which both protocols converged toward a QBER of 50%. Moreover, the free-space channel simulation continued to display anomalous results

Figure 14. QBER vs. Distance (Full Eavesdropping — e = 1.0)



In contrast to the partial eavesdropping scenario, the CHSH S-values under full attack showed a complete loss of correlations. As illustrated in Figure 15, all recorded values remained below 0.25, with the exception of a few statistical artifacts previously discussed.

Figure 15. 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 to be less susceptible to drastic QBER escalation under eavesdropping attacks. For E91, an additional metric — CHSH S values — served as an indicator or 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, the channel noise, not the protocol, limited secure entanglement-based QKD under those physical conditions.

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) is the next step to secure communication. Thus, practical implementation needs to take place in the near future to protect secret information from the threats that quantum computers' algorithms impose. 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.

Despite the result, it is crucial to recognize that E91 has theoretical advantages not captured by the performance metrics analyzed here. 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, continued research into overcoming the fragility of entanglement in E91-like protocols is essential for achieving next-generation quantum networks.

With these insights, we believe that future research and practical implementations have valuable information 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. So, bridging the gap between theoretical and practical quantum communication is essential to unveil the full potential of this technology.

5 - Bibliography

1. Agrawal, G. P. (2012). *Fiber-Optic Communication Systems*. John Wiley & Sons.
2. 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
3. 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
4. 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
5. Bernstein, D. J., Heninger, N., Lou, P., & Valenta, L. (2017, June 4). Post-quantum RSA. https://doi.org/10.1007/978-3-319-59879-6_18
6. Bhatia, V., & Ramkumar, K. R. (2020). An Efficient Quantum Computing technique for cracking RSA using Shor's Algorithm. *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*, 89–94. https://doi.org/10.1109/ICCCA49541.2020.9250806
7. 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
8. 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

9. 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
10. Czerwinski, A., & Czerwinska, K. (2022). Statistical Analysis of the Photon Loss in Fiber-Optic Communication. *Photonics*, *9*(8), Article 8. https://doi.org/10.3390/photonics9080568
11. Díaz, F., & Lenin, J. (2014, March 28). *Geração de emaranhamento de polarização entre pares de fótons no regime de fentossegundos* [Master's thesis]. Universidade Federal de Pernambuco. https://repositorio.ufpe.br/handle/123456789/18296
12. 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
13. Maloo, S. (n.d.). *Quantum Cryptography and Communication: Protocols, Limitations, and Solutions.*
14. 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), 076106. https://doi.org/10.1117/1.OE.57.7.076106
15. Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information* (10th anniversary ed.). Cambridge University Press.
16. 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), 057901. https://doi.org/10.1103/PhysRevLett.92.057901
17. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134. https://doi.org/10.1109/SFCS.1994.365700
18. 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
19. Teich, M. C., & Saleh, B. (2007). *Fundamentals of photonics* (Vol. 2). Wiley.
20. 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), 7. https://doi.org/10.1038/ncomms1005
21. 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
22. 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), nwaf147. https://doi.org/10.1093/nsr/nwaf147

23. 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

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

7 - Acknowledgements

We wish to thank [mentor name redacted] 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 [mentor name redacted] 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 which 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 was fundamental for both the writing and the empirical process. Therefore, we are extremely grateful to everyone involved.

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

Changes are highlighted in yellow

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 optic 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, Quantum Communication, Communication Protocols, BB84, E91.

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, since the development of quantum computers and algorithms, the security of many traditional cryptographic methods has been fundamentally threatened. 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 quantum mechanics' uncertainty principle and no-cloning theorem (Nielsen & Chuang, 2010). By using two conjugated 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 bases, and assuming a noiseless channel, Bob will measure the correct bit. But, if Alice sends a photon encoded in the rectilinear basis and Bob chooses the diagonal, quantum uncertainty dictates a 50% probability of obtaining the correct value. Then, using a classical insecure channel, Alice and Bob can 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 non-compatible 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. Then, to verify the security of the quantum channel, they can compare a subset of their measurements' results to check for violations. If Bell's inequalities are satisfied rather than violated, it implies 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 was 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 on 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 sifting 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 travelling 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 law (Teich & Saleh, 2007) can be employed:

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

where $I(d)$ denotes the intensity of light after propagating a distance d (km) through an absorbing or scattering medium, I_0 represents the initial power and α (dB/km) the attenuation coefficient (Czerwinski & Czerwinska, 2022). Then, to get 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 decibels 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 on 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 kilometers, 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:

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

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

For this simulation typical values of λ 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 approximate as randomizing processes. If future experimental data shows bias toward particular error axes, the model can be replaced by a Pauli channel with pX, pY, pZ fit from data.

Table 2 : Depolarization length (λ), measured 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 has 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,

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

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

Then, these photons travel through noisy and lossy channels before reaching Bob's randomly chosen polarization bases and single-photon detectors. After, 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 are 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 $\{ai\}$ with $ai \in \{0, 1\}$ 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 BB84 protocol

Polarization	**Basis**	**Bit Representation**
0	Z (Rectilinear)	0
π/2 (90°)	Z (Rectilinear)	1
π/4 (45°)	X (Diagonal)	0
3π/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) ∈ {0, 1}. Similarly, a photon suffers depolarization, represented by the application of random Pauli X, Y, or Z errors with equal probability as described in Table 4, if k is smaller than the depolarization probability.

Table 4. 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.*

After channel effects are applied, Bob receives the photons and measures each one in a randomly chosen basis. He generates a basis string {ϕi} with ϕi ∈ {Z, X} and length n. For each incoming photon, Bob uses the corresponding basis ϕi to perform his measurement. For example, if Bob detects a photon polarized in the rectilinear basis (horizontal |H⟩ (0) or vertical |V⟩ (π/2)) and measures its value with the Z basis, he deterministically records either 0 for |H⟩ or 1 for |V⟩. 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⟩ — defined by Equation (5)) when the photon is actually |H⟩ is given by the squared overlap (Born rule) (Nielsen & Chuang, 2010):

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

The probabilities of obtaining bit 0 or 1 when measured in the Z (rectilinear) or X (diagonal) basis, for each of the four polarization states of a photon, are shown in Table 5.

Table 5. Measurement outcome probabilities for BB84 states in the Z and X bases.

Prepared State	**Z Basis: *P*(0), *P*(1)**	**X Basis: *P*(0), *P*(1)**
|H⟩ (0)	1.0, 0.0	0.5, 0.5
|V⟩ (π/2)	0.0, 1.0	0.5, 0.5
|A⟩ (π/4)	0.5, 0.5	1.0, 0.0
|D⟩ (3π/4)	0.5, 0.5	0.0, 1.0

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 with 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, it is introduced in the communication channel, after all loss and noise is applied, an observer, Eve. 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. Table 6 and Table 7 show an example of the protocol without and with eavesdropping, respectively.

Table 6. 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	Z	Z	X	X	Z	X	Z	X	X	Z

Detector										
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 incorrect basis		**1**		**0**	**1**				**0**	**0**

Table 7. 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 6 — when no eavesdropper was present — all matching bases correspond to matching bits. However, in Table 7, after introducing eavesdropping, the bits in positions b4 and b8 (which share the same bases) are corrupted. 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 an entangled pair. 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).

Similarly 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 individual, Victor, equally distant to Alice and Bob sends, to both parties, photons prepared in the maximally entangled singlet state

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

Next, Alice and Bob independently select one of three measurement bases (angles) randomly, with uniform probabilities. Table 8 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 is reserved for key generation. In this simulation, the basis that corresponds to a measurement angle of π/2 is used to generate the final key.

Table 8. Possible Measurement Bases for Alice and Bob

Basis Index	**Alice's bases**	**Bob's bases**
0	π/2	π/2
1	0	π/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) $\in \{0, 1\}$. 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 ($|0\rangle$) or -1 ($|1\rangle$), 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

$$P(b = -a \mid \theta_A = \theta_B) = 1, \quad (9)$$

where a,b and θA, θB represent Alice and Bob's measurement outcomes and selected angles, respectively. It is also important to mention that the singlet state $|\Psi\rangle$ defines a 50% probability of measuring each outcome for both parties, because the probability of Alice measuring +1 is given by

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

and after this measurement, $|\Psi\rangle$ collapses to just

$$|\Psi^-\rangle = |01\rangle, \quad (11)$$

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):

$$E(\theta_A, \theta_B) = P_{++} + P_{--} - P_{+-} - P_{-+}, \quad (12)$$

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:

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

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

$$E(\theta_A, \theta_B) = -\cos[2(\theta_A - \theta_B)], \quad (14)$$

finally giving the expression in the form:

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

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. Table 9 shows more examples.

Table 9. Equation (15) applied to various measurement angles combinations

Bits	θA (Alice)	θB (Bob)	θA − θB	− cos[2(θA − θB)]	P_{same} **(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

In sum, step three of the simulation starts with Alice measuring the value $a \in \{+1, -1\}$ 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 $(k) \in \{0, 1\}$. If P_{same} 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 offer 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.

Quantum Bit Error Rate (QBER) is one of the most critical metrics of quantum key distribution protocols. By measuring the fraction of bits of the sifted key that differ between Alice and Bob, the communication's security can be evaluated. Therefore, it is given by

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

where N is the total number of bits in the sifted key; *ai*, *bi* are the i-th bit from Alice and Bob, respectively; δ(ai≠bi) is a function that returns 1 if $a_i \neq b_i$ and 0 otherwise. While a low QBER indicates stronger security guarantees, a QBER above a certain threshold points to the presence of malicious interference or excessive noise.

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: 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.

The sifted key rate refers to the proportion of raw key bits that remain after Alice and Bob discard all bits for which they used incompatible measurement bases. Thus, it is an important metric to evaluate the effectiveness of a protocol: a higher sifted rate means more usable bits per transmission — which makes it more practical for real-world implementations.

In contrast, the secure key rate represents the portion of the sifted key that can be securely used. Since some of the bits in the sifted key may be compromised by noise, losses and potential eavesdropping, it is important to discard them to prevent leaking

valuable information. Therefore, the secure key rate reflects the protocol's real-world viability by considering just the net amount of safe key material. Its calculation is given by (Shor & Preskill, 2000):

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

where R_{sifted} is the sifted rate and H_2 is a binary entropy function:

$$H_2(p) = -p\, log_2\, p - (1-p) log_2(1-p). \quad (18)$$

The key length refers to the total number of secure bits generated after all post-processing steps. Similarly to the sifted key rate metric, the key length is particularly relevant for assessing the practical usability of the protocol. Since most cryptographic applications require large key lengths to be effective, the protocol's ability to generate long, secure bit strings is a crucial factor for in-the-field quantum communication.

Lastly, the CHSH (Clauser–Horne–Shimony–Holt) S-Value (Clauser, Horne, Shimony, & Holt, 1969) is used to evaluate the security of quantum communication based on the E91 protocol exclusively. It quantifies the strength of the correlations between Alice and Bob's outcomes. By computing four correlation coefficients — described by Equation (12) — for which Alice and Bob used different measurement angles, the S-Value is obtained:

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

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√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).

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 10 presents these intervals and their respective amount of sampling points.

