Stealthy Low Earth Orbit Satellite-to-Ground Quantum Communication

Guanqun Song
Department of Computer Science and Engineering, The Ohio State University, United States

Ting Zhu
Department of Computer Science and Engineering, The Ohio State University, United States

Abstract

Quantum key distribution (QKD) leveraging satellites holds promise for global-scale secure communication. However, its practical deployment is threatened by the inherent predictability of satellite orbits, which exposes quantum channels to targeted eavesdropping attacks, compromising the physical-layer security guarantees of QKD. Through security analysis, we demonstrate that such attacks can drastically increase the quantum bit error rate (QBER) from 4.7% to 27.5%, effectively disrupting secure key generation. To address this fundamental vulnerability, we introduce a novel defense framework that integrates two strategies: (1) Stealthy Deployment, which obfuscates quantum satellites within massive LEO constellations to drastically increase an adversary's search space, and (2) Dynamic Re-routing, which is an adaptive countermeasure that re-establishes QKD sessions via alternative paths upon eavesdropping detection. Evaluated through large-scale simulations incorporating real-world satellite data, our framework demonstrates up to a 90% improvement in key generation rate under active attack, ensuring robust and resilient satellite-based QKD without modifications to the underlying quantum hardware.

2012 ACM Subject Classification Security and privacy → Network security

Keywords and phrases LEO satellites, QKD, quantum communication

Digital Object Identifier 10.4230/OASIcs.NINeS.2026.11

Funding This work is partially supported by CQISE Initiative Partnership Seed Award and NSF CNS-2305246.

Acknowledgements We thank our shepherd, Scott Shenker, and the reviewers for their valuable input that significantly improved this manuscript.

1 Introduction

Quantum key distribution (QKD) leverages the fundamental principles of quantum mechanics to provide information-theoretic security, with any eavesdropping attempts introducing detectable disturbances in the quantum states [3, 4]. This security guarantee, embodied in the monitoring of quantum bit error rate (QBER), has propelled QKD from theoretical concept to practical deployment, culminating in recent satellite-based demonstrations that overcome the distance limitations of terrestrial systems [11, 19].

Satellite-based QKD offers a compelling solution to global secure communication by exploiting the vacuum of space for most of the photon transmission path, dramatically reducing losses compared to terrestrial fiber or atmospheric links [18, 8]. As illustrated in Figure 1, quantum-enabled satellites can distribute entangled photon pairs to ground stations across continents, enabling secure key establishment on a global scale.

However, this architectural shift from terrestrial to space-based QKD introduces a fundamental and previously overlooked vulnerability: *the inherent predictability of satellite orbits.* Unlike ground-based quantum channels that can be physically secured, LEO satellites follow publicly known trajectories accessible through Two-Line Element (TLE) data. This predictability enables adversaries to precisely anticipate satellite passes and position

1st New Ideas in Networked Systems (NINeS 2026).
Editors: Katerina J. Argyraki and Aurojit Panda; Article No. 11; pp. 11:1–11:28
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

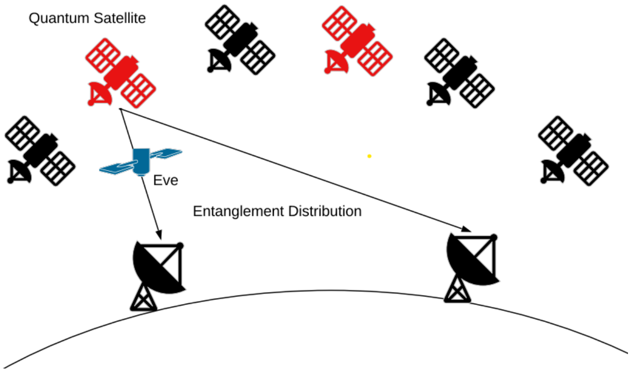


Figure 1 Mixed deployment of quantum and conventional satellites in the same satellite constellation, with alternate quantum satellites reconstituting the quantum key distribution channel after detecting eavesdropping.

themselves for targeted eavesdropping attacks. Worse yet, once identified within a constellation, quantum-capable satellites become high-value targets whose compromise could disrupt entire secure communication networks. Despite growing interest in space-based QKD, existing work largely focuses on physical-layer implementations, and prior work assumes physical-layer guarantees suffice, but ignores system-level attack surfaces introduced by constellation-scale deployment.

In this paper, we investigate defense strategies for satellite-based QKD systems that do not require changes to quantum hardware but instead leverage the inherent characteristics of large-scale satellite constellations [21, 20, 9, 10, 14]. Specifically, our approach employs existing quantum communication theory within LEO satellite constellations, exploiting the distribution characteristics of these satellites. This strategy is designed to be straightforward to implement and highly covert, with the objective of minimizing the exposure of satellites equipped with quantum devices and reducing the risk of QKD channels being eavesdropped on. However, achieving these goals poses a number of challenges, particularly the following three:

- **How to ensure efficient QKD over dynamic satellite-ground links?** Unlike terrestrial QKD strategies with stable fiber or atmospheric channels, satellite-ground QKD is inherently intermittent due to orbital movement, Earths rotation, and line-of-sight constraints. As a result, entanglement distribution opportunities are limited to short time windows when the satellite is in favorable position relative to both ground stations. To support sustainable key generation, we propose a model for the entanglement distribution between satellites and ground stations that predicts the temporal availability of QKD channels based on satellite orbits and optical constraints. The objective is to maximize the distribution of entangled photon pairs during each available window, ensuring that even with the intermittent distribution by a single satellite, sufficient secure keys can be accumulated over time.
- **How to prevent adversaries from identifying quantum-enabled satellites?** In large-scale constellations, quantum satellites often differ from conventional nodes in physical appearance, communication patterns, or orbital behavior. These differences can be exploited by adversaries to isolate and monitor quantum nodes for targeted eavesdropping. We address this threat by proposing a stealthy deployment strategy that conceals quantum-enabled satellites within the broader LEO network, making quantum satellites

indistinguishable from conventional ones under passive surveillance.

