



A Comparative Study between Three Encryption Systems in a Quantum Computer (BB84, B92, BBM92) in Free Space Communication

Wala M Emran a , Fadel E Al-Sharif b , and Ahmed A Albashir b (a)

Department of physics, Faculty of Education, University of Zawia, Zawia, Libya

(b) Department of physics, School of Basic Sciences, The Libyan Academy, Tripoli, Libya

E-mail address: wala.emran@academy.edu.ly

ORCID id: <https://orcid.org/0009-0002-4819-3588>

تاريخ الاستلام: 2026/01/07 - تاريخ المراجعة: 2026/02/01 - تاريخ القبول: 2026/02/12 - تاريخ النشر: 2026/3/13

ABSTRACT

This research explores the fundamental principles of quantum computing and their application in enhancing communication security through Quantum Key Distribution (QKD) in free-space channels. Classical cryptographic methods face inherent limitations, particularly with the advent of quantum computational capabilities. Quantum mechanics, specifically the principles of superposition and entanglement, offers a robust framework for secure communication, ensuring that any attempt at eavesdropping inevitably perturbs the quantum state, thus revealing the intruder's presence. Through comprehensive simulations, this study analyzes the performance of QKD systems in free-space communication. Key parameters such as transmittance efficiency (η_T), Quantum Bit Error Rate (QBER), and Secret Key Rate (SKR) are evaluated. Results indicate that transmittance efficiency in free space generally decreases with increasing zenith angle, with downlink scenarios (day and night) exhibiting higher efficiencies compared to uplink during the night. For all protocols, simulations demonstrate an increase in QBER and a corresponding decrease in SKR as the zenith angle increases, with downlink performance consistently surpassing uplink in terms of a higher SKR and a lower QBER.

Keywords: Quantum Computing, Quantum Key Distribution (QKD), Free-space Communication, Quantum Bit Error Rate (QBER), Secret Key Rate (SKR).

(92) في اتصالات الفضاء الحر BB84, B92, BBM دراسة مقارنة بين ثلاثة أنظمة تشفير كمومية)

المخلص

ركز هذا البحث على المبادئ الأساسية قاتها في تعزيز أمن الاتصالات من خلال توزيع المفاتيح الكمية (QKD) في قنوات الفضاء الحر. تواجه طرق التشفير الكلاسيكية قيوداً جوهرية، لا سيما مع ظهور القدرات الحسابية الكمية. وتقدم ميكانيكا الكم، وتحديداً مبادئ التراكب والتشابك، إطاراً قوياً للاتصالات الآمنة، مما يضمن أن أي محاولة للتنصت ستؤدي حتماً إلى اضطراب الحالة الكمية، وبالتالي كشف وجود التنصت.

من خلال عمليات محاكاة شاملة، تحلل هذه الدراسة أداء أنظمة توزيع المفاتيح الكمية في اتصالات الفضاء الحر؛ حيث جرى تقييم معايير أساسية مثل كفاءة النفاذية (η_T)، ومعدل خطأ البت الكمي (QBER)، ومعدل المفتاح السري (SKR). وتشير النتائج إلى أن كفاءة النفاذية في الفضاء الحر تتخفض عموماً مع زيادة زاوية الذروة (Zenith angle)، مع ملاحظة أن سيناريوهات الوصلة الهابطة (Downlink) (ليلاً ونهاراً) أظهرت كفاءة أعلى مقارنة بـ الوصلة الصاعدة (Uplink) خلال الليل. وبالنسبة لجميع البروتوكولات، أظهرت عمليات المحاكاة زيادة في معدل خطأ البت الكمي (QBER) وانخفاضاً مقابل في معدل المفتاح السري (SKR) مع زيادة زاوية الذروة مع تفوق أداء الوصلة الهابطة عموماً على الوصلة الصاعدة من حيث تحقيق معدل مفتاح سري أعلى ومعدل خطأ بت كمي أقل.

الكلمات المفتاحية: الحوسبة الكمومية، توزيع المفتاح الكمي (QKD)، اتصالات الفضاء الحر، معدل الخطأ في البت الكمي (QBER)، معدل المفتاح الآمن (SKR)

1. Introduction

The continuous advancements in quantum mechanics and quantum computing represent a transformative development in the 21st century, with profound implications for secure communications. Unlike classical computing, quantum computing leverages the principles of superposition and entanglement to enable Quantum Key Distribution (QKD) [1]. This technique guarantees the generation of a shared secret key with information-theoretic security, where any eavesdropping attempt inevitably introduces detectable disturbances due to the fundamental laws of physics. This research presents a comparative study of prominent QKD protocols, focusing on evaluating their performance in a free-space communication environment. The study is conducted using numerical simulations, focusing on performance indicators such as Quantum Bit Error Rate (QBER), Secret Key Rate (SKR), and transmittance efficiency. The analysis examines these parameters under the influence of variables like zenith angle and distance, with the primary objective of providing recommendations for selecting the most suitable protocol for real-world quantum communication systems [2].

2. Theoretical Background:

2.1. Quantum Key Distribution (QKD) Protocols

Quantum Key Distribution (QKD) protocols are a cornerstone of secure communication, allowing two parties, typically called Alice and Bob, to establish a shared secret key while simultaneously detecting any potential eavesdropping attempts [3]. Below are three prominent QKD protocols [4].