Table 10. 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

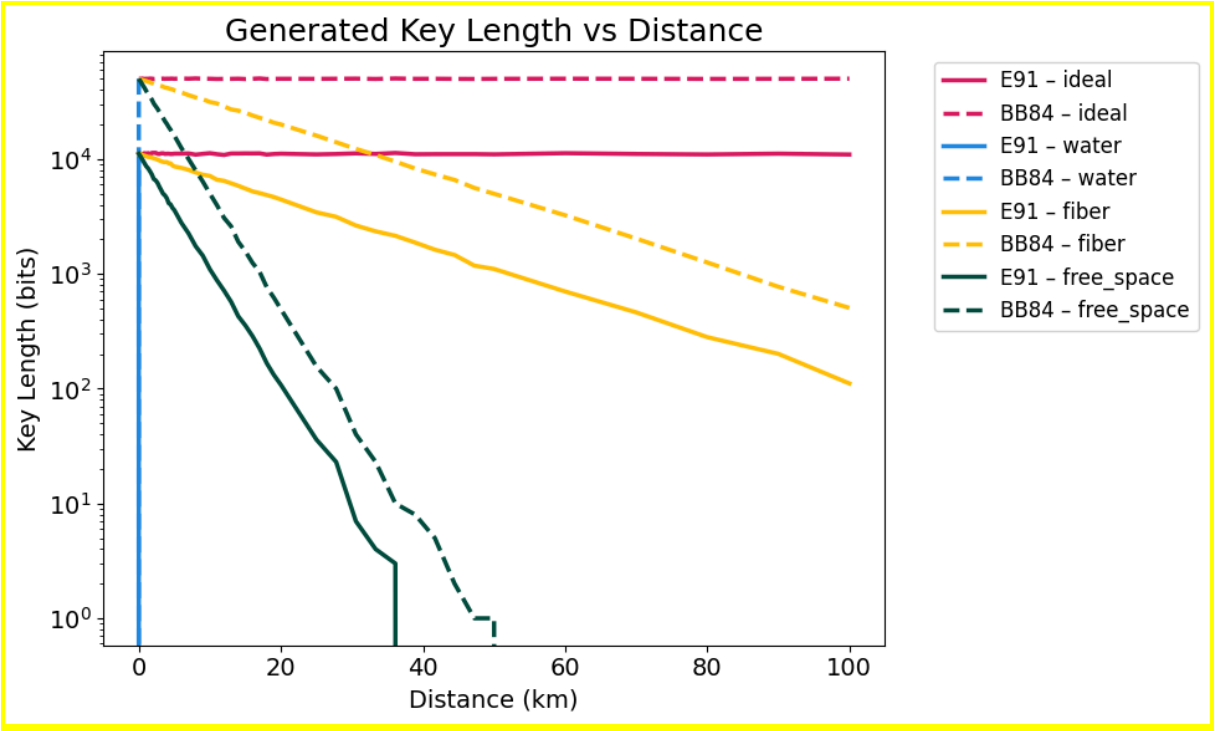
This section is divided into four subsections. Each of the first three subsections is dedicated to describe the results of both protocols under each simulated quantum channel. Subsection **(3.1)** presents the results for the generated key length across all channels. Subsection **(3.2)** shows the secure 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), 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 achieved 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 was 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. Nonetheless, for completeness, the results for 50% and 100% eavesdropping are presented, respectively, in Figures 2–3.

Figure 2. Key Length vs. Distance (Partial Eavesdropping — e = 0.5)

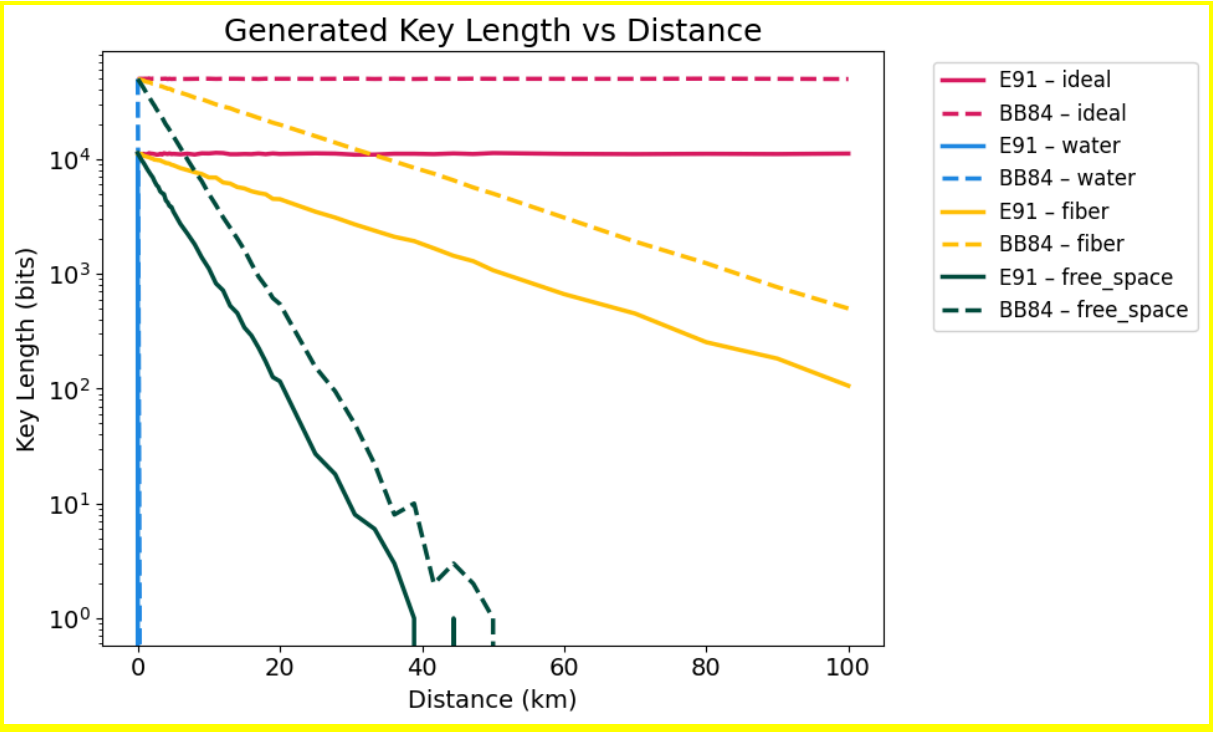
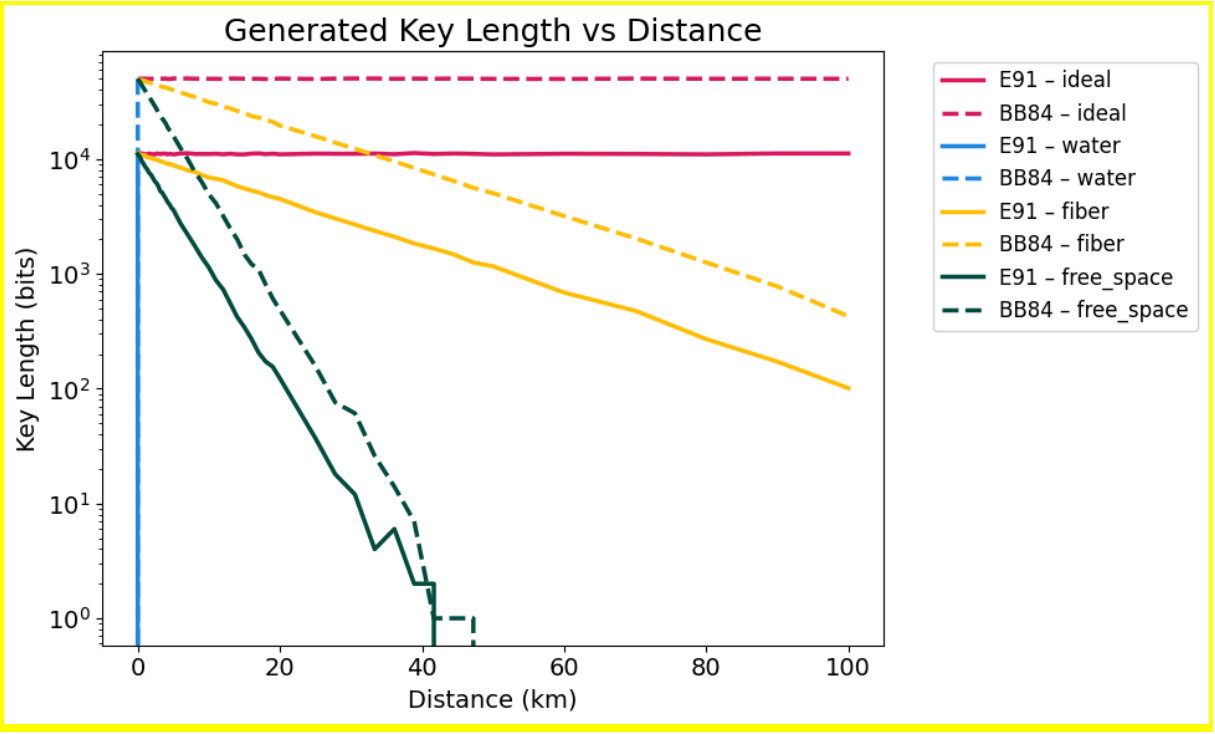


Figure 3. Key Length vs. Distance (Full Eavesdropping — $e = 1.0$)



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 4

shows the secure and sifted key rate as a function of distance for the BB84 protocol, under ideal, fiber-optic (fiber), underwater (water), free-space transmission. Figure 5 depicts the same metrics but for the E91 protocol.

Figure 4. BB84 — Secure and Sifted Key Rate vs. Distance (Without Eavesdropping)