- **How to maintain QKD continuity under active attacks?** Even with stealthy deployment, persistent or high-frequency eavesdropping can still compromise QKD sessions by increasing the QBER beyond usable thresholds. To ensure continuity of service, the system must respond swiftly to detected attacks. We introduce a dynamic re-routing mechanism that monitors QBER in real time and automatically reassigns QKD links to alternate satellites upon detecting anomalies. This fast failover strategy reduces downtime and enables secure key generation to resume with minimal interruption.

Our work represents the first comprehensive study of security vulnerabilities in satellite-based QKD from a networking perspective. The key contributions are summarized as follows:

- We develop a data-driven framework that integrates real-world LEO satellite constellations with quantum communication theory. This is the first study to analyze the security and reliability of QKD through satellites in the context of large-scale satellite networks.
- We propose a stealthy deployment strategy that obfuscates quantum satellites within large-scale constellations, reducing the success rate of targeted attacks by orders of magnitude in constellations of thousands of satellites.
- We design a dynamic re-routing algorithm that leverages QKD's sensitivity to eavesdropping to detect compromised links and adapt routing accordingly. Simulations show up to 90% improvement in key generation rate under adversarial attacks.

2 Background and related work

2.1 Quantum Communication

Quantum communication leverages fundamental principles of quantum mechanics to achieve information-theoretic security [17, 16]. At its core is quantum entanglement, where correlated quantum states enable parties to establish shared randomness. Quantum key distribution (QKD), exemplified by BB84 [3] and E91 [6], guarantees that any eavesdropping attempt introduces detectable disturbances due to the no-cloning theorem and measurement disturbance principle. As a result, legitimate parties can monitor the quantum bit error rate (QBER) to determine whether a key is secure.

2.2 QKD via LEO Satellites

While QKD has been successfully demonstrated over fiber-optic and free-space terrestrial links [4], these approaches face severe distance limitations. Optical fibers introduce exponential attenuation (0.2–0.3 dB/km), and free-space terrestrial QKD suffers from atmospheric scattering, turbulence, and alignment constraints. As a result, traditional ground-based QKD is generally limited to distances below 300 km.

LEO satellites offer a compelling alternative [1, 2, 15]. In satellite-based QKD, the photons traverse most of their path through vacuum, minimizing loss and allowing communication over thousands of kilometers [18, 13]. Experiments such as those conducted with China's *Micius* satellite have demonstrated QKD over 1200+ km with key rates in the kilohertz range [11, 19].

LEO satellites orbit at altitudes of 500–2000 km and complete a revolution around the Earth every 90–120 minutes. These satellites periodically come into line-of-sight with ground stations, creating short but recurring time windows suitable for QKD. Each window typically

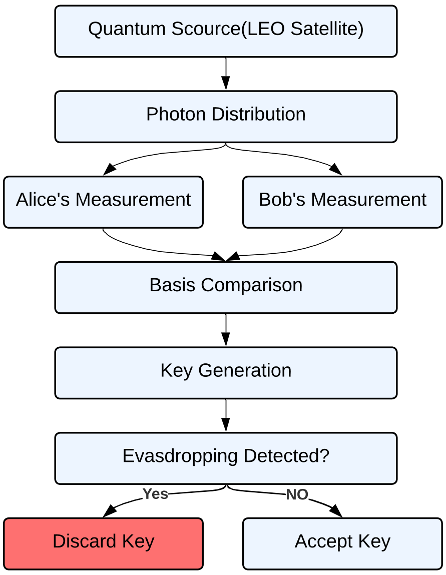


Figure 2 QKD Analysis

lasts 100–500 seconds, during which entangled photon pairs are distributed to two ground stations.

Satellite-based QKD follows a procedure similar to terrestrial protocols but introduces new challenges due to the satellite's mobility, Doppler shifts, beam pointing errors, and dynamic environmental conditions. Furthermore, satellite-ground links suffer from atmospheric attenuation near the Earth's surface and must consider elevation angles to determine visibility and efficiency.

2.3 QKD Security

Existing research on QKD security has primarily focused on *physical-layer* vulnerabilities and countermeasures. Measurement-Device-Independent QKD (MDI-QKD) [17] addresses detection-side vulnerabilities, while device-independent QKD provides security even with untrusted devices. Quantum repeater networks [5, 12] aim to extend range through intermediate nodes, though practical implementation remains challenging.

However, these approaches largely neglect the *system-level* vulnerability introduced by satellite orbit predictability. Prior work on satellite QKD security has concentrated on improving physical transmission efficiency and reducing channel loss [7, 8], with limited attention to protecting the satellites themselves from being identified and targeted. The use of public TLE data for satellite tracking, while essential for coordination, creates an attack surface that has been largely overlooked in the quantum communication literature.

Recent work on satellite network security has addressed classical threats such as jamming and spoofing [21, 10], but these solutions do not account for the unique sensitivity of quantum channels to subtle disturbances caused by eavesdropping.

2.4 Secure Satellite QKD Deployment

The convergence of predictable satellite orbits and the extreme sensitivity of quantum states to measurement creates a critical security gap. Unlike classical communication systems that can tolerate some level of interference, QKD links become unusable when QBER exceeds protocol-specific thresholds (typically 11% for E91). This makes quantum satellites particularly vulnerable to targeted attacks.

Our work addresses this gap by proposing the first system-level defense framework that leverages the scale and redundancy of modern LEO constellations. Unlike hardware-based solutions that require specialized quantum components, our approach operates at the network architecture level, making it complementary to existing physical-layer security measures. By combining *stealthy deployment* to prevent satellite identification with *dynamic re-routing* to maintain service continuity, we create a multi-layered defense that is uniquely suited to the challenges of satellite-based QKD.

3 Threat Model and Design

In this section, we first introduce the QKD model based on the quantum communication E91 protocol. Then, we illustrate the threats of satellite quantum communication, and the defense strategy design overview.

3.1 QKD Model

The system model for satellite-based QKD uses LEO satellites as quantum sources to distribute entangled photon pairs for two ground stations, typically referred to as Alice and Bob. The process of QKD is shown in Figure 2. A full algebraic derivation is deferred to Appendix A.

Once the entangled photons are generated by the satellite, they are transmitted to the ground stations. After receiving the photons, both Alice and Bob perform measurements using randomly chosen bases, such as rectilinear or diagonal bases. Alice and Bob then engage in a process called basis comparison, where they publicly share the bases used for each measurement. They only keep the results where their measurement bases match. Alice and Bob then use the matched measurement results to generate shared secret keys. To ensure the security of the communication, Alice and Bob continuously monitor the QBER. If the error rate exceeds a predefined threshold, indicating a potential eavesdropping attempt, they will discard the affected key. Conversely, if no anomalies are detected, the key is accepted for secure use.