2.1.1. BB84 Protocol

The BB84 protocol, proposed by Bennett and Brassard, is a foundational QKD scheme. Alice prepares a random sequence of qubits encoded in one of four non-orthogonal quantum states and sends them to Bob [2]. Bob randomly selects a measurement basis for each qubit. Subsequently, he publicly announces his choices. Alice and Bob only keep the qubits where their bases matched, which statistically occurs about 50% of the time [5]. To ensure the key's integrity, they compare a subset of their remaining qubits. If the error rate is too high, the protocol is aborted; otherwise, the remaining qubits form a secure key [3].

2.1.2. B92 Protocol

The B92 protocol is a simplified version of BB84 that uses only two non-orthogonal quantum states, $|0\rangle$ and $|+\rangle$ [3]. Unlike BB84, Bob does not publicly announce his measurement basis. Instead, he only keeps the qubits that yield a measurement outcome of $|1\rangle$ or $|-\rangle$. From these results, Bob can deduce Alice's encoding for a subset of the retained qubits, allowing them to create a shared key. The security of this protocol relies on the fact that certain measurement outcomes provide no conclusive information, while others can only be obtained if Alice encoded the qubit in a specific way [6].

2.1.3. BBM92 Protocol

The BBM92 protocol is an entanglement-based QKD scheme. In this protocol, Alice generates pairs of Einstein-Podolsky-Rosen (EPR) particles, keeps one particle, and sends the other to Bob. Both Alice and Bob independently choose a measurement basis for each particle (either the Z-basis or the X-basis) and keep only the results from matching bases [6]. By publicly comparing a subset of their results, they estimate the Quantum Bit Error Rate (QBER). If the QBER is within an acceptable range, the remaining correlated outcomes are used to generate a shared key. The security of BBM92 is based on the principle that any attempt by an eavesdropper to measure the entangled particles will inevitably disturb the entanglement and introduce detectable errors [5].

2.2. Quantum Bit Error Rate (QBER)

The Quantum Bit Error Rate (QBER) serves as a quantitative metric representing the proportion of incorrectly received bits to the total number of received bits. It effectively measures the probability of a false detection relative to the overall detection probability per pulse [7].

2.3. QBER in Free-Space Quantum Key Distribution

Free-space optical (FSO) links, unlike fiber optics, provide flexibility and the potential for global-scale QKD, including ground-to-satellite and satellite-to-satellite communication. A major

performance metric in QKD systems is the Quantum Bit Error Rate (QBER), which quantifies the error level in the transmitted quantum bits [7, 5].

In the context of the BB84 quantum key distribution protocol, the QBER (e_{84}) can be calculated using the following relation:

$$e_{84} = \frac{c p_{\text{signal}} + \frac{1}{2}(p_{\text{dark}} + p_{\text{straycounts}})}{p_{\text{click}}} \quad (1)$$

The quantum bit error rate (e_{92}) for this protocol is quantified by:

$$e_{92} = \frac{c p_{\text{signal}} + \frac{1}{4}(p_{\text{dark}} + p_{\text{straycounts}})}{p_{\text{click}}} \quad (2)$$

The quantum bit error rate for the BBM92 protocol is given by:

$$e_{M92} = \frac{c p_{\text{true}} + \frac{1}{2}(p_{\text{false}} + p_{\text{straycounts}})}{p_{\text{coin}}} \quad (3)$$

Parameter	Value	Brief description
t	20km	Atmospheric thickness
H	500km	Minimum altitude (zenith)
C_n^2	$1.2 \times 10^{-16} m^{-2/3}$	Night time, clear weather
C_n^2	$1.64 \times 10^{-16} m^{-2/3}$	Day time, not windy
Sky brightness, H_b	$1.5 \times 10^{-6} W m^{-2} sr^{-1} nm^{-1}$	Night, clear sky
Sky brightness, H_b	$1.5 \times 10^{-3} W m^{-2} sr^{-1} nm^{-1}$	Day, clear sky
Field of view, Ω_{fov}	$(100 \times 10^{-6})^2 sr$	Night-time downlink
Field of view, Ω_{fov}	$(10 \times 10^{-6})^2 sr$	Day-time downlink
Field of view, Ω_{fov}	$(30 \times 10^{-6})^2 sr$	Night-time uplink
Time Window Δt	0.5ns	Night and day time
Spectral filter width, B_f	1nm	Night-time downlink
Spectral filter width, B_f	0.2nm	Day-time downlink
Spectral filter width, B_f	1nm	Night-time uplink
H_{sun}	4.610 $\times 10^{18} plot s^{-1} nm^{-1} m^{-2}$	Solar spectral irradiance
A_E	0.300	Earth's albedo
A_M	0.136	Moon's albedo
R_M	$1.737 \times 10^6 m$	Moon's radius
d_{EM}	$3.600 \times 10^8 m$	Earth-moon distance

Table.1 Parameters related to the atmospheric weather conditions, stray photons and environmental light [8] [7].

2.4. Secret Key Rate (SKR)

In the context of Quantum Key Distribution (QKD), the key rate represents the metric quantifying the generation and secure sharing of cryptographic key bits between two communicating entities, conventionally designated as

Alice and Bob. It defines the temporal efficiency of secure key establishment, directly impacting the practicality and effectiveness of a QKD system [7].

2.5. SKR in Free-Space Quantum Key Distribution

A quantum key distribution (QKD) system's key rate, measured in bits per second (bps), is a crucial metric for evaluating its performance and practicality. It is influenced by factors like the quality of quantum states, detection efficiency, channel attenuation, and potential eavesdropping. The key rate calculation incorporates the Quantum Bit Error Rate (QBER), denoted as 'e', and also accounts for all loss mechanisms, including atmospheric losses and geometric divergence, providing a comprehensive measure of the system's efficiency in real-world scenarios [7].