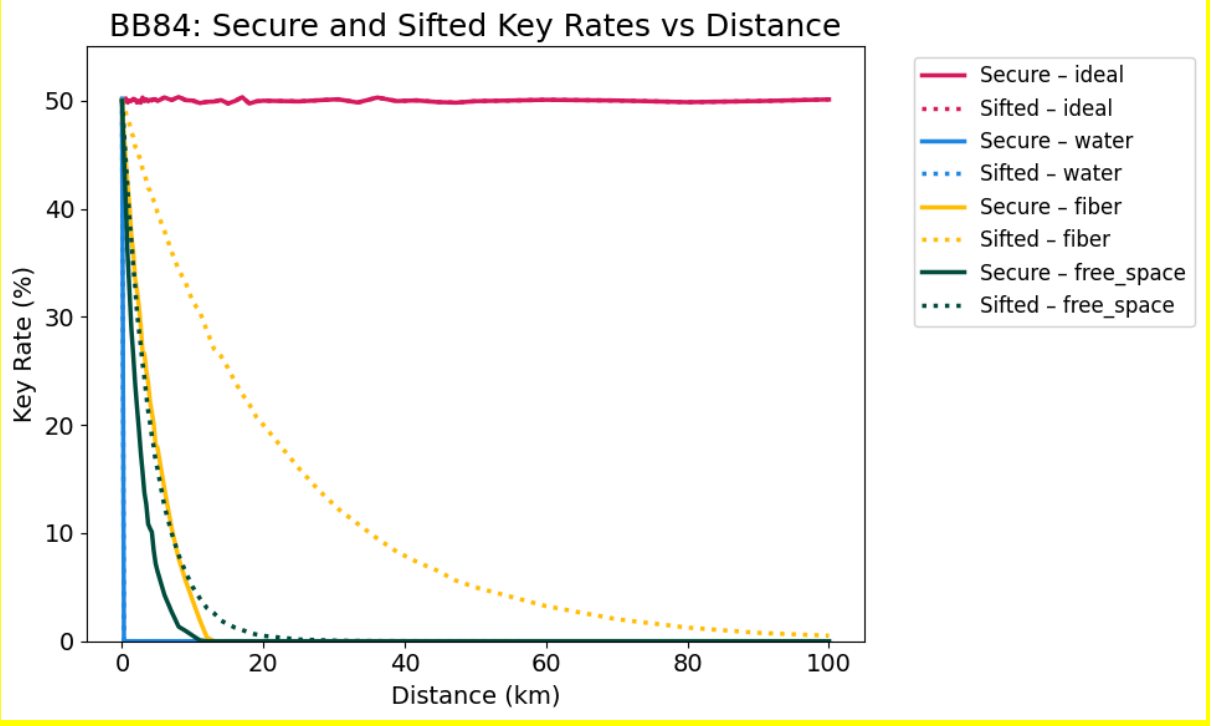
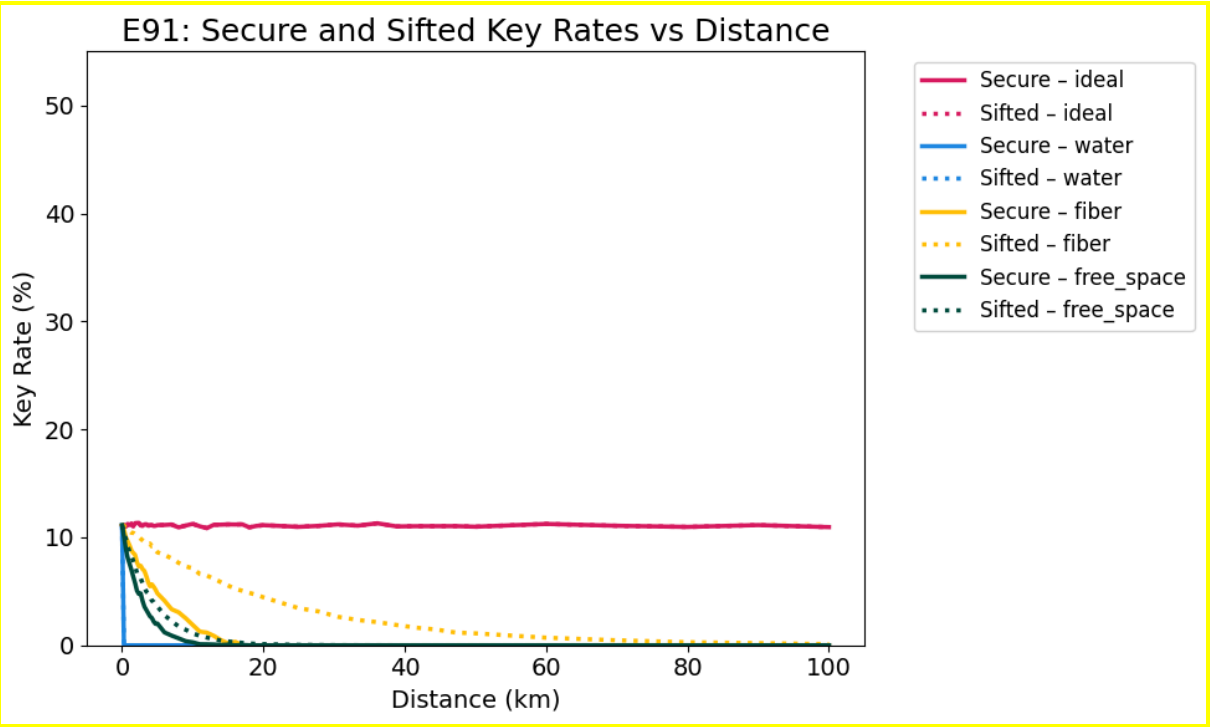


Figure 5. E91 — Secure and Sifted Key Rate vs. Distance (Without Eavesdropping)



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 minimal distances the difference between the two protocols is huge. 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 6-7. 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 remember, though, that this limit is not a strict boundary and may change in practical implementations.

Figure 6. BB84— Secure and Sifted Key Rate vs. Distance (Partial Eavesdropping — e = 0.5)

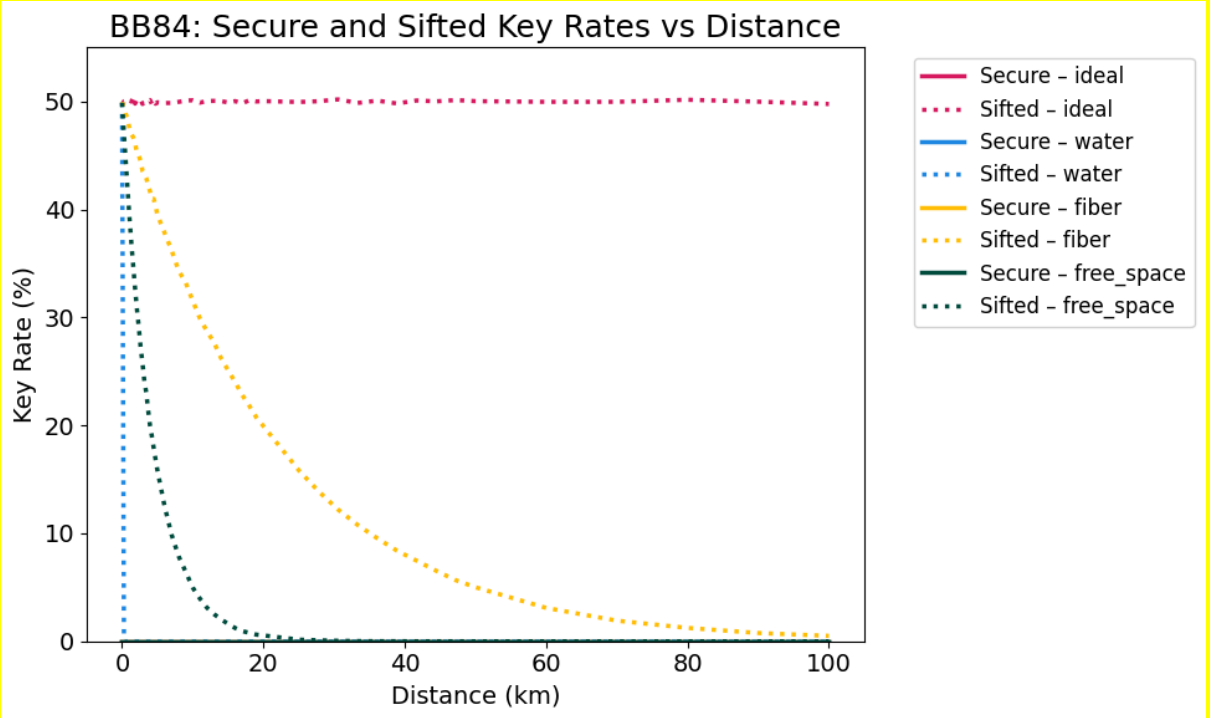
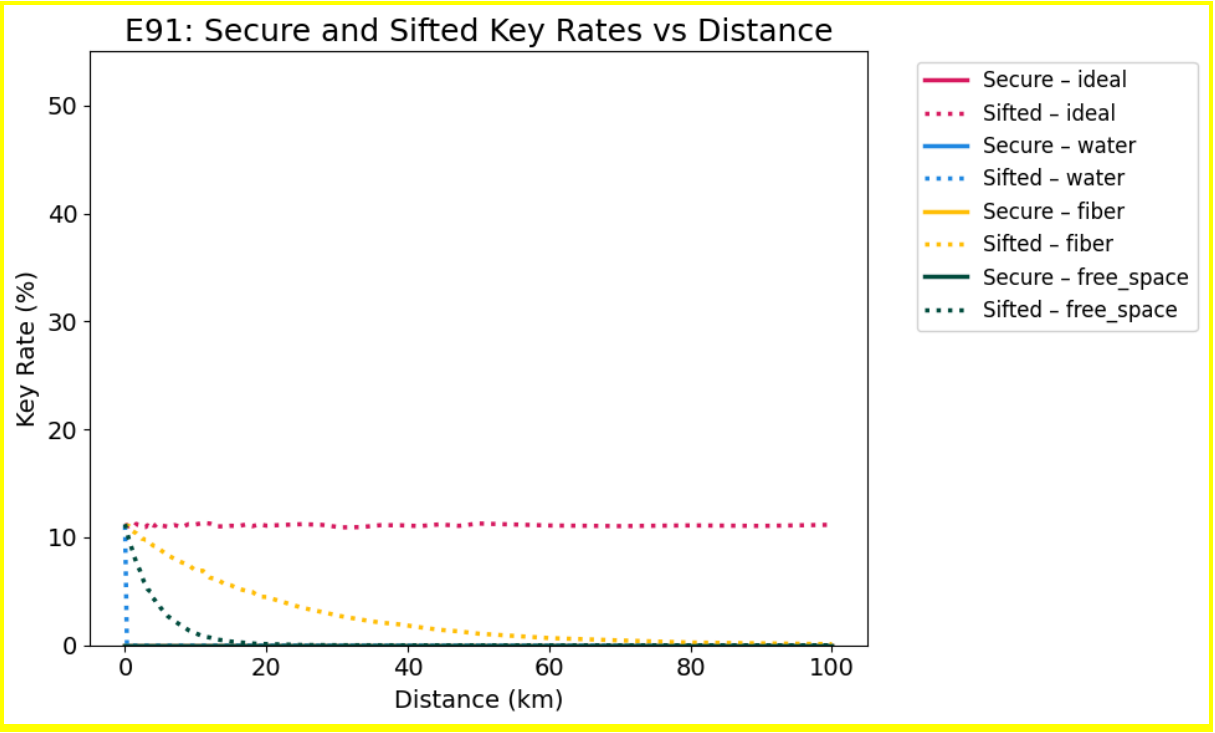


Figure 7. E91 — Secure and Sifted Key Rate vs. Distance (Partial Eavesdropping — e = 0.5)



In addition, a similar behavior was analysed under full eavesdropping (e = 1.0). Figures 8–9 depict, respectively, BB84 and E91's secure and sifted key rate in this condition.

Figure 8. BB84 — Secure and Sifted Key Rate vs. Distance (Full Eavesdropping — e = 1.0)