3.2 Threat Model

3.2.0.1 Predictability of Satellite Orbits.

The predictability of satellite orbits, particularly in low Earth orbit, presents a significant security vulnerability for QKD systems. LEO satellites typically orbit the Earth at altitudes ranging from 500 to 2000 kilometers, moving rapidly relative to ground stations. To maintain effective communication, these satellites rely on predictable orbits that allow ground stations to determine when a satellite will be within line-of-sight. While this predictability is crucial for reliable communication, it also exposes the system to potential eavesdropping.

Public TLE data provides precise orbital parameters for satellites, including their inclination, right ascension, eccentricity, and mean motion. Using this data, attackers can accurately predict the satellites position at any given time. This enables them to strategically position eavesdropping equipment at the optimal locations to intercept quantum signals as the satellite passes overhead.

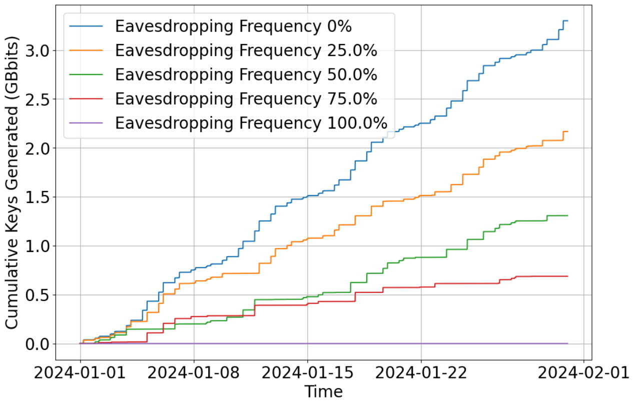


Figure 3 Cumulative keys generated under the Baseline scenario with varying eavesdropping frequencies.

The availability of TLE data allows adversaries to anticipate when and where a quantum-enabled satellite will communicate with a specific ground station. During these predictable communication windows, when the satellite is within the line-of-sight of the ground station, the quantum signals are most vulnerable to interception or jamming. The rapid motion of LEO satellites results in multiple passes over ground stations throughout the day, each representing a potential window of vulnerability.

3.2.0.2 Public Exposure of Satellite-to-Ground Transmission Channels.

The open nature of the transmission channels between satellites and ground stations further exacerbates security risks in satellite-based QKD systems. Quantum satellites, particularly those in LEO, use publicly accessible communication paths that are regulated and standardized to ensure global interoperability. While this transparency supports legitimate communication, it also provides adversaries with detailed information about the operating parameters of satellite-ground station links.

We build a satellite-ground station entanglement distribution simulator to illustrate the impact of Eve's eavesdropping frequency on the secure key generation efficiency. We analyze the cumulative generated keys in the first month of 2024 UTC time. Figure 3 shows total cumulative keys under different Eve's eavesdropping frequencies in the same time range. The total generated keys decrease with the increase of eavesdropping frequency. The results reveal a clear downward trend: as the eavesdropping frequency increases, the number of successfully generated keys declines substantially. Even partial eavesdropping leads to noticeable degradation, and under persistent interception, the QKD channel can be rendered entirely ineffective.

By exploiting these public channels, attackers can monitor the predictable communication windows and attempt to intercept the quantum signals transmitted during these times. Since quantum bits (qubits) transmitted via photons are highly sensitive to measurement, any unauthorized interception will disturb their quantum state, leading to detectable anomalies in QBER. However, the challenge lies in distinguishing these anomalies from natural errors that occur in the transmission process.

3.2.0.3 Targeted Attacks on Quantum-Enabled Satellites.

Once quantum-enabled satellites are identified within a constellation, they become prime targets for adversaries due to their critical role in QKD. These satellites, equipped with advanced quantum communication devices, facilitate the secure exchange of entangled photons between ground stations. The direct interception of quantum states by an eavesdropper (commonly referred to as Eve) is one of the most significant threats to these satellites.

In quantum communication, the no-cloning theorem and the principles of quantum mechanics dictate that any measurement of a quantum state will disturb that state. Eve might attempt to intercept and measure the quantum states using a randomly chosen basis, then retransmit a photon based on her measurement. Although this introduces errors, if the resulting QBER remains below a certain threshold, the attack might go unnoticed, compromising the security of the distributed keys.

The predictability of satellite orbits and the public exposure of transmission channels, combined with targeted attacks on quantum-enabled satellites, create a multifaceted threat landscape for satellite-based QKD systems. Without effective countermeasures, these systems remain vulnerable to interception and interference by adversaries, undermining the security of quantum communication.

4 Defense Model

To safeguard satellite-based QKD against adversarial interception, we propose two complementary defense strategies: (1) stealthy deployment of quantum satellites within a mixed satellite constellation, and (2) dynamic re-routing of entanglement distribution paths. These approaches address the twin challenges of adversarial identification and real-time communication disruption, respectively.

4.1 Stealthy Deployment within a Mixed Satellite Constellation

To reduce the risk of quantum satellites being identified and targeted, we camouflage their operational characteristics within a large LEO satellite network. This strategy includes the following components:

- **Orbital and Visual Camouflage:** Quantum-enabled satellites are assigned orbital parameters and physical profiles that match those of conventional communication satellites. This makes them indistinguishable from other nodes in the constellation when observed via standard tracking or optical means.
- **Functional Obfuscation:** Each quantum satellite is equipped with conventional communication modules and performs standard relay or communication tasks. As a result, its activity profile mimics that of a non-quantum node, adding further ambiguity.
- **Beam Overlap:** Entanglement distribution beams are spatially and spectrally overlapped with classical communication traffic. This beam multiplexing conceals the quantum transmission within broader traffic patterns, complicating signal isolation by potential eavesdroppers.

These techniques collectively reduce the probability that an adversary can detect, track, or distinguish quantum-enabled nodes, thus preempting targeted attacks.