The secure key generation rate of the BB84 protocol against photon number splitting (PNS) attacks is given by:

$$R_{BB84} = \frac{1}{2} p_{click} \{ (1 - \tau' + f(e_{84})(e_{84}(e_{84}) + (1 - e_{84})(1 - e_{84}))) \} \quad (4)$$

The secure key generation rate of the B92 protocol against a Photon Number Splitting (PNS) attack can be formulated as:

$$R_{B92} = \frac{1}{4} p_{click} \{ (1 - \tau' + f(e_{92})(e_{92}(e_{92}) + (1 - e_{92})(1 - e_{92}))) \} \quad (5)$$

The key rate for BBM92 protocol against double blinding attack is given by:

$$R_{BBM92} = \frac{1}{2} p_{coin} \{ (\tau(e_{M92}) + f(e_{M92})(e_{M92}(e_{M92}) + (1 - e_{M92})(1 - e_{M92}))) \} \quad (6)$$

3. Numerical Results and Discussion

3.1. Transmittance efficiency (η_T) vs. Zenith Angle in all scenarios in free space

Based on a Python simulation, the graph in Fig.1 shows how transmittance efficiency (η_T) changes with the zenith angle for three free-space scenarios: uplink at night, downlink at night, and downlink during the day. In general, (η_T) decreases as the zenith angle increases for all scenarios. The highest efficiency is seen during the downlink during the day, followed by the downlink at night, with the uplink at night consistently showing the lowest efficiency

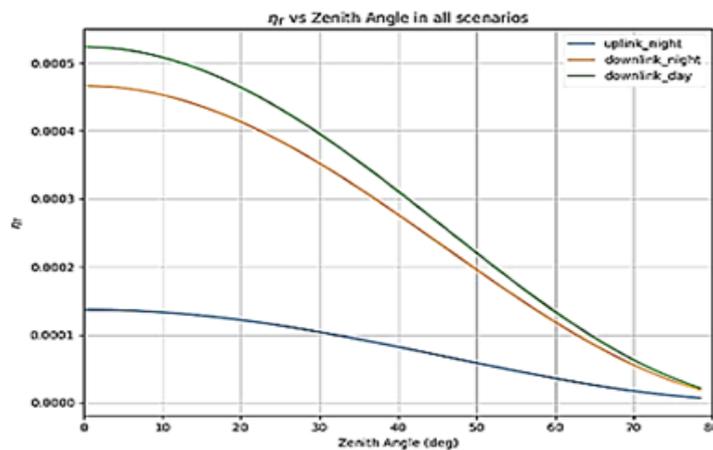


Fig .1 shows how transmittance efficiency (η_T) changes with the zenith angle for three free-space scenarios

3.2. Simulation Results for BB84 Protocol in Free-Space Quantum Key Distribution

Based on a Python simulation of the BB84 protocol and using Eq(1), Fig .2 illustrates the relationship between the zenith angle, Quantum Bit Error Rate (QBER), and Secret Key Rate (SKR) for different communication links. The simulation results of the BB84 protocol reveal a distinct degradation in quantum channel quality as the zenith angle increases, the ($QBER_{BB84}$), values range from approximately 0.035 at low zenith angles to about 0.19 at 80 degrees.

Crucially, the downlink configuration consistently outperforms the uplink, exhibiting a higher Secret Key Rate (SKR) and a lower Quantum Bit Error Rate (QBER). This performance disparity is governed by the relative position of atmospheric turbulence layers with respect to the optical source:

In the Uplink scenario: The laser beam encounters turbulent atmospheric layers immediately upon transmission from the ground station. The Secret Key Rate (SKR_{BB84}) is highest at low zenith angles. As the zenith angle increases, the (SKR_{BB84}) decreases. This decrease appears to be more pronounced at higher zenith angles. The SKR_{BB84} starts at around 7000 bps at low zenith angles and drops close to 0 bps as the zenith angle approaches 80 degrees

In the Downlink scenario: This graph shows two curves one for "Downlink Day" and one for "Downlink Night". For both day and night downlink, the ($QBER_{BB84}$), starts at a low value at small zenith angles and increases with the zenith angle. The "Downlink Night" ($QBER_{BB84}$), is generally lower than the "Downlink Day" ($QBER_{BB84}$), across all zenith angles; both curves show an accelerated increase in ($QBER_{BB84}$), at higher zenith angles (above 60 degrees). The ($QBER_{BB84}$), values for "Downlink Day" range from approximately 0.025 to 0.10, while for "Downlink Night", they range from about 0.02 to 0.075 over the plotted zenith angle.

The graph also shows two curves: "Downlink Day" and "Downlink Night, The Secret Key Rate (SKR_{BB84}) is highest at low zenith angles for both day and night downlink. As the zenith angle increases, the (SKR_{BB84}) decreases for both scenarios. The "Downlink Day" (SKR_{BB84}) is significantly higher than the "Downlink Night" (SKR_{BB84}) across the range of zenith angles. The (SKR_{BB84}) for "Downlink Day" starts at over 20000 bps and decreases to near 0 bps at 80 degrees. For "Downlink Night", it starts at around 16000 bps and drops towards 0 bps at higher zenith angles.