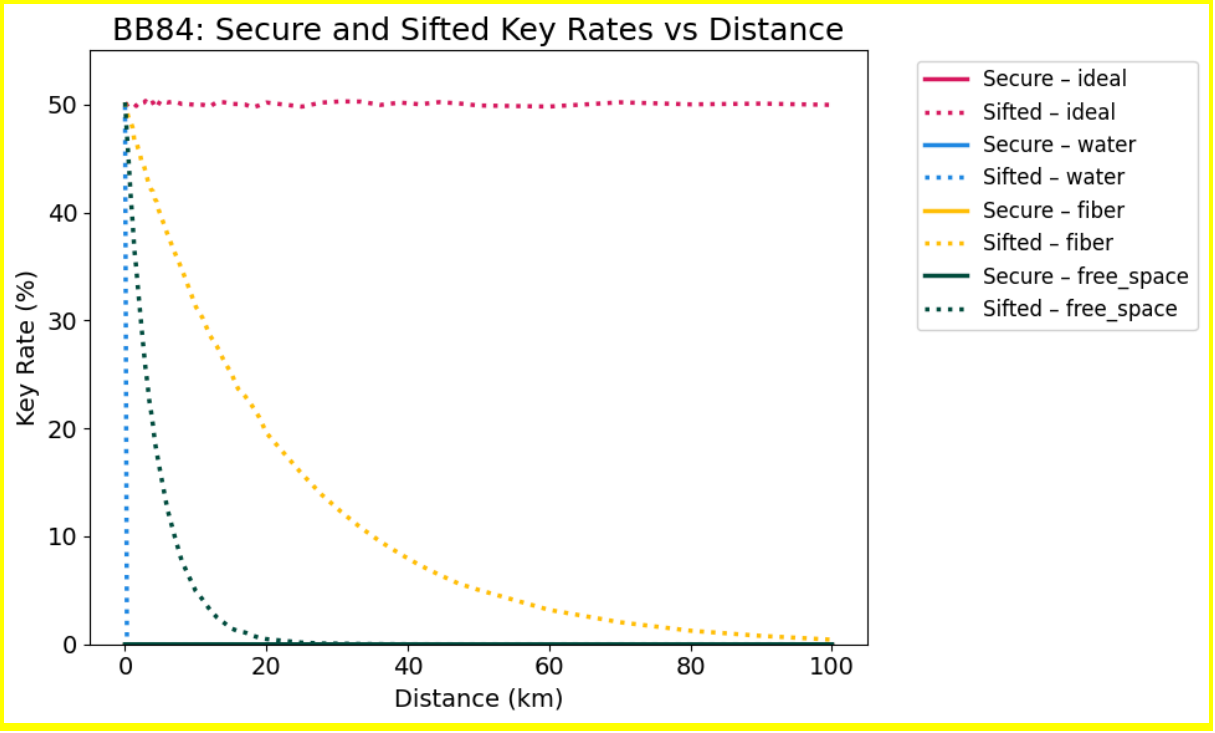
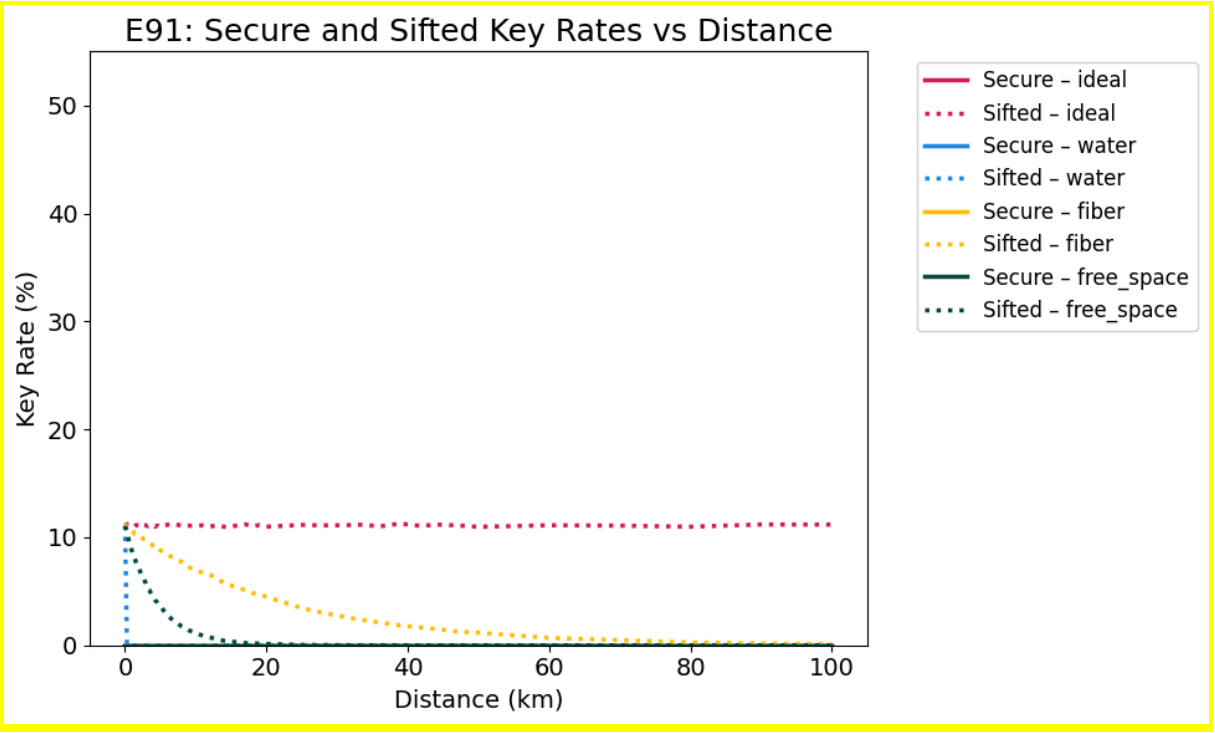


Figure 9. E91 — Secure and Sifted Key Rate vs. Distance (Full Eavesdropping — e = 1.0)



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 10-11 depict simulations of both protocols under no attack.

Figure 10. QBER vs. Distance (Without Eavesdropping)

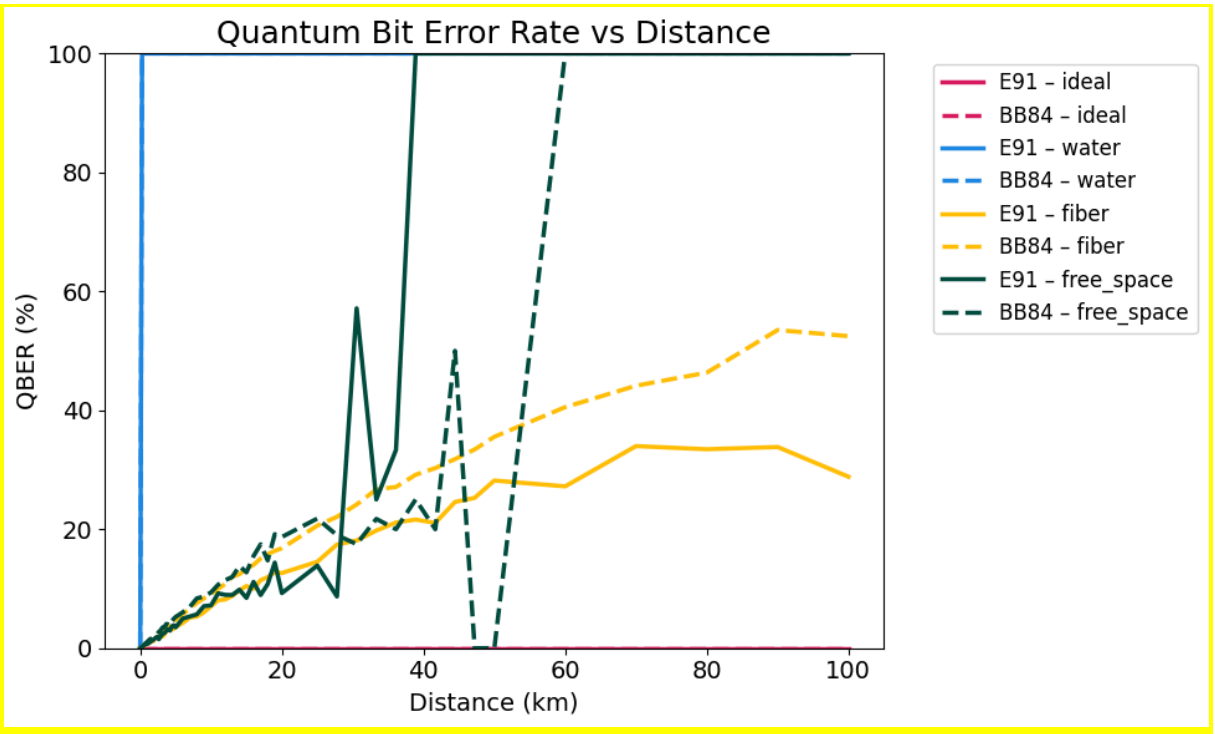
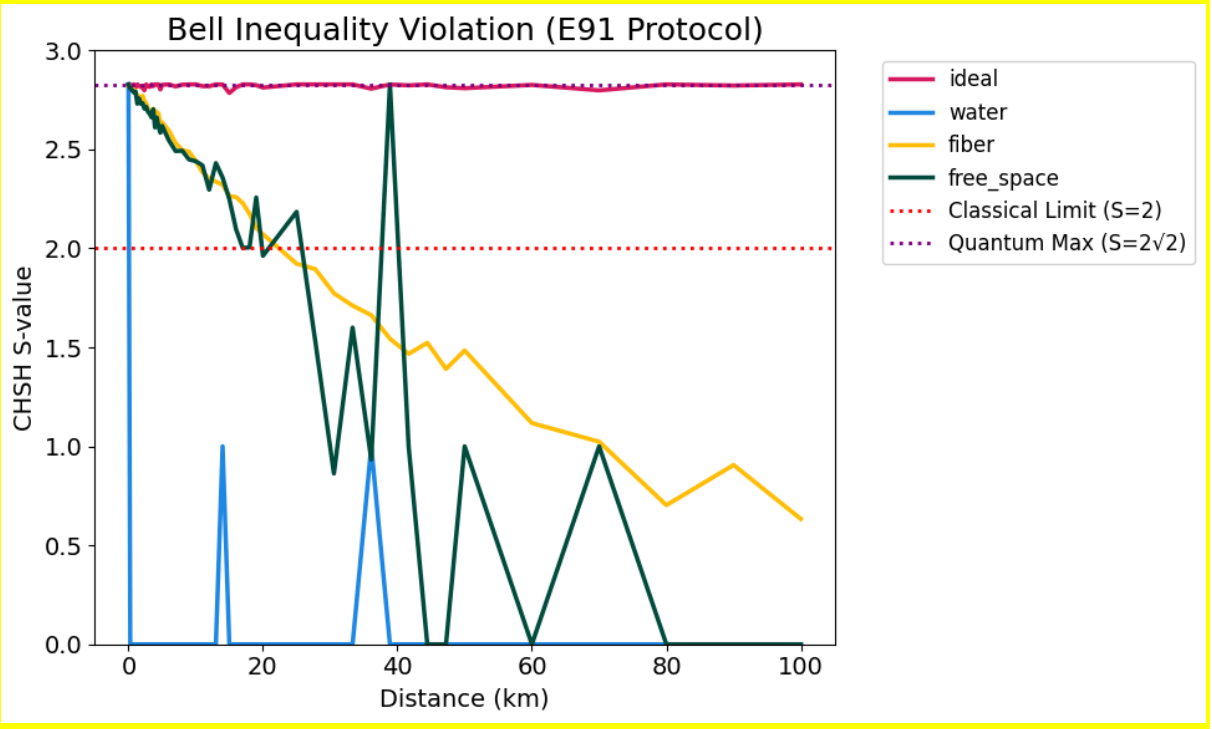


Figure 11. CHSH S-value vs. Distance (Without Eavesdropping)