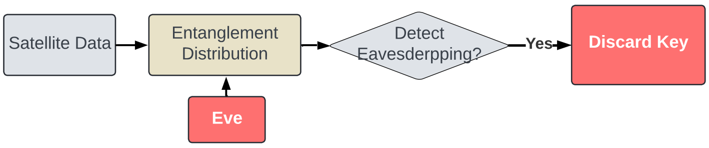


Figure 4 Original Eavesdropping Example.

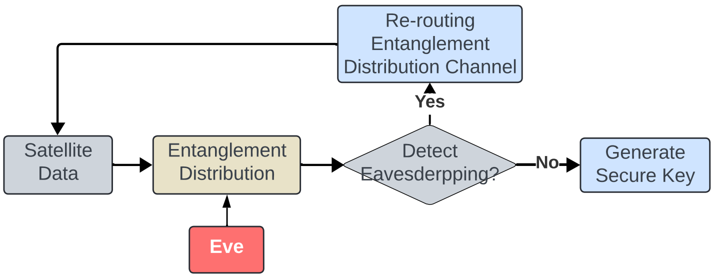

Re-routing Entanglement Distribution Channel
Yes
Satellite Data
Entanglement Distribution
Detect Eavesderpping?
No
Generate Secure Key
Eve

Figure 5 New Eavesdropping Example.

4.2 Dynamic Re-Routing

Despite stealthy deployment, high-frequency eavesdropping attempts may still compromise QKD sessions. To maintain operational continuity, we introduce a dynamic re-routing mechanism that detects anomalies (e.g., elevated QBER) and immediately switches the QKD session to an alternative quantum satellite.

- **Redundant Path Planning:** During the planning phase, each entanglement session is pre-associated with multiple candidate satellites that have overlapping visibility windows. This redundancy enables seamless failover if an attack is detected, and eliminates real-time path calculation overhead.
- **Responsive Channel Switching:** Upon detection of anomalous QBER values, Alice and Bob notify the network to suspend the current session. The QKD task is then re-assigned to a backup satellite with an active line-of-sight to both stations.
- **Resilience to High-Frequency Eavesdropping:** Because each attack only disrupts one session, and the system can immediately resume via another satellite, the adversary must compromise multiple satellites in rapid succession to significantly degrade key throughput.

Figure 4 and 5 illustrate the original and re-designed entanglement distribution processes to defend against detected eavesdropping. Different from the process in Figure 4, the new entanglement distribution process reroutes to a backup quantum source (LEO satellite), allowing a new quantum satellite to continue the QKD execution, thereby mitigating the risk of eavesdropping.

Figure 6 shows the dynamic re-routing process in a satellite-ground station entanglement distribution system. In step 1, the satellite in the top left distributes entangled photon pairs to two ground stations, Alice and Bob. Alice and Bob then measure the received photons and exchange information through the public channel in step 2. However, the QKD fails due

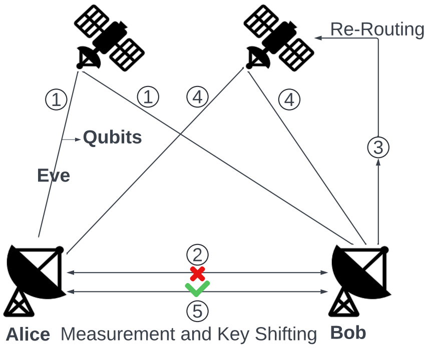


Figure 6 Dynamic Re-routing Process

to Eve's eavesdropping between the satellite and Alice. After detecting the eavesdropping, Alice and Bob notify the satellite constellation and switch the QKD channel via dynamic re-routing. In the last step, the two ground stations generate the secure key based on photon pairs from the new quantum satellite.

5 Space Model

5.1 Satellite Orbit Prediction with Real-World Data

Our space model is built upon real-world satellite data to ensure practical relevance and accuracy. We utilize publicly available Two-Line Element (TLE) data from the Starlink constellation, comprising approximately 6,000 operational satellites at 550 km altitude. The orbital dynamics are simulated using the Simplified General Perturbations 4 (SGP4) model, which provides kilometer-level position accuracy for short-term predictions.

The quantum satellite network consists of satellites $\mathrm{Sat} = \{s_1, s_2, \ldots, s_m\}$ and ground stations $\mathrm{GS} = \{g_1, g_2, \ldots, g_n\}$. Each satellite is characterized by standard orbital parameters:

$$s_i = (\theta_i, \Omega_i, h_i, \omega_i, M_i, n_i, T_i) \tag{1}$$

where θ_i represents inclination (the tilt of the orbit relative to Earth's equator), Ω_i is the right ascension of the ascending node (horizontal orientation), h_i is altitude above Earth's surface, ω_i is the argument of perigee (point of closest approach to Earth), M_i is the mean anomaly (position along orbit at reference time), n_i is the mean motion (orbits per day), and T_i is the epoch time (reference time for orbital parameters).

Ground stations are defined by geographic coordinates:

$$g_j = (\lambda_j, \beta_j) \tag{2}$$

where λ_j is latitude and β_j is longitude.

The SGP4 model predicts satellite positions as:

$$\mathbf{r}_i(t) = \mathrm{SGP4}(s_i, t) \tag{3}$$

with the complete constellation state described by:

$$\mathbf{R}(t) = \{\mathbf{r}_1(t), \mathbf{r}_2(t), \ldots, \mathbf{r}_m(t)\} \tag{4}$$

Our analysis focuses on the current Starlink deployment of approximately 6,000 satellites as it represents a realistic operational scale while providing sufficient diversity for stealth deployment. The methodology naturally extends to future mega-constellations through straightforward parameter scaling.