The optical beam propagates primarily through a vacuum, maintaining its coherence over a long distance. It encounters atmospheric turbulence only during the final stage of propagation near the ground receiver. Consequently, the beam suffers less energy dispersion and wavefront degradation, allowing for superior photon coupling efficiency and a significantly higher key generation rate.

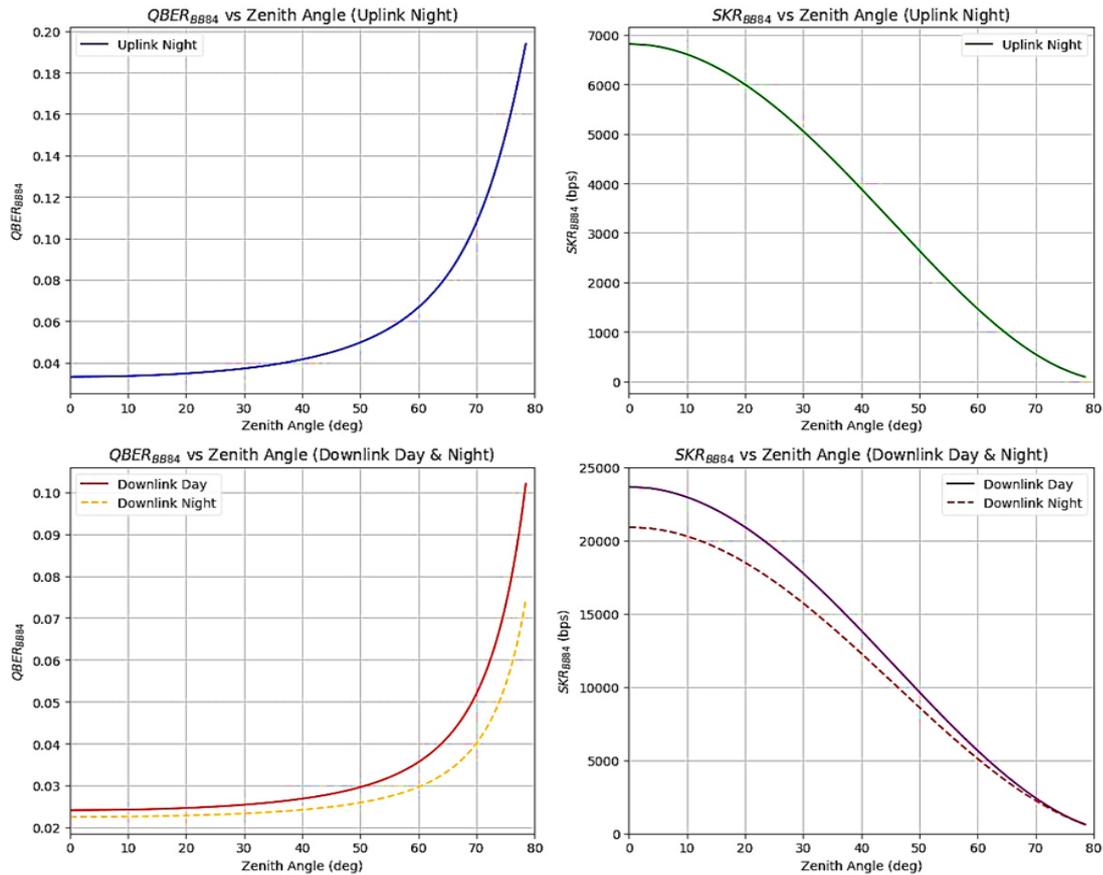


Fig.2 illustrates the relationship between the Zenith Angle, Quantum Bit Error Rate ($QBER_{BB84}$), and Secret Key Rate (SKR_{BB84}).

Two graphs in Fig.3 show the performance of a BB84 quantum key distribution (QKD) downlink over varying distances, comparing day and night conditions. As the transmission distance increases, the Quantum Bit Error Rate (QBER) rises, while the Secret Key Rate (SKR) decreases sharply. For any given distance, both the QBER is higher and the SKR is lower during the day compared to the night.

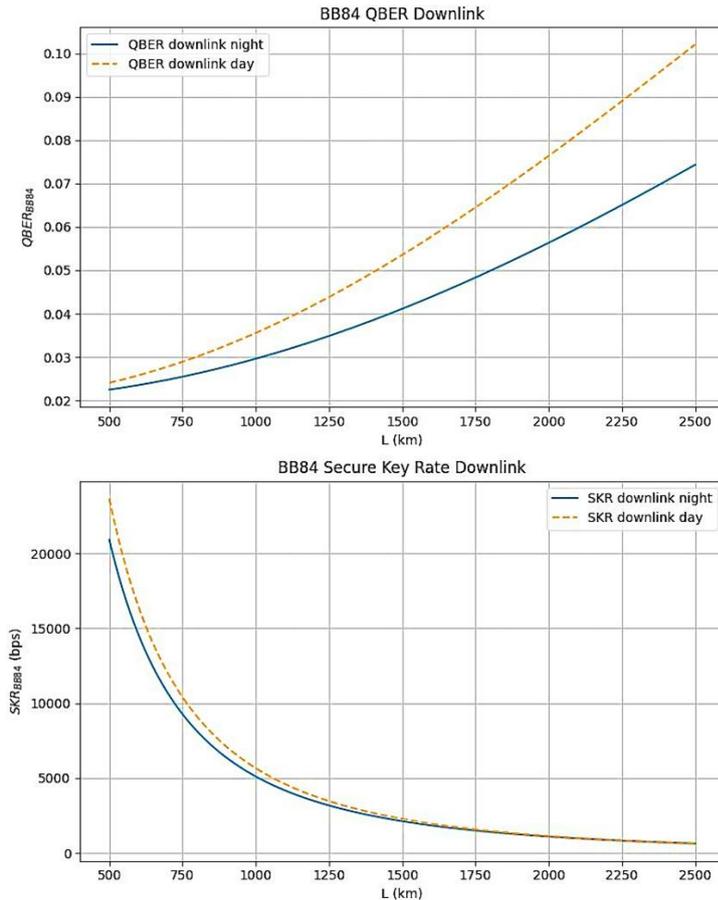


Fig .3 shows the performance of a BB84 quantum key distribution (QKD) downlink over varying distances.