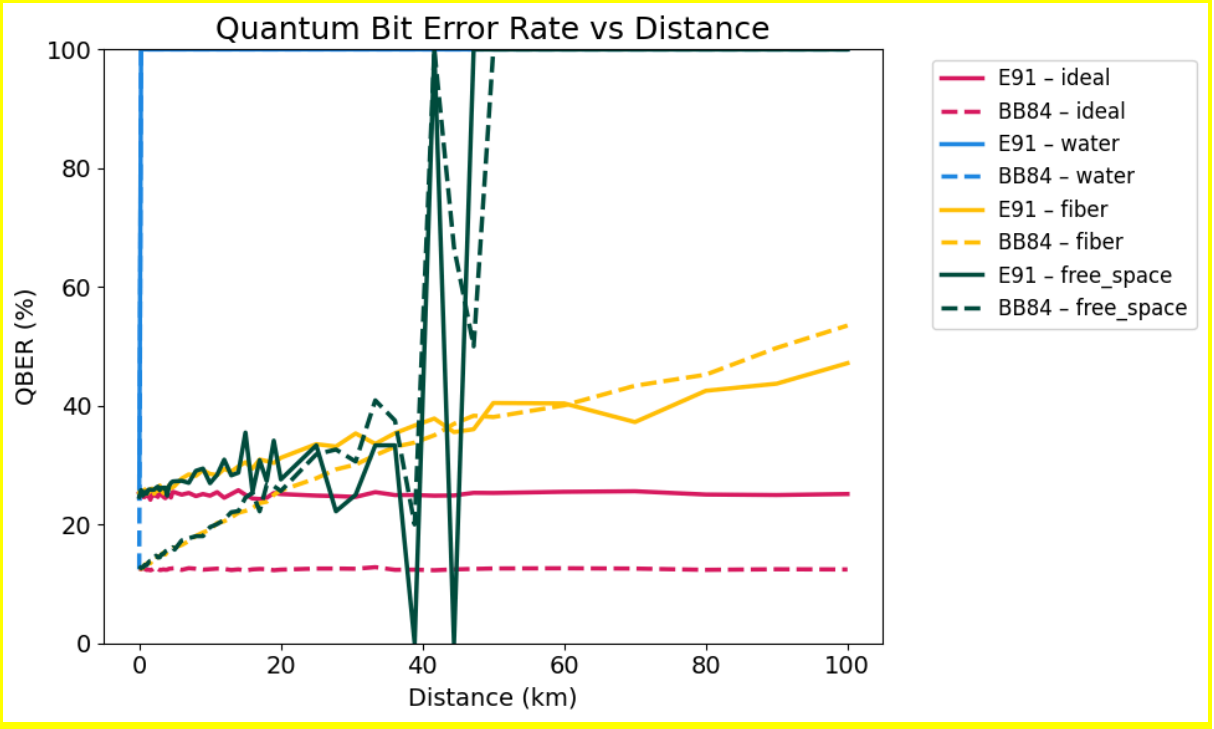


In a scenario with no eavesdroppers, both protocols displayed low QBER values at short distances. While QBER climbed steeply to 100% for the underwater channel, due to its highly imperfect conditions, the metric increased slowly and approximately at the same rate for both free-space and fiber-optic transmission 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 phenomena. 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.

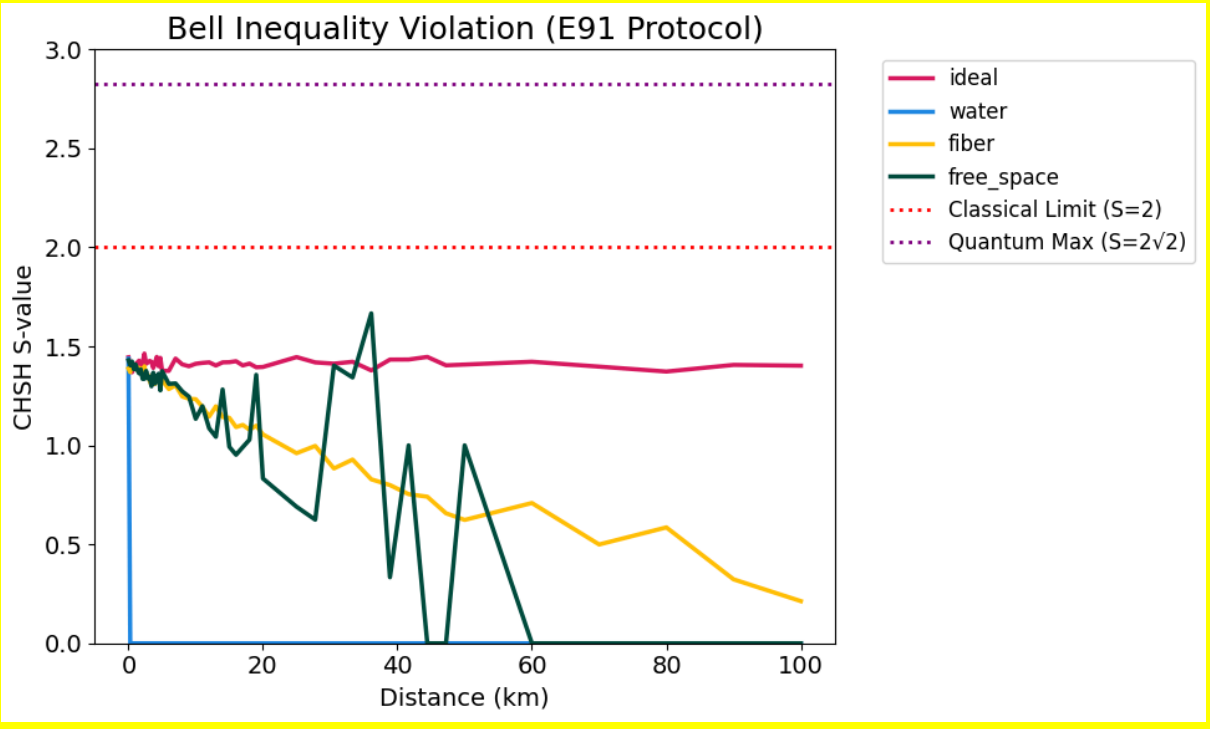
Figure 12. QBER vs. Distance (Partial Eavesdropping — e = 0.5)



Under partial eavesdropping, Figure 12 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, shown in Figure 2.

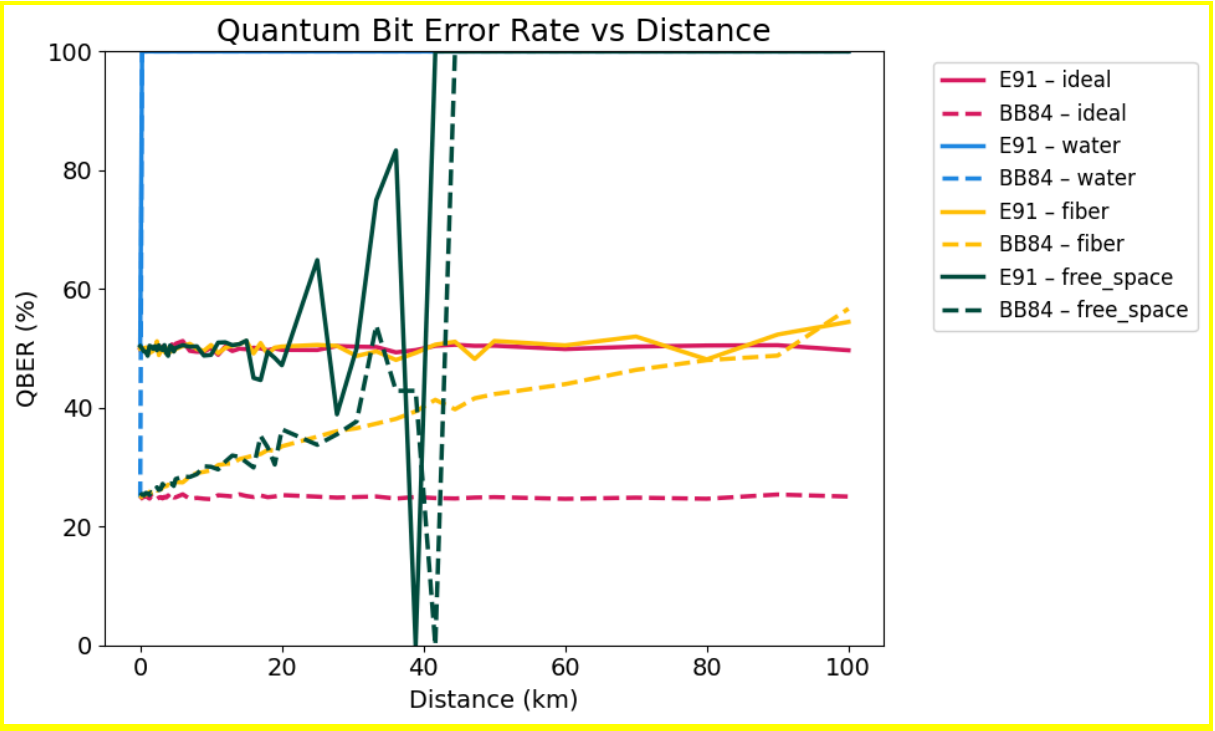
Figure 13. CHSH S-value vs. Distance (Partial Eavesdropping — e = 0.5)



For the CHSH S-values, our simulation demonstrated in Figure 13 that the eavesdropper interceptions dismantled quantum correlations. In fact, for all channels and distances experimented, this metric never surpassed the classical threshold.

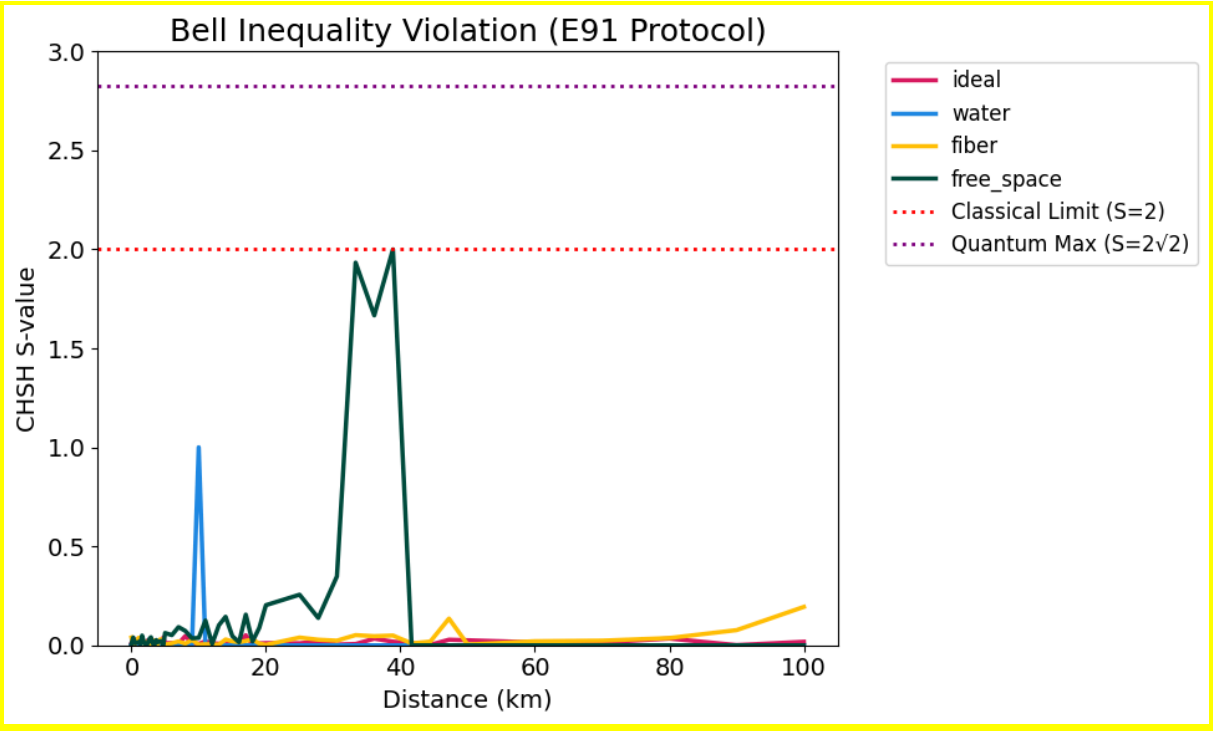
When the eavesdropper activity was increased to full interception (e = 1.0), the observed effects intensified across all metrics. As shown in Figure 14, QBER values exceeded 25% even at short communication distances. Interestingly, BB84 maintained noticeably lower QBER values than the E91 protocol up to approximately 80km, beyond which both protocols converged toward a QBER of 50%. Moreover, the free-space channel simulation continued to display anomalous results

Figure 14. QBER vs. Distance (Full Eavesdropping — e = 1.0)



In contrast to the partial eavesdropping scenario, the CHSH S-values under full attack showed a complete loss of correlations. As illustrated in Figure 15, all recorded values remained below 0.25, with the exception of a few statistical artifacts previously discussed.