5.2 Transmission Channel Prediction

Given the known coordinates of the satellite and the ground station, one can calculate the transmission beam range for entanglement distribution. The position of the satellite $\mathbf{r}_{\text{sat}}(t)$ and the ground station $\mathbf{r}_{\text{gs}}$ are used to determine the line-of-sight and the effective communication window. The visibility condition is given by:

$$\mathbf{r}_{\text{sat}}(t) \cdot \mathbf{r}_{\text{gs}} > 0 \tag{5}$$

Considering atmospheric losses, the transmission range of satellite-to-Earth station links is affected by the elevation angle. When considering the effects of the atmosphere, we ignore the effects caused by weather conditions and turbulence. Without considering the interference of background noise, the transmission efficiency η is divided into two parts:

$$\eta_{sg} = \eta_{fs} \cdot \eta_{atm} \tag{6}$$

where η_{atm} is determined by the atmosphere, and η_{fs} is influenced by diffraction, following the same mathematical formulation as the atmospheric transmittance formula used in vacuum conditions. The atmosphere is modeled as an absorbing layer of equal thickness and uniformity everywhere. The quantum distribution link from satellite to ground station, where the distance transmitted in the atmosphere is determined by the zenith angle between the satellite and the ground station ζ, is given by:

$$\eta_{atm}(\zeta) = \begin{cases} (\eta_{atm}^{\text{zen}})^{\sec(\zeta)}, & \text{if } |\zeta| \leq \frac{\pi}{2}, \\ 0, & \text{if } |\zeta| > \frac{\pi}{2}. \end{cases} \tag{7}$$

When the absolute value of ζ is greater than $\frac{\pi}{2}$, the distribution link intersects the ground plane, and in this case, the transmission efficiency is 0. The parameters r, w_0, L_R, and η_{atm}^{zen} are used for the QKD network model.

In the vacuum of space, the photon transmittance from satellite to satellite can be represented as:

$$\eta_{fs}(L) = 1 - \exp\left(-\frac{2r^2}{w(L)^2}\right) \tag{8}$$

where $w(L)$ at the distance L is defined as:

$$w(L) = w_0\sqrt{1 + \left(\frac{L}{L_R}\right)^2}. \tag{9}$$

The transmission channel prediction involves calculating the instantaneous visibility condition, the resulting communication time window, and the transmission beam range while accounting for atmospheric losses. This comprehensive approach ensures that the transmission channel is well-defined and allows for precise targeting, although it also exposes the communication to potential eavesdropping.

At any given time t, a satellite s is considered visible to a ground station g if the elevation angle satisfies:

$$e(\mathbf{r}_s(t), \mathbf{r}_g) \geq e_{\text{min}}, \tag{10}$$

where $e(\cdot)$ denotes the elevation angle between the satellite and the ground station, and e_{min} is a predefined minimum elevation threshold.

A communication link (s, g) is said to be available if this visibility condition holds continuously over a non-zero time interval. Accordingly, the communication time window t_{transmit} is defined as the maximal contiguous interval:

$$t_{\text{transmit}} = [t_1, t_2], \tag{11}$$

such that $e(\mathbf{r}_s(t), \mathbf{r}_g) \geq e_{\text{min}}$ for all $t \in [t_1, t_2]$.

The diffraction angle θ, which represents the transmission beam range, is the area within which the satellite's communication signal can effectively reach the ground station. The angle θ can be derived using the diffraction limit formula, which relates the wavelength λ of the transmitted signal and the initial aperture or beam width D:

$$\theta = \frac{\lambda}{D} \tag{12}$$

The diffraction angle θ describes the extent of this spreading and thus directly influences the effective range of the transmission beam. This range can be calculated considering the satellite's altitude h, the Earth's curvature, and the beam divergence angle θ:

$$\text{Beam Range} = 2h\tan(\theta) \tag{13}$$

5.3 Eavesdropping Impact on Quantum Channel

The public nature of satellite transmission channels enables interception attempts that directly impact quantum bit error rates. We model Eve's capabilities and their system-level effects through a comprehensive analysis of interception mechanics and error propagation.

Eve's interception follows an intercept-resend strategy consisting of photon capture within the beam footprint using strategically positioned equipment, random basis measurement (X or Z basis with equal probability), and photon resending in the measured state to maintain channel appearance.

The quantum bit error rate quantifies eavesdropping impact and is defined as:

$$\text{QBER} = \frac{\text{Number of erroneous bits}}{\text{Total number of bits compared}} \tag{14}$$

For the E91 protocol with ideal equipment, the baseline QBER is approximately 4.7% due to natural channel imperfections. Eve's interception introduces additional errors because with probability 0.5, Eve chooses the wrong measurement basis, and each wrong basis measurement randomizes the resent photon state, creating a 0.25 probability of bit error per intercepted photon.

The resulting QBER under eavesdropping becomes:

$$\text{QBER}_{\text{eve}} = \text{QBER}_{\text{base}} + 0.25 \cdot P_{\text{intercept}} \tag{15}$$

where $\text{QBER}_{\text{base}} = 0.047$ represents the baseline error rate from channel imperfections and $P_{\text{intercept}}$ denotes the fraction of intercepted photons.

To illustrate the basis mismatch impact, consider Alice sending $|+\rangle$ in the X-basis. Eve intercepts and measures in the Z-basis (wrong choice with 50% probability), causing the measurement to collapse the state to $|0\rangle$ or $|1\rangle$ with equal probability. Eve then resends in the measured Z-basis state, and Bob measures in the original X-basis, obtaining an incorrect result with 50% probability. This single interception attempt thus has 25% probability of introducing a bit error, demonstrating the sensitivity of QKD to eavesdropping and validating our threat model.

In summary, Eve's actions, although concealed, introduce detectable errors into the system. By carefully monitoring the error rate, Alice and Bob can identify potential eavesdropping attempts and ensure the security of their quantum communication.

6 System Design

Our integrated simulation framework implements a comprehensive pipeline for evaluating stealthy deployment and dynamic re-routing strategies in satellite-based QKD systems. The architecture comprises three core modules: the **Satellite Data Center** for orbital dynamics and visibility prediction, the **Quantum Simulator** for physical-layer QKD protocol emulation, and the **Dispatch Center** for network coordination and defense strategy execution. These components operate synergistically to maintain robust quantum communication under dynamic network conditions and adversarial threats.

6.1 Satellite Data Center

The Satellite Data Center provides the foundational spatial-temporal context for quantum communication scheduling through precise orbital prediction and visibility analysis. This module continuously ingests publicly available TLE data from operational LEO constellations, with provenance tracking to ensure experimental reproducibility.

The orbit propagation submodule transforms TLE orbital elements into precise Earth-centered inertial coordinates using the standard SGP4 formulation:

$$\mathbf{r}_{\text{sat}}(t) = \text{SGP4}(\text{TLE}_{\text{data}}, t) \tag{16}$$

where $\mathbf{r}_{\text{sat}}(t)$ denotes the satellite position vector at time t derived from the TLE parameters. The propagation outputs latitude, longitude, altitude, and line-of-sight geometry at configurable temporal resolution.