3.3. Simulation Results for B92 Protocol in Free-Space Quantum Key Distribution

Using a Python simulation of the B92 protocol and using Eq.(2), Fig.4 illustrates the relationship between the Zenith Angle, Quantum Bit Error Rate (QBER), and Secret Key Rate (SKR) for (uplink and downlink) and times of operation (day and night).

The simulation results indicate that the degradation in channel quality with increasing zenith angle is physically driven by the exponential growth of atmospheric optical depth. According to the Beer-Lambert law, larger zenith angles lengthen the optical path through the atmosphere, intensifying photon scattering and extinction, which in turn drastically lowers the Signal Noise Ratio (SNR).

The graph shows the relationship between the Quantum Bit Error Rate ($QBER_{B92}$) and the zenith angle during the night for the uplink. We observe that the ($QBER_{B92}$) value gradually increases as the zenith angle increases, at low zenith angles (close to zero), the $QBER_{B92}$ is at its minimum, as the zenith angle increases, the ($QBER_{B92}$) rises noticeably, especially at angles higher than around 60 degrees.

The graph displays the Secret Key Rate (SKR_{B92}) versus the zenith angle during the night for the uplink. It shows an opposite trend to the previous graph, where the (SKR_{B92}) decreases as the zenith angle increases, the secret key rate is highest at low zenith angles. With an increasing zenith angle, the (SKR_{B92}) gradually decreases, and then the decrease becomes steeper at higher angles.

The graph compares the ($QBER_{B92}$) versus the zenith angle for the downlink during the day and night. In general, the ($QBER_{B92}$) increases with the zenith angle in both scenarios (day and night), It appears that the ($QBER_{B92}$) values during the day (red line) are slightly higher than the night values

(dashed yellow line) at higher zenith angles, at low zenith angles, the ($QBER_{B92}$) values are quite similar for both conditions.

The graph illustrates the (SKR_{B92}) versus the zenith angle for the downlink during the day and night. The (SKR_{B92}) decreases as the zenith angle increases for both day (purple line) and night (dashed red line), the secret key rate during the day appears to be significantly higher than that during the night across all shown zenith angles, and decreases gradually initially and then the decrease becomes more pronounced at higher zenith angles in both cases.

A critical physical distinction is observed between link configurations: the downlink consistently outperforms the uplink due to the specific interaction between the laser beam and atmospheric turbulence. In the uplink scenario, the beam encounters turbulence immediately at the transmitter output, leading to severe beam wandering and wavefront distortion that cause significant geometric loss before the signal reaches space. Conversely, in the downlink scenario, the beam propagates primarily through a vacuum, preserving its spatial coherence and minimizing divergence until it reaches the final atmospheric layers. This results in superior photon coupling efficiency and a significantly higher Secret Key Rate (SKR), even under daytime background radiance.