Figure 15. 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 to be less susceptible to drastic QBER escalation under eavesdropping attacks. For E91, an additional metric — CHSH S values — served as an indicator or 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, the channel noise, not the protocol, limited secure entanglement-based QKD under those physical conditions.

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) is the next step to secure communication. Thus, practical implementation needs to take place in the near future to protect secret information from the threats that quantum computers' algorithms impose. 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.

Despite the result, it is crucial to recognize that E91 has theoretical advantages not captured by the performance metrics analyzed here. 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, continued research into overcoming the fragility of entanglement in E91-like protocols is essential for achieving next-generation quantum networks.

With these insights, we believe that future research and practical implementations have valuable information 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. So, bridging the gap between theoretical and practical quantum communication is essential to unveil the full potential of this technology.

5 - Bibliography

1. Agrawal, G. P. (2012). *Fiber-Optic Communication Systems*. John Wiley & Sons.
2. 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
3. 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
4. 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
5. Bernstein, D. J., Heninger, N., Lou, P., & Valenta, L. (2017, June 4). Post-quantum RSA. https://doi.org/10.1007/978-3-319-59879-6_18
6. Bhatia, V., & Ramkumar, K. R. (2020). An Efficient Quantum Computing technique for cracking RSA using Shor's Algorithm. *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*, 89–94. https://doi.org/10.1109/ICCCA49541.2020.9250806
7. 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
8. 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

9. 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
10. Czerwinski, A., & Czerwinska, K. (2022). Statistical Analysis of the Photon Loss in Fiber-Optic Communication. *Photonics*, *9*(8), Article 8. https://doi.org/10.3390/photonics9080568
11. Díaz, F., & Lenin, J. (2014, March 28). *Geração de emaranhamento de polarização entre pares de fótons no regime de fentossegundos* [Master's thesis]. Universidade Federal de Pernambuco. https://repositorio.ufpe.br/handle/123456789/18296
12. 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
13. Maloo, S. (n.d.). *Quantum Cryptography and Communication: Protocols, Limitations, and Solutions.*
14. 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), 076106. https://doi.org/10.1117/1.OE.57.7.076106
15. Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information* (10th anniversary ed.). Cambridge University Press.
16. 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), 057901. https://doi.org/10.1103/PhysRevLett.92.057901
17. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134. https://doi.org/10.1109/SFCS.1994.365700
18. 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
19. Teich, M. C., & Saleh, B. (2007). *Fundamentals of photonics* (Vol. 2). Wiley.
20. 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), 7. https://doi.org/10.1038/ncomms1005
21. 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
22. 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), nwaf147. https://doi.org/10.1093/nsr/nwaf147

23. 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

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

7 - Acknowledgements

We wish to thank [mentor name redacted] 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 [mentor name redacted] 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 which 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 was fundamental for both the writing and the empirical process. Therefore, we are extremely grateful to everyone involved.

Referee Report — Convergence

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

Overview. This student manuscript compares BB84 and E91 across fiber, free-space, and underwater channels using simulation. It reports QBER, sifted and secure key rates, and—for E91—CHSH *S*-values, both with and without an intercept–resend eavesdropper. The topic is timely and well-suited to *Convergence*'s audience. With a focused round of revisions—mainly clarifications, consistency checks, and presentation polish—the paper will make a strong pedagogical contribution.

Comments

1) Channel models and units.

   Loss. You cite Beer–Lambert with attenuation α in dB/km but do not show the exact conversion from dB/km to linear transmittance per distance used to compute $P_{\text{survive}}(d)$. Please write the explicit formula used in the simulator (e.g.,

   $$P_{\text{survive}}(d) = 10^{-\alpha d/10},$$

   include units for α and d, and state any additional loss terms (coupling/detection).

   Depolarization. The model applies a distance-dependent random Pauli error with equal *X/Y /Z* probabilities. Specify the underlying quantum channel (e.g., depolarizing channel $E(\rho) = (1 - p)\rho + p\, I/2$, or a Pauli channel with (p_X, p_Y, p_Z)), explain how λ maps to the error probability $p(d)$, and justify equal weighting. Replace the future-dated citation ("Zhang et al., 2025") with a published estimate or clearly mark it as a provisional assumption.

   Loss: Showed the exact conversion from dB/km to linear transmittance; updated formula; included units for parameters; stated that additional loss terms weren't simulated.

   Depolarization: Specified the underlying quantum channel (single-qubit Pauli channel with equal probabilities for X, Y, and Z errors); justified equal weighting; marked future-dated citation as a provisional assumption.

2) Security thresholds and claims. Treat the ~ 11% BB84 QBER threshold carefully: it assumes idealized, asymptotic conditions and one-way error correction/privacy amplification. You currently zero the secure key rate beyond ~ 20 km based on this cutoff. At minimum, state these assumptions explicitly and soften the language from "hard limit" to "guideline under our assumptions." If feasible, add a brief note on finite-key sensitivity.

   Stated assumptions explicitly and softened language mentioning that practical implementations operate under finite-key constraints and may tolerate slightly different error levels.

3) Eavesdropping models. For E91 you describe intercept–resend where Eve "measures on a random basis and resends a random state," which destroys entanglement; however, different intercept strategies affect correlations differently. Define Eve's behavior precisely for both protocols (basis choice, measurement rule, resend rule). For E91, briefly state the expected change in correlations and in *S* under your attack model

before presenting simulation results.

Defined Eve's behaviour precisely for both BB84 and E91; briefly stated expected change in correlations and CHSH S-values under attack.

4) Numerical stability and anomalies. The free-space results show QBER oscillations (including unexpected zeros) and CHSH spikes above the classical limit under full eaves dropping at 35–50 km. These suggest inadequate averaging or an implementation issue. Increase runs, vary seeds, report means with uncertainty (error bars or shaded bands), and comment on any residual anomalies rather than over-interpreting single points.

   Varied seeds, substantially reducing the number of anomalies; commented on residual anomalies explaining that these were largely due to statistical artifacts caused by the low amount of measured bits.

5) Sifting details. Report the expected and observed sifting fraction (≈ 50% for BB84 with random bases) at short distance and no attack, and confirm that your observed fraction matches expectation within statistical error. This serves as a simple end-to-end sanity check.

   Reported metrics for a perfect channel to serve as a simple sanity check.

6) Figures and captions. A couple of figure references don't seem to resolve cleanly (the numbering appears to skip), and some axes are hard to read. Please ensure every referenced figure is present, bump font sizes, put units on axes, and keep comparable axis limits across media so side-by-side comparisons are fair.

   Corrected the numbering of figures; improved readability by bumping font sizes; included units on axes; normalized axis limits.

7) Reproducibility basics. Because the conclusions rest on a simulator, include either a minimal code link or an appendix with pseudo-code, random seeds, and a compact parameter table (e.g., α, λ, distance grid, trials per point). Without this, readers can't sanity-check the pipeline.

   Included minimal code Google Colab link that includes the seeds and parameters used.

Reply

Thank you for the amazing feedback. I greatly appreciate the time and care you took to evaluate my work and provide such constructive and detailed comments. I hope I was able to properly implement your suggestions, which certainly refined the manuscript and strengthened both its scientific and pedagogical quality. Thank you again for helping me improve this research.

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

Overview: In this manuscript, the author explores the performance of two well-known quantum key distribution protocols, BB84 and E91, under realistic conditions of physical noise. The author models the effects of both photon loss and depolarization in different media and defines a number of metrics against which these algorithms are tested and compared.

The paper is very thorough and targets a timely topic. However, it could be better written and illustrated in certain places; in particular, to be most valuable to many audiences, much of the text should be written for concision and many figures should be combined. It should also be thoroughly checked for grammar since there were grammatical errors in many places. I thus suggest that this paper be accepted with major revisions (acceptance conditional on satisfactory major revisions). A thorough set of comments follow below.

Substantive Edits

1. I would strongly recommend making the paper more concise by condensing the Methods section. Too long of a Methods section conceals your more important original results. I would suggest citing certain discussions away to the original papers. This may also be facilitated by using equations, which are naturally more direct, as opposed to text to explain many things. Your discussion of Bell's inequality is repeated, for example.
   I appreciate this comment and understand the concern regarding the length of the Methods section. However, I believe that maintaining the current level of detail is important for the pedagogical clarity of the paper, which aims to make the modeling process and quantum communication concepts accessible to readers with varying backgrounds. This explanatory depth was also highlighted by another referee as one of the manuscript's main strengths. In contrast, I did fix the repetition of the discussion of Bell's inequalities by deleting the explanation in the beginning of the E91 section.
2. All figures should be enlarged. In particular, all figure fonts should be relatively large and clear to facilitate interpretation, including axis labels and legend fonts. Moreover, curves that represent different data types should be plotted both in different colors AND using different types of lines (solid, dash, dotted, etc.) to facilitate interpretation by a range of people, including those with color-blindness. There are color-blind palettes available.
   Enlarged all figures to facilitate interpretation. Used dashed and solid lines and color-blind palette.
3. Moreover, in many cases, it would make more sense to condensed the multiple figures into one where figures that study the same phenomena in slightly different ways are made into a single panel.
   Instead of having a graph for each metric and for each channel, I condensed all channels into a single figure for each metric (merged secure and sifted key rate).
4. The meaning of this sentence isn't quite correct: "Due to the absence of real quantum hardware (such as single-photon sources and detectors), polarization states, measurements, and channel effects were modeled computationally." Quantum hardware is very real, including

single-photon sources. I believe what you mean is that you did not have access to such hardware. If so, the sentence should be rewritten.
Rewrote the sentence to correct ambiguity. Now it properly expresses that although quantum hardware exists, I did not have access to such equipment.

5. Papers typically number sections, as opposed to letter them.
Numbered all sections properly and adjusted “structure paragraphs” to reflect the change.
6. The methods section would be improved if the key equations underlying both methods were stated.
I do not understand this comment. I believe the key equations underlying both methods are already stated. I would like to know which equations this is referring to.

Minor Edits

1. In the abstract, “Quantum key distribution (QKD) has emerged in recent decades as a hopeful approach to guarantee secure data transmission, …” should replace the word hopeful with potential, prospective, or possible.
Replaced word hopeful with potential to to convey a more formal and objective tone appropriate for academic writing.
2. In the abstract, “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.” should replace the word independence with dependence since BB84 depends upon entangled pairs.
BB84 is independent of entangled pairs, so the original wording is correct and has been kept.
3. The key word “Realistic Simulation” should be removed since it is not clear what that means technically (many things can map to that phrase that have nothing to do with your paper).
Removed the key word “Realistic Simulation.” However, I do not completely agree with this comment because I believe that explicitly mentioning that this paper is based on a simulation in the title or in the key words is important. I also do not understand the reasoning behind the comment since many things that have nothing to do with the paper could also map to the other key words.
4. Still isn’t the right transition word for this sentence since you are not making a contrast: “Still, we predict that underwater channels are not viable for practical implementation.”
Replaced “Still” with “Accordingly”. Also changed the whole paragraph to improve the presentation of the hypothesis.
5. “For both protocols, the transmission of 100000 particles” should replace particles with photons.
Replaced “particles” with “photons.”

Reply

I would like to sincerely thank you for the careful and detailed review of my manuscript. I greatly appreciate the constructive feedback and thoughtful suggestions, which have significantly improved the clarity and academic presentation of the paper. It’s an honor to receive such feedback. Thank you again for your time and expertise.