The visibility and entanglement window estimation submodule computes, for each candidate ground-station pair (g_a, g_b), the set of time intervals $W_{s,g_a,g_b} = \{[t_1, t_2]\}$ during which satellite s simultaneously meets minimum elevation and link-quality thresholds for both stations. These windows represent the fundamental temporal constraints for entanglement distribution and are continuously updated as the constellation evolves.

6.2 Quantum Simulator

The Quantum Simulator implements a comprehensive emulation of the E91 protocol with configurable physical parameters and adversarial conditions. This modular framework accurately models quantum state evolution, measurement processes, and environmental effects to provide realistic performance assessment under both ideal and contested operational environments.

The entangled photon generation module initializes quantum states according to the Bell state formulation:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{17}$$

This entangled state ensures perfect correlation between measurement outcomes when identical bases are employed. The simulator generates photon pairs in batches of up to 10^6 entangled pairs per experimental run, reflecting practical satellite emission capabilities while maintaining computational efficiency.

Photon transmission modeling incorporates both free-space and atmospheric effects through a multi-stage efficiency calculation. The comprehensive link budget accounts for diffraction losses, atmospheric attenuation, and pointing errors:

$$\eta_{\text{total}} = \eta_{\text{fs}} \cdot \eta_{\text{atm}} \cdot \eta_{\text{pointing}} \cdot \eta_{\text{detection}} \tag{18}$$

where η_{fs} represents free-space diffraction efficiency calculated using Gaussian beam propagation models, η_{atm} models zenith-angle dependent atmospheric transmittance, η_{pointing} accounts for satellite pointing inaccuracies, and $\eta_{\text{detection}}$ incorporates ground station receiver efficiency.

The measurement and basis selection module implements the core E91 protocol mechanics. Upon receiving photons, Alice and Bob each randomly select a measurement basis from the Z-basis (computational basis) and X-basis (diagonal basis). The Z-basis includes $|0\rangle, |1\rangle$, while the X-basis includes:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{19}$$

Measurements are simulated using matrix operators corresponding to the selected bases. If both parties use the same basis, their results are correlated and retained for key generation.

Key sifting and post-processing implement the classical communication phase of QKD. Following measurement, Alice and Bob publicly compare basis choices through an authenticated classical channel, retaining only outcomes where measurement bases aligned. The sifted key undergoes error correction using low-density parity-check codes with efficiency factor $f(Q) \approx 1.1$, followed by privacy amplification to eliminate potential eavesdropper information. The final secure key rate follows the established formulation:

$$R = S \cdot [1 - f(Q) \cdot H_2(Q)] \tag{20}$$

where S represents the raw key rate, Q denotes the measured quantum bit error rate, and $H_2(Q)$ is the binary entropy function quantifying the information theoretically available to an eavesdropper.

The QBER monitoring and eavesdropping simulation module implements real-time security assessment by continuously tracking the quantum bit error rate across sifted key segments. The simulator incorporates configurable adversarial models, including intercept-resend attacks with basis selection strategies ranging from random choice to optimized interception. When the measured QBER exceeds the E91 security threshold of 11%, the system flags the key material as compromised and initiates countermeasures through the Dispatch Center.

6.3 Dispatch Center

The Dispatch Center operates as the strategic control layer that orchestrates quantum communication sessions and executes defense mechanisms in response to detected threats, bridging predictive capabilities with physical-layer emulation.

QKD session scheduling employs a utility-based optimization that ranks candidate entanglement windows by expected key yield:

$$U(w) = \hat{S}(w) \cdot [1 - f(\hat{Q}(w))H_2(\hat{Q}(w))] - \alpha \cdot C_{\text{switch}}(w) \tag{21}$$

where $\hat{S}(w)$ and $\hat{Q}(w)$ are predicted raw rate and QBER for the window, C_{switch} captures operational switching costs, and α is a tunable trade-off parameter. The scheduler allocates sessions to maximize cumulative expected key yield subject to operational constraints.

The dynamic re-routing mechanism implements our primary active defense strategy by rapidly responding to security incidents. Upon detecting QBER exceeding the policy threshold τ, the system immediately suspends the compromised session and executes a handover to a pre-identified backup satellite that maximizes residual utility within overlapping visibility constraints. To mitigate adversarial forcing through repeated triggerings, the policy incorporates rate-limiting and increasing switch penalties for consecutive failovers, favoring stability unless substantial utility gains justify switching.

Practical considerations for denial-of-service resistance include statistical confirmation of anomalies through multiple QBER samples before triggering costly switches, adaptive penalty mechanisms that increase with switching frequency, and optional randomized backup satellite selection to enhance adversarial uncertainty about quantum payload distribution.

The integrated operation of these three modules creates a resilient quantum communication infrastructure capable of adapting to both natural network dynamics and active adversarial interference. Through continuous monitoring, rapid response mechanisms, and strategic resource allocation, our system design provides the foundation for practical satellite-based QKD deployment in contested environments.

7 Experimental Evaluation

7.1 Experimental Setup and Methodology

Our experimental evaluation employs a rigorous methodology grounded in real-world satellite data and established quantum communication parameters. We utilize TLE data from the Starlink constellation (Space-Track.org, January 2024) comprising 6,174 operational satellites at 550 km altitude across three orbital planes (53ř, 70ř, 98ř). The quantum simulator implements the E91 protocol with parameters validated against Micius satellite experiments: wavelength $\lambda = 800$ nm, transmitter aperture $D = 0.2$ m, receiver aperture $r = 0.5$ m, and baseline QBER = 4.7%. All experiments simulate one-month operational windows with photon pair emission rates of 10 Gb/s, incorporating realistic channel losses and atmospheric effects.

7.2 Satellite Constellation Analysis

Our constellation-wide analysis reveals the fundamental scalability advantages of LEO satellite networks for global QKD. Through large-scale simulation of up to 50 randomly sampled Starlink satellites, we quantify the aggregate availability of secure entanglement links over 24-hour periods. Each satellite provides 8-10 viable QKD windows daily for fixed ground station pairs, with durations of 2-5 minutes. When scaled across multiple satellites, the constellation achieves near-continuous coverage, reducing key generation latency from hours to minutes.