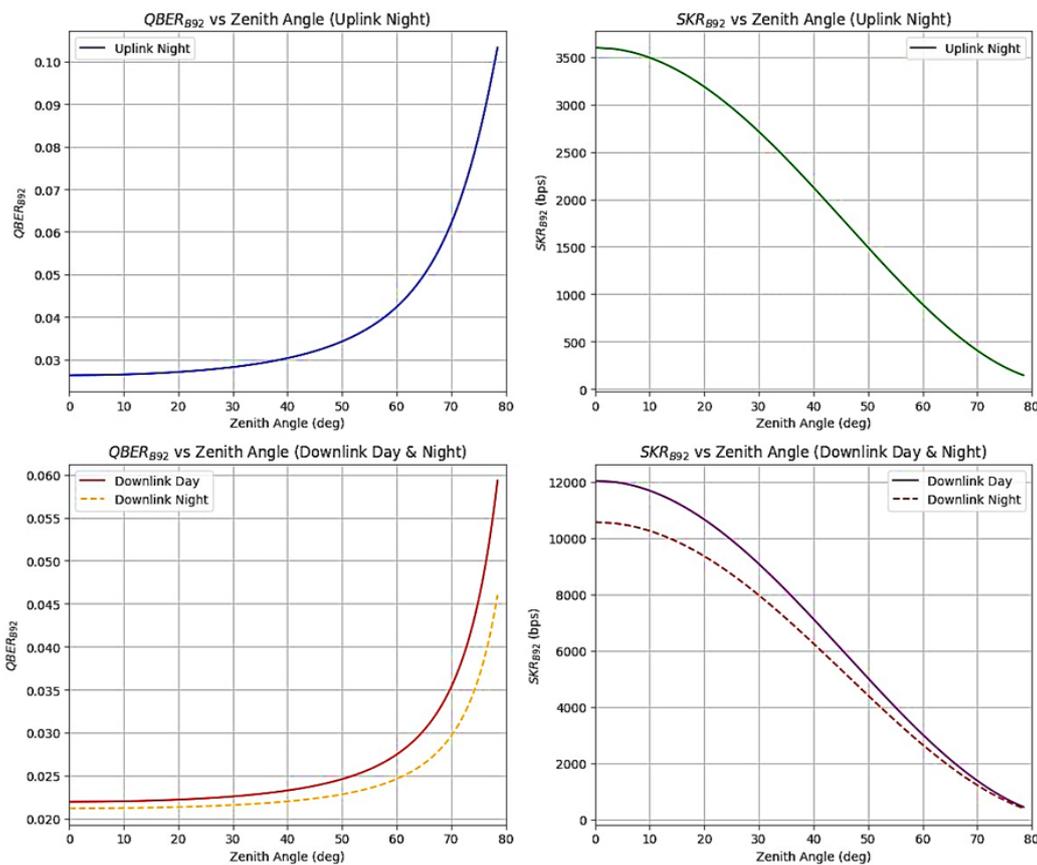


Fig.4 illustrates the relationship between the Zenith Angle, Quantum Bit Error Rate ($QBER_{B92}$), and Secret Key Rate (SKR_{B92}) for different communication links

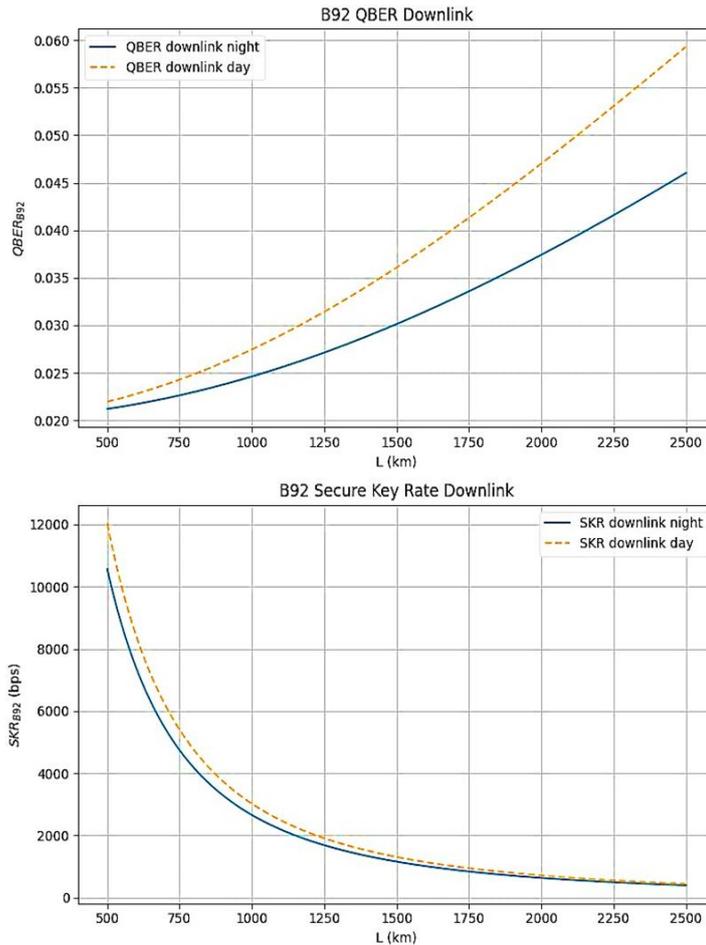


Fig .5 shows the performance of a B92 quantum key distribution (QKD) downlink over varying distances

Based on the graphs in Fig.5, the performance of a B92 quantum key distribution (QKD) downlink is significantly affected by transmission distance and time of day. As the distance increases, the Quantum Bit Error Rate (QBER) rises and the Secure Key Rate (SKR) drops sharply. At any given distance, the QBER is consistently higher during the day, and the SKR is lower during the day compared to night.

3.4. Simulation Results for BBM92 Protocol in Free-Space Quantum Key Distribution

The BBM92 protocol was simulated using a Python environment and Eq.(3), the graph Fig .6 contains four line graphs that present the relationship between Zenith Angle (in degrees) on the x-axis and two different parameters on the y-axis: QBER (Quantum Bit Error Rate) and SKR (Secret Key Rate) for BBM92 protocol.

The graph illustrates the relationship between the Quantum Bit Error Rate ($QBER_{BBM92}$) and the zenith angle during the night for the uplink, the ($QBER_{BBM92}$) shows a gradual increase with the rising zenith angle. At lower zenith angles, the ($QBER_{BBM92}$) remains relatively low, as the zenith angle exceeds approximately 60 degrees, the ($QBER_{BBM92}$) starts to increase more sharply.

The graph presents the Secret Key Rate (SKR_{BBM92}) as a function of the zenith angle during the night for the uplink. The(SKR_{BBM92}) exhibits a decreasing trend as the zenith angle increases, the highest secret key rates