Review of: "Comparative Performance Analysis of BB84 and E91 Quantum Key Distribution Protocols Under Real-World Imperfections"
Author 100061, Submission 100056
Date: October 19, 2025

To the Author,

Recommendation: **Accept with major revisions**

This recommendation reflects the paper's strong research premise and sound methodology. The identified issues, while significant, are well-defined and achievable to address through revision. The core of the research is strong, and a revised version that incorporates these suggestions will meet the high academic standards of the journal.

I am confident that by incorporating the suggestions below, this paper will be an excellent candidate for publication. You have done a wonderful job on a challenging topic, and I strongly encourage you to incorporate the revisions below. I look forward to reading the next version of your manuscript.

Review Summary

Strengths:

- Ambitious and well-executed simulation project.
- Exceptional clarity and pedagogical value in explaining complex quantum protocols.
- Strong, logical structure and excellent use of figures and tables.
- Thorough engagement with foundational and contemporary literature.

Limitations:

- The primary limitations are the unaddressed statistical anomalies in the free-space simulation results and the inconsistencies in explaining how probabilities were dealt with in the methodology section, which currently detract from the paper's rigor.

This is a high-quality manuscript with the potential to be an outstanding contribution to the journal. The identified limitations are significant but correctable with relatively minor revisions.

General Assessment

Thank you for submitting your work to Convergence Journal! It was a pleasure to read such a well-structured and ambitious paper from an early-career researcher. You have undertaken a significant computational project and presented the results with remarkable clarity. The work is well-suited for the journal's audience and provides an excellent, accessible bridge between the theory of quantum communication and the practical challenges of

implementation. My review is structured according to the journal's key evaluation criteria, followed by a summary and final recommendations. You have tackled a difficult and highly relevant topic with clarity and academic rigor. The feedback below is offered in the spirit of mentorship, with the goal of helping you refine this already impressive manuscript into an even stronger publication. Some of the recommendations start from errors and should be definitely addressed in order to prepare the manuscript for publication. By contrast, the remaining feedback is aimed at helping the author improve the paper even more and the author is the one to decide whether they believe it is worth the effort to address these recommendations.

This is a very strong manuscript that demonstrates a solid understanding of quantum key distribution principles and a commendable proficiency in computational simulation. You clearly present the research question, develop a sound methodology for modeling the quantum channels and protocols, and present the results in a logical fashion. The paper's greatest strength is its pedagogical value; the explanations of the BB84 and E91 protocols, channel effects like photon loss and depolarization, and the relevant performance metrics are exceptionally clear and would be highly beneficial for high school and undergraduate readers. While the overall quality is high, there are specific areas, particularly concerning the interpretation of some simulation results, that require revision to enhance the paper's scientific rigor.

Thank you very much for your thoughtful and encouraging feedback. I truly appreciate the time and care you took to evaluate my work and provide such constructive and detailed comments. I hope I was able to properly implement your suggestions, which certainly refined the manuscript and strengthened both its scientific and pedagogical quality. Thank you again for helping me improve this research.

Detailed Feedback Based on Evaluation Criteria

1. Originality & Significance:
While a comparative study of BB84 and E91 is not novel in the broader field of quantum physics, this paper's contribution is significant and original within the context of student research and for the journal's target audience. The direct comparison of the protocols across three distinct and physically motivated channels (fiber optic, underwater, and free-space), complete with simulated eavesdropping, provides a comprehensive and insightful analysis. It is a creative and well-executed project that synthesizes complex theoretical concepts into a tangible computational experiment, which is a valuable contribution.

2. Clarity & Structure:
The paper's structure and clarity are exemplary. The manuscript is organized logically, beginning with a well-motivated introduction, followed by a detailed methodology, a systematic presentation of results, and a concluding discussion. The use of subsections for each channel and eavesdropping scenario makes the results section easy to navigate. Furthermore, the inclusion of tables to summarize parameters (e.g., Table 1 for attenuation coefficients) and illustrate protocol steps (e.g., Table 6 for a BB84 example) significantly enhances readability and understanding. You have done an excellent job of making a

complex topic accessible.

One important remark is that the figures should be slightly larger, maybe even double in size to ensure clarity. The axes labels and figure title are difficult to read without zooming into the page.

Enlarged figures and changed the color palette to improve visibility and accessibility.

3. Use of Evidence & Research Methods:
The methodology is generally sound and well-explained. You correctly employ standard physical models, such as the Beer-Lambert law for photon loss and a Markovian model for depolarization, and ground the simulation parameters in cited literature. The implementation of the protocols and the eavesdropping attack models are appropriate.

However, a significant concern arises from the results of the free-space channel simulation. The paper reports that the Quantum Bit Error Rate (QBER) "oscillated, even unexpectedly reaching zero" at intermediate distances (Figure 15) and that the CHSH S-value showed "anomalous spikes" under eavesdropping (Figure 22). These results are highly irregular and suggest statistical artifacts rather than physical phenomena. They are likely caused by a very low number of photons surviving transmission at those distances, making the calculated metrics unreliable.

Specific Recommendation: To address this, I recommend the author perform one of the following:

- Increase simulation trials: Re-run the free-space simulation with a much larger number of initial photons (e.g., 1,000,000 instead of 100,000) if computationally possible. This will improve the statistical significance of the results at longer distances and likely smooth out the anomalous oscillations.

  To address this problem, I first attempted to increase the number of photons sent to 1,000,000. However, this increase did not help for the first random seed tested, as there were still numerous anomalous oscillations. I could have continued experimenting with other seeds, but each simulation was extremely time-consuming (over nine hours). Ultimately, I decided to reduce the number to 100,000 and test different seeds until I found one that substantially minimized the anomalies.
- Acknowledge and discuss uncertainty: If re-running the simulation is not feasible, the author must add a discussion of this anomaly. It should be explicitly stated in the Results and Discussion sections that the oscillations are likely statistical noise due to a low count of surviving photons.

  Acknowledged moments when QBER reached 0, explaining that it was caused by a very low number of photons surviving transmission.

Addressing this point is crucial for the paper's scientific integrity.

4. Engagement with Literature:
You demonstrate a strong engagement with the relevant scientific literature. The paper

correctly cites the foundational works of Bennett & Brassard (BB84) , Ekert (E91) , and Shor & Preskill (for the BB84 security proof). Furthermore, the use of a standard textbook like Nielsen & Chuang and references to experimental papers for channel parameters shows that the author has conducted thorough background research. The work is well-situated within the established knowledge of the field. I encountered one case where you did not cite the original paper, but a more recent one, which I highlighted below in the feedback for the corresponding section.

5. Grammar & Language:
The quality of the writing is suitable for a research journal. The language is clear, professional, and precise. You explain complex concepts without resorting to unnecessary jargon, making the paper highly accessible to its intended audience. The manuscript is polished and free of any significant grammatical errors.
Additional specific recommendations

A. Abstract and Introduction

- This is a tiny typographic advice but it is applicable for the entire manuscript: you should replace the hyphens (-) with em (—) or en (–) dashes. Check when each one should be used and please use them accordingly in your manuscript.

Replaced all hyphens with the appropriate dash. P.S: Prior to this comment I had no idea that there was a difference between an em and an en dash. Thanks for teaching me something!

- Some recommendations on the paragraph where you explain the BB84 protocol:
    - Clarify what is meant by “representing binary values”: “Alice and Bob can send polarized photons representing binary values (0 and 1)”

      Added a brief clarification stating that the binary values are encoded through different polarization directions. I could have been more specific and mentioned the representations for each base, but since this is just the introduction and I already mentioned this later, I chose to approach it this way. Please let me know what you think.
    - Refine the explanation of eavesdropping detection: The photon’s state doesn’t just “collapse with the wrong basis”, rather, *Eve’s measurement disturbs the quantum state*, leading to observable error rates in the sifted key.

      Refined the explanation of eavesdropping detection explaining that attacks disturb quantum states, introducing detectable errors in the sifted key.
    - Cite Bennett & Brassard correctly**:** “Bennett & Brassard, 2014” likely refers to a *reprint* or *retrospective publication*. I believe the **original** paper is *Bennett & Brassard (1984)* You could clarify this.

      Indeed, the citation refers to a retrospective publication celebrating 30 years of BB84. Honestly, I am not sure where exactly to clarify this and I do not consider it a problem since many of the papers I cited used the same citation.
    - Add one line to complete the flow (optional): It might help to close by mentioning that after sifting, error correction and privacy amplification are performed to finalize a secure key.

      I decided not to add this line since one of the other feedbacks I received

mentioned that I should try not to repeat things. Although I agree that this line would improve the flow, I chose not to add it.

- Some recommendations on the paragraph where you explain the E91 protocol: ○ Clarify the correlation behavior: The correlations are strongly correlated only when compatible measurement settings are used, not “even when different bases are chosen.” In fact, for certain non-compatible basis choices, quantum correlations deviate from classical predictions, allowing the Bell test, but the measurement results themselves are not deterministic.

Clarified the correlation behavior explaining that when compatible measurement settings are used, the results are strongly correlated, indicating direct entanglement. Also explained that for certain non-compatible basis choices, the correlations might still demonstrate a violation of Bell’s inequalities.

○ Bell test interpretation: It’s not that “violation confirms entanglement” per se, but that it rules out local realistic (classical) explanations, which is evidence of entanglement and no eavesdropping.

Properly interpreted bell test by explaining that if Bell’s inequalities are satisfied, it can be implied that the correlations could be explained by local realistic models, suggesting that entanglement may have been lost due to eavesdropping or depolarization.

○ Terminology tweak: “Check the integrity of the key exchange” → better phrased as “verify the security of the quantum channel.”

Improved terminology: “verify the security of the quantum channel”

○ Minor stylistic polish: Replace some dashes with commas or semicolons for smoother academic flow.

Replaced some dashed with commas.

- Consider reframing the hypothesis to explain why this performance difference is expected. This reframing elevates the hypothesis from a simple prediction to a more sophisticated physical argument, demonstrating a deeper level of understanding.

Reframed the hypothesis using physical arguments to explain predictions.

- The introduction could also benefit from acknowledging the dual nature of E91's sensitivity to noise and interference. The manuscript correctly identifies this sensitivity as a practical drawback leading to higher QBER. However, this sensitivity is also the very foundation of its security model. An eavesdropper's interaction with the entangled pair inevitably disturbs the delicate quantum correlations, causing a detectable drop in the CHSH S-value and a spike in the QBER. In this sense, E91's "fragility" is also its strength, as it makes eavesdropping attempts more conspicuous.

Refined the introduction explaining that the same sensitivity underpins the security of the protocol by facilitating eavesdropping detection.

B. Methodology

It is not expected that you implement a full-scale atmospheric turbulence simulation, as these often require complex numerical methods like split-step propagation and the generation of random phase screens. However, acknowledging this limitation is a crucial part of rigorous scientific reporting. It is recommended that you:

1. Acknowledge the limitation**:** In subsection II-a) on Channel Modeling, add a

paragraph explicitly stating that the current free-space model is a simplification that does not account for the effects of atmospheric turbulence.

Acknowledged the limitation explaining that the model is an overly simplified description of atmospheric conditions that does not account for turbulence.

2. Describe the physics**:** Briefly explain what turbulence is and its primary effects (e.g., Atmospheric turbulence causes random fluctuations in signal strength and phase, leading to bursty errors and time-varying channel loss, rather than a smooth degradation with distance).

Explained what turbulence is, mentioning its effects of photon transmission and pointing out why it was not modeled in the simulation.

3. Contextualize the results**:** In the Results and Discussion sections, explicitly connect the observed oscillations in the free-space data to this model limitation. This demonstrates a mature understanding of both the underlying physics and the boundaries of the simulation.