The orbital diversity across inclination planes (53ř, 70ř, 98ř) enables comprehensive global coverage, with mid-latitude satellites serving populated regions and polar orbits en-

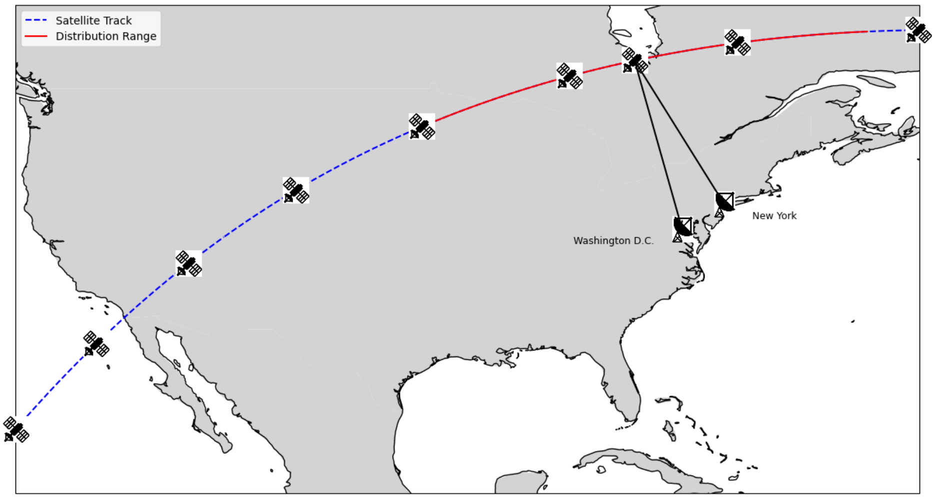
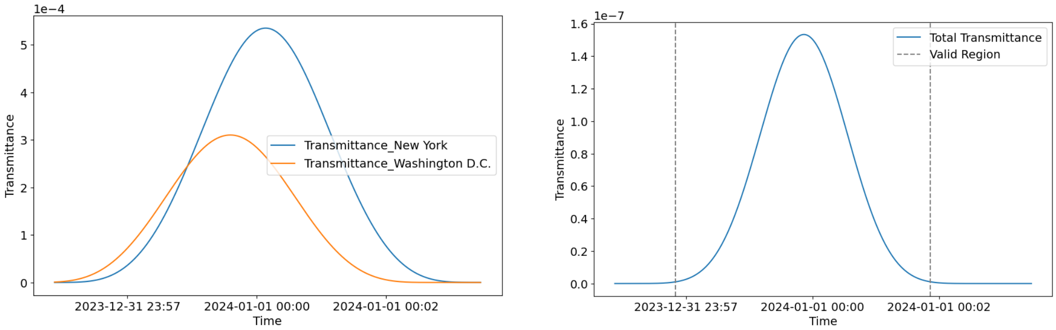


Figure 7 Satellite trajectory projection during the effective entanglement distribution window.



(a) Transmittance rate

(b) Entanglement distribution efficiency

Figure 8 Performance metrics over the distribution window: (a) Transmittance rate to ground stations in New York and Washington D.C.; (b) Entanglement distribution efficiency between the two ground stations.

suring service availability in high-latitude areas. This spatial diversity forms the foundation for our defense strategies, providing the redundant paths essential for both stealthy deployment and dynamic re-routing.

Figure 8 illustrates the photon transmission behavior between one satellite and two ground stations located in New York and Washington, D.C., over a 5-minute window. Specifically, Figure 8a depicts the photon transmittance of the satellite distributing photons to each of the two ground stations. The efficiency rises as the satellite approaches each station and falls as it departs, following the elevation angle. Figure 8b captures the aggregate entangled photon pair transmission efficiency for both links. We define an entanglement distribution as effective if the link efficiency exceeds 1×10^{-9}. The region between the two dashed lines highlights the valid distribution window. Correspondingly, Figure 7 provides a geographic projection of the satellites trajectory during this interval. The satellite trajectory is indicated by the blue dashed line and the red solid line, with the ground stations located in New York and Washington, D.C. The red solid line denotes the orbital segment where the satellite can simultaneously reach both ground stations with sufficient fidelity.

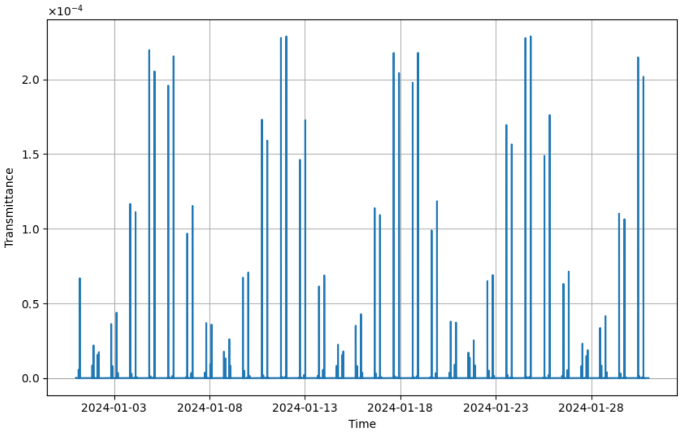


Figure 9 Transmission efficiency over time during January 2024.

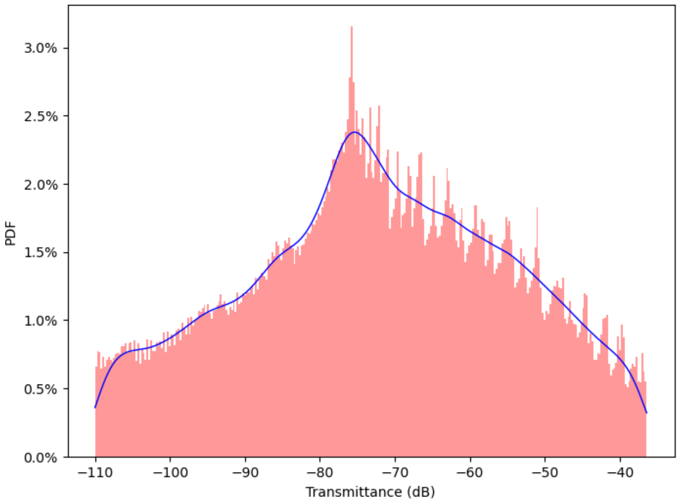


Figure 10 Distribution and PDF of transmission efficiency (dB) for instances above 110 dB.