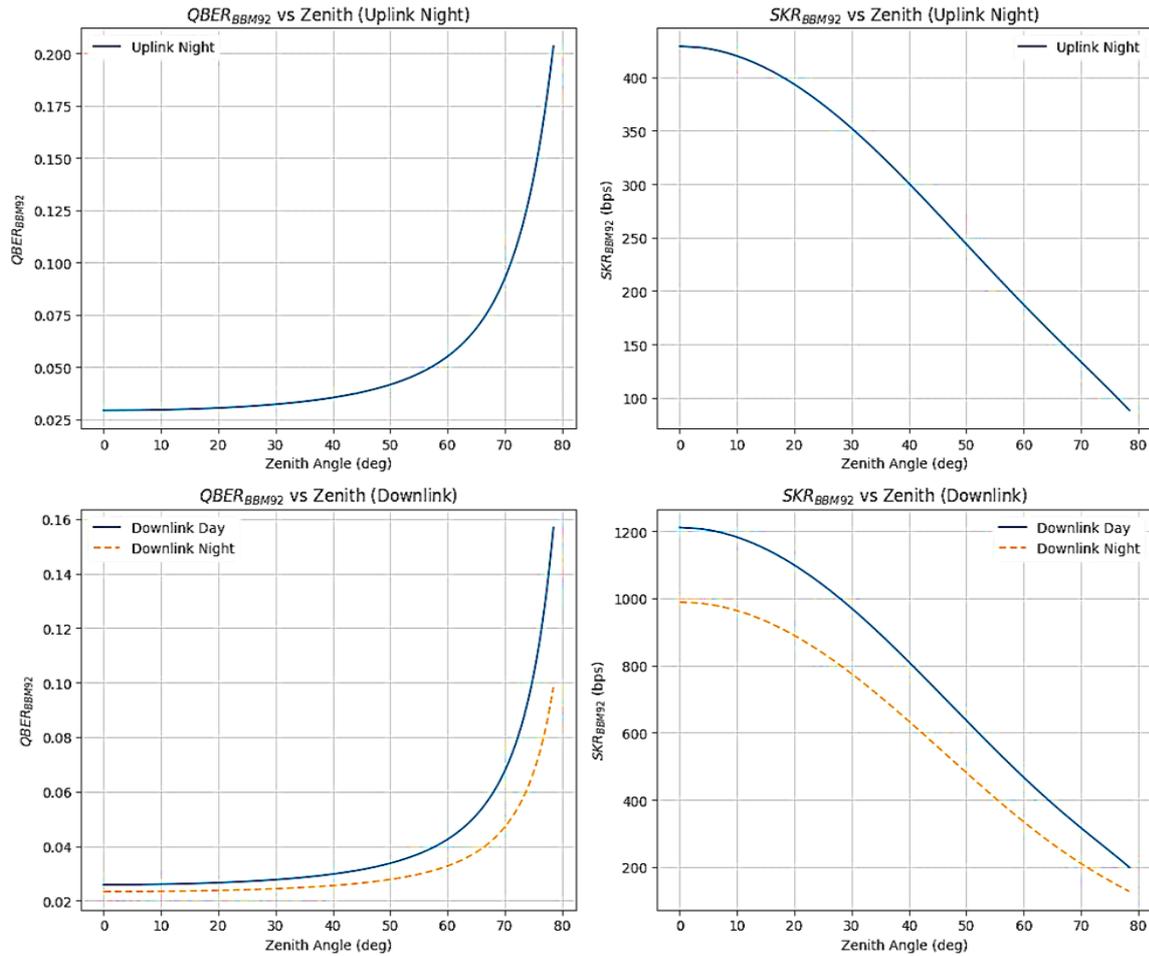


Fig.6 illustrates the relationship between the Zenith Angle, Quantum Bit Error Rate ($QBER_{BBM92}$), and Secret Key Rate (SKR_{BBM92}) for different communication links.

are observed at smaller zenith angles. The rate of decrease in (SKR_{BBM92}) appears to become more pronounced at higher zenith angles.

This graph compares the ($QBER_{BBM92}$) versus the zenith angle for the downlink during both day and night. In both daylight (solid blue line) and nighttime (dashed orange line) conditions, the($QBER_{BBM92}$) tends to increase with increasing zenith angle. The $QBER_{BBM92}$ values during the day appear to be slightly higher than those at night, particularly at larger zenith angles. At lower zenith angles, the($QBER_{BBM92}$) values for day and night are quite close.

The graph shows the Secret Key Rate (SKR_{BBM92}) against the zenith angle for the downlink during the day and night. The (SKR_{BBM92}) decreases as the zenith angle increases for both daytime (solid blue line) and nighttime (dashed orange line).The secret key rate is notably higher during the day compared to the night across the range of zenith angles shown, The decline in (SKR_{BBM92})becomes steeper at higher zenith angles for both day and night.

The graphs are further divided based on the communication link direction (Uplink and Downlink) and time of operation (Night, and Day & Night).

As illustrated in Fig. 6, the performance degradation of the BBM92 protocol with increasing zenith angle is physically driven by the lengthening of the optical path through the atmosphere. This increase in air mass intensifies photon scattering and absorption—governed by the Beer-Lambert law—resulting in a consistent rise in the Quantum Bit Error Rate (QBER) and a monotonic decline in the Secret Key Rate (SKR).