Since I have substantially reduced the number of oscillations and explained them adequately, I believe that contextualizing the results is no longer necessary.

I am afraid section II-a) contains a critical error which I hope is just a typo and not the actual way in which the photon loss was modelled. In a per-photon Monte Carlo, you keep the photon if the random number you draw from [0,1] is <= P_survive(d) and drop it otherwise. Your text says “If the number is lower, the photon is considered lost,” which is the opposite of what “survival probability” means. At the beginning of the channel, P_survive(0) = 1, so by the method you describe we would drop all the photons…The same description with the inverted logic repeats in section II-b) so please check this aspect thoroughly (“A photon is considered lost - and its value is set to None - if the survival probability is smaller than a randomly generated number (k) ∈ {0, 1}. “)...In section II-c), your logic is the correct one (“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}.”) so I hope this is how the algorithm worked in your simulation.

Please also correct the descriptions of how the depolarization is applied in section II-b) and II-c) since the two descriptions are not consistent (they represent the two opposite cases). For example, the logic in section II-c) is backwards (“On the other hand, when the depolarization probability is smaller than (k), the photon becomes mixed, resulting in completely random measurement outcomes.”) and not correct. Think about the starting location, where P_depol = 0. By your description, all photons would depolarize from the start no matter the value of k in (0, 1].

Please also correct and double check the part of the algorithm described by “Subsequently, this probability is compared to a randomly generated number (k) ∈ {0, 1}. If P_same is smaller, Bob’s outcome matches Alice’s.”. The logic here is also inverted compared to the correct one. If P_same = 1, and you compare it to any k, you will always conclude that Bob’s outcome does not match Alice’s even though we started with a 100% probability for the outcomes to be the same….

Corrected critical errors. The algorithm was using the correct logic in the simulation. However, when I was writing the paper, I accidentally inverted the logic.

C. Results and Analysis

You should re-interpret these anomalous results by discussing the potential high effect of statistical artifacts in the results presented in your figures. At longer distances in a highly lossy channel, the number of photons that survive to be measured by Bob becomes very small. For instance, out of 100,000 initial particles, only a tiny fraction might reach the detector at 40 km or 50 km. When performance metrics like QBER or correlation coefficients are calculated from a very small statistical sample, they are subject to large random fluctuations. A few "unlucky" random errors can cause a large swing in the calculated QBER. This effect explains the jagged, non-monotonic behavior seen in the graphs.

A particularly telling example is Figure 22, which shows spikes in the CHSH S-value that appear to violate the classical limit of $|S| \leq 2$ even with a strong eavesdropper present. This is an unphysical result. The CHSH test requires calculating four separate correlation coefficients from the measurement outcomes. When the number of surviving photon pairs available for this calculation becomes statistically insignificant, the resulting S-value is essentially random noise and can fluctuate into these unphysical regimes.

You should explicitly discuss this in the analysis. For example, when discussing Figure 22, you should highlight some of the following aspects. The anomalous spikes observed in the CHSH S-value at longer distances, particularly under eavesdropping, are likely statistical artifacts. At these distances, high photon loss drastically reduces the number of correlated pairs available for the CHSH calculation. When the sample size is very small, the calculated correlation values are not statistically significant and can fluctuate randomly. This highlights a practical challenge in implementing the E91 protocol: a sufficient number of transmitted particles is required to perform a statistically meaningful security check.

Rewrote the whole section with new results obtained from different simulation seeds that reduced statistical anomalies. While there were still some oscillations, I explained that those were statistical artifacts caused by the low number of measured photons, showing the key length figures.

For figures showing key rate or key length versus distance (e.g., Figure 2, Figure 3, Figure 4), consider using a logarithmic scale for the y-axis. This is standard practice in QKD literature as it allows the performance at longer distances to be visualized more clearly, rather than appearing to crash to zero immediately.

Used logarithmic scale for the y-axis for key length versus distance figures. This proved to be extremely useful to explain the oscillations seen in other metrics since it helped visualize the moments when the key length was minimal.

Additional specific recommendations:

- The underwater channel claims are plausible but contextual. Stating “<200 m works; >200 m is impractical” is site- and spectrum-dependent (water type, turbidity, wavelength (blue-green window ~450–550 nm, beam divergence, background light,

polarization scrambling). It's fine to say your data shows feasibility below ~200 m for your water type and hardware, but avoid universalizing it.

Explained that, while our results indicate short-range feasibility, the precise distance limit should not be interpreted as universal but as representative of the modeled conditions because this limit is highly dependent on environmental and optical characteristics.

- CHSH S-values "below classical even with no eavesdropper"
    - This is a red flag about the link, not proof E91 is weaker.
    - CHSH S is exquisitely sensitive to visibility, alignment, depolarization, detector noise, and loss. If S<2 without an eavesdropper, your state visibility V was too low (misalignment/depolarization/multi-pair, or accidental coincidences). The rough mapping S < 2 implies QBER > approx. 14.6%, i.e. already beyond BB84's one-way security threshold. So the "quick S degradation" is consistent with channel/device noise, not a protocol flaw.
    - When an article says "CHSH S-values were below the classical threshold even without eavesdropping in the water channel," that likely means:
        - The channel noise (not eavesdropping) destroyed entanglement,
        - The measured correlations were too weak to show a Bell violation, and
        - Therefore, secure entanglement-based QKD was not achievable under those physical conditions.
        - That's a scientifically valid observation, not an error, but it should be clearly explained as environmental decoherence, not as a classical limit of quantum theory or a weakness of the protocol itself.

Explained that CHSH S-values falling below the classical limit under no eavesdropping do not indicate a flaw of the protocol, but rather reflects its sensitivity to harsh conditions, which is expected.

D. Discussion and Conclusion

The conclusion that BB84 is more "practical" is fair based on the simulation results. However, it is important to acknowledge the unique theoretical advantages of E91 that are not fully captured by these performance metrics. The E91 protocol is the conceptual foundation for Device-Independent QKD (DI-QKD), an advanced form of quantum security where a secure key can be established even if the quantum devices used by Alice and Bob are untrusted or have been tampered with by an adversary. This provides a level of security that prepare-and-measure protocols like BB84 cannot achieve.

In addition, you can demonstrate a more profound understanding of the field's trajectory by discussing this. A paragraph could be added to the discussion or conclusion. While your results indicate BB84's superior performance in the presence of channel noise, it is important to note the distinct theoretical advantages of the E91 protocol. E91's reliance on Bell's inequality paves the way for Device-Independent QKD, which aims to provide security

without having to trust the internal workings of the communication hardware. Therefore, while BB84 may be more suitable for near-term practical implementations, research into overcoming the fragility of entanglement in protocols like E91 is crucial for developing next-generation quantum networks with even stronger security guarantees.
Added a paragraph in the conclusion recognizing that E91 has theoretical advantages that were not captured by the performance metrics in the simulation, mentioning DI-QKD as a promising technology that is based on the fundamental concepts of E91.

The conclusion rightly mentions quantum repeaters as a key technology for extending the range of QKD. To further showcase the breadth of the author's knowledge, this point could be briefly expanded to include other mitigation techniques being actively researched. These include adaptive optics, which use deformable mirrors to correct for atmospheric turbulence in real-time in free-space links, and advanced classical error correction codes tailored for the low signal regimes of QKD. Mentioning these would add further depth to the outlook on future research.

Expanded this paragraph to include other technologies that are actively being researched, such as adaptive optics and error correction codes.

Decision: Accept.

The revision is substantially clearer and more careful than the original, especially in the channel modelling and in how you frame the 11% QBER threshold. The explicit Beer–Lambert expression and the Pauli-channel description are helpful, and the added comments about statistical artefacts in the free-space plots show good scientific maturity.

That said, the Discussion and Conclusion would still benefit from one more explicit paragraph on limitations. You briefly note that detector dark counts, misalignment, and possible decoy-state refinements are not included in the present model, but these remarks are scattered. Pulling them together into a short “limitations and next steps” paragraph would make it much clearer what is inside and outside the scope of your analysis, and where you see the most natural extensions.

I would also suggest being a bit more careful in how you connect the E91 results to fully device-independent QKD. As it stands, the wording could be read as implying that the simple intercept–resend toy model you study speaks directly to DI-QKD security, which is a stronger claim than you actually need.

Finally, in the Results, there is still some repetition between Sections 3.1–3.3, where the same qualitative ranking of underwater, free-space, and fibre channels is restated several times. This part could be tightened by trimming repeated sentences so that each subsection adds something distinct."

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

Overview: While lengthy, I think this paper has substantially improved, clearly articulating its points through carefully-selected subsections and corroborating them with data and appropriate citations. Some of the conclusions are obvious in retrospect, but I think this represents a good exercise in modeling and nicely disentangles the effects of different types of errors on different quantities. I would therefore recommend publication with minor revisions at this point.

Substantive Edits

1. I will reiterate my position that the paper should generally be shorter. As a well-regarded quantum physicist, I want you to understand that no physics or computer science journal publishes papers more than 15 pages in length these days. A core concept of all quantitative fields is to be concise so as not to blur results - what is your hypothesis, what are the results, what are their novelty, and what do they imply. I will not stick to my guns about this for a high school article, but you should be well-aware of the role of concision in reporting physical science research.
2. I think the paragraph “In the BB84 protocol,...” should be moved to after you define the terms used in the paragraph such as secure key rate and shifted key rate, etc.
3. The paper is much better divided into sections than I previously recall. Great job clearly dividing your work for understanding and to focus the attention of readers.
4. You can likely omit Figures 2 and 3 since this can just be stated in words.
5. What is the expectation for the the E91 sifting fraction?
6. Would Figure 11 be the same if you simply ran with more photons? Would you expect it to smooth?
7. One thing that is somewhat strange about these results is that you used probabilities to lose photons. Where are these statistics represented? Did you run these simulations in replicates? If so, where are the statistical error bars? For instance, in Figure 12, with averaging, some of the kinks would likely smooth. [This is my most significant technical concern.]
8. I don’t fully understand the statement that one must research into overcoming “the fragility of entanglement.” Entanglement is inherently fragile. To preserve entanglement, one must think about changing environments and/or involved carriers.

Minor Edits

1. Should be Beer-Lambert’s Law or the Beer-Lambert Law.
2. Should be “photons are probabilistically dropped according to the loss model defined by Equation 2.”
3. Should be “For this simulation, typical values of lambda…”
4. You should like define pX, pY, and pZ as the probability of Pauli noise along the different directions. Perhaps, p(X), p(Y), and p(Z) would be clearer notation.
5. Should be “Depolarization length (lambda), measured in kilometers, for each…”
6. Should be “Bit representation of different states of polarization in the BB84 protocol.”

7. The fonts in the paper seem to vary in different places. These should be reconciled if this isn't just a file issue on my end.
8. This sentence is incomplete: "In this sense, it is introduced in the communication channel, after all loss and noise is applied, an observer, Eve." By an observer Eve?
9. Should be "Each of the metrics offers insights…"
10. Instead of "the secure key rate to zero once…" should likely be "set the secure key rate to zero…"?
11. Should be "is the binary entropy function" not "is a binary entropy function" since this is the definition of the binary entropy.
12. You mention the CHSH-S value before defining it. You should either point toward the subsequent definition, or briefly define it above section 2.4.
13. Should be "served as an indicator of entanglement quality…"
14.

I have reviewed the revised submission and the author's reply to my initial round of feedback and I believe the paper should be accepted for publication. My rather extensive list of recommendations has been integrated into the revised manuscript to a high degree, so I will not provide further feedback on this occasion.