A critical physical asymmetry is observed between link directions: the downlink configuration generally outperforms the uplink. In the uplink, the laser beam interacts with turbulent atmospheric layers immediately upon emission, causing severe beam wandering and wavefront distortion that result in high geometric loss before reaching the satellite. Conversely, the downlink beam propagates through a vacuum first, preserving spatial coherence and maximizing photon coupling efficiency at the ground receiver. regarding temporal effects, the daytime downlink exhibits a higher QBER compared to the night due to the influx of solar background radiance, which introduces noise photons into the quantum channel, elevating the noise floor compared to the pristine, dark-count-limited environment of night operation downlink configuration generally outperforms the uplink

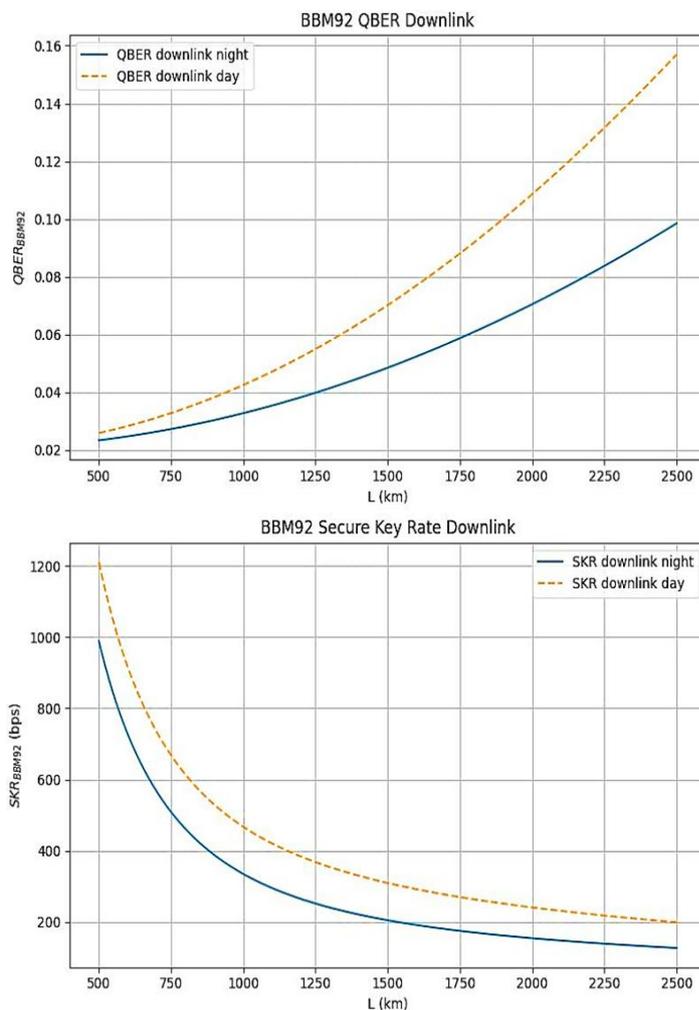


Fig.7 shows the performance of a BBM92 quantum key distribution (QKD) downlink over varying distances

The graphs in Fig.7 illustrates the performance of BBM92 quantum key distribution (QKD) downlink over varying distances (L in km), distinguishing between night and day conditions. The upper graph shows the Quantum Bit Error Rate (QBER) for the BBM92 downlink, indicating that QBER increases with distance for both night and day, with day conditions consistently yielding a higher QBER than night conditions. The lower graph presents the Secure Key Rate (SKR) in bits per second (bps) for the BBM92 downlink. This graph demonstrates that the SKR decreases significantly as the distance increases, with the secure key rate during the day generally being lower than at night for the same distance.

4. Conclusion

This study provided an extensive analysis of the BB84, B92, and BBM92 quantum key distribution (QKD) protocols within satellite-based free-space communication systems. A fundamental observation across all protocols is the inverse relationship between the secure key rate (SKR) and transmission parameters; specifically, the SKR generally decreases, while the Quantum Bit Error Rate (QBER) increases, as both transmission distance and zenith angle increase.

Among the evaluated protocols, BB84 demonstrated superior performance, consistently achieving higher secure key rates and lower QBER compared to the B92 and BBM92 protocols. This superiority was particularly evident in downlink scenarios.

Regarding environmental conditions, the results highlighted significant performance variations between day and night operations in downlink scenarios. Notably, daytime conditions yielded higher secure key rates compared to nighttime for all protocols, despite experiencing higher QBER due to background noise. Specifically for the B92 and BBM92 protocols, the downlink SKR was markedly better during the day, while QBER values remained comparable to nighttime at low zenith angles, showing only a slight increase at larger angles. Furthermore, lower zenith angles were consistently identified as the optimal operational range, maximizing the secure key rate while minimizing errors.

References

- [1 M.A.Nielsen and I.L.Chuang, *Quantum Computation and Quantum Information*, Cambridge,UK: Cambridge Univ.Press, 2010.
- [2 C.H.Bennett and G.Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceeding of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore,India, 1984.
- [3 M.Elboukhari, M.Azizi and A.Azizi, "Quantum key distribution protocols: A survey," *Int.J.Universal Comput.Sci*, pp. 67-59, 2010.
- [4 M.A.Siddiqui and H.Kim, "Performance Analysis of Satellite-Based QKD Protocols Using the Circular Beam Model," *arXiv preprint arXiv:2308.01036*, pp. 1-12, 2023.
- [5 N.Gisin, G.Ribordy, W.Tittel and H.Zbinden, "Quantum cryptography," *Rev.Mod.Phys.*, vol. 1, pp. 195-145, March 2002.
- [6 R.Nandal, A.Nandal:K.Joshi and A.K.Rathee, "A survey and comparison of some of the most prominent QKD protocols," in *Proc.Int.Conf.Intell.Comput.Netw.(ICICNIS2020)*, 2021.
- [7 Muskan, R.Meena and S.Banerjee, "Analysing QBER and secure key rate under various losses for satellite based free space QKD," 2024. [Online]. Available: <https://arxiv.org/abs/2308.01036>.
- [8 D.Y.Vasylyev, W.Vogel and F.S.Semenov, "Atmospheric quantum channels with weak strong turbulence," *Physical Review A*, vol. 3, 2016.