We simulated the orbital trajectory of a satellite in January 2024 and calculated the entangled photon pairs transmission efficiency of the satellite to two target ground stations over the course of a month. Figure 9 shows the function of transmission efficiency over time. Due to the changing position of the LEO satellite relative to Earth coordinates, continuous quantum entanglement distribution is not possible. Instead, the effective entanglement distribution occurs within specific time windows along the timeline. Despite these intermittent windows, they reoccur consistently, ensuring that a single satellite can reliably distribute entangled photon pairs to both ground stations over long periods. Figure 10 presents the statistical distribution and probability density function (PDF) of transmission efficiency. The figure highlights efficiency values above 110 dB, which represent high-fidelity transmission opportunities suitable for entangled photon pair delivery.

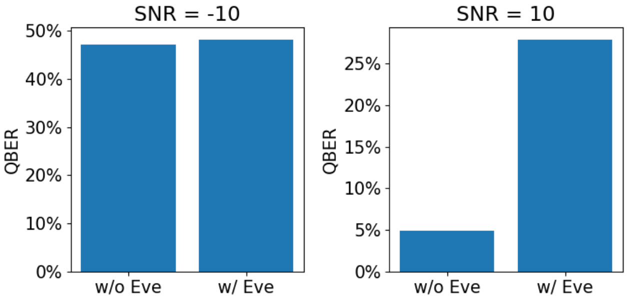


Figure 11 QBER under SNR = -10, 10 dB, with and without eavesdropping.

7.3 Entanglement Distribution

We develop an entanglement distribution simulator that faithfully replicates the full QKD workflow based on the E91 protocol. The simulator encompasses four core stages: entangled photon pair generation, quantum state measurement, key sifting, and QBER estimation.

The qubit generator simulates the emission of 1×10^6 entangled photon pairs per experiment, which are independently transmitted to Alice and Bob. Both parties randomly select measurement bases (Z-basis or X-basis) for each received photon. During transmission, photon pairs are subject to channel noise, and potential interception by an adversary (Eve) is simulated by introducing basis-dependent measurement disturbances. When Eve measures a photon using a basis mismatched with Alice or Bob, the quantum state collapses, potentially altering the final measurement result.

The simulator also incorporates eavesdropping by an adversary (Eve) and noise models to investigate the performance of the entanglement distribution under different environmental conditions and the potential eavesdropping attack effects of Eve throughout the process. We set up different experimental scenarios to analyze the QBER of the entanglement distribution under different conditions. In each scenario, we perform ten experiments where the qubit generator produces 1×10^6 entangled photon pairs per experiment, which are then measured by Alice and Bob. They publicly exchange information to calculate the QBER for each experiment. Our experiment focuses on the QBER as metric for evaluating the effectiveness and security of QKD.

Figure 11 illustrates the QBER observed during the entanglement distribution between Alice and Bob, under signal-to-noise ratios (SNR) of -10 dB and 10 dB. The simulations are performed both in the presence and absence of an eavesdropper, Eve. Under high noise conditions (SNR = -10 dB), the QBER approaches 50% regardless of Eve's presence, indicating that the generated keys are nearly random and therefore unusable. Conversely, under lower noise conditions (SNR = 10 dB), the QBER is 4.7% without Eve's eavesdropping and increases to 27.5% with Eve's eavesdropping. This increase is due to the fact that Eve's measurements have a 50% probability of perturbing the entangled states, so that 50% of these altered measurements yield random 0 or 1 results, resulting in about 25% of the keys being invalid.

Figure 12 further explores the QBER variation with changing SNR levels during entanglement distribution. As SNR increases, QBER decreases in both scenarios (with and without Eve's eavesdropping). However, in the presence of Eve, the QBER plateaus at around 25%, highlighting the threshold below which successful entanglement-based QKD cannot be achieved due to the potential for undetected eavesdropping. For secure key distribution, it is crucial that the QBER remains low, particularly when there is no eavesdropping, and that

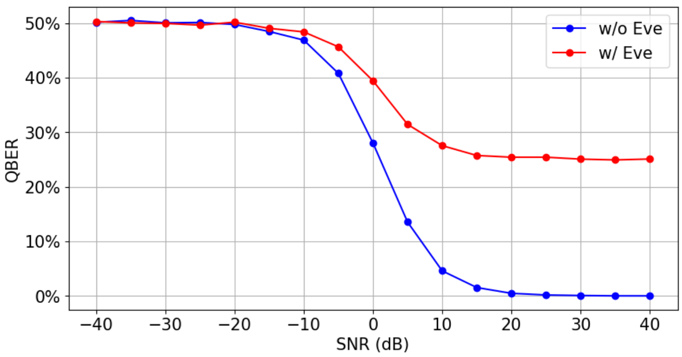


Figure 12 QBER variation with different SNR levels, showing the impact of eavesdropping.

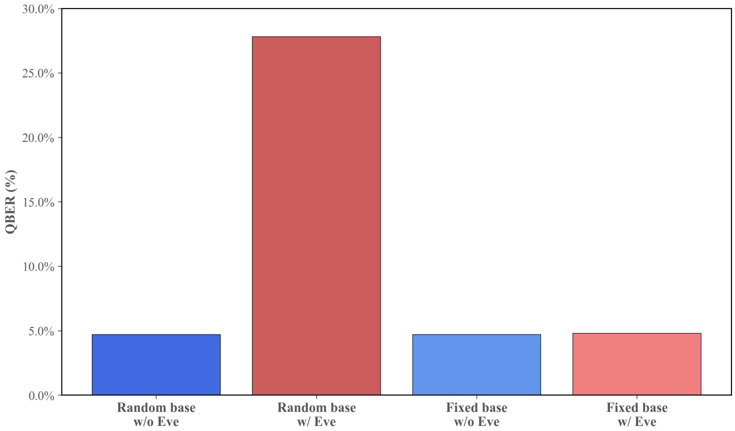


Figure 13 QBER under different measurement base selection, with and without eavesdropping.

the disparity between QBER values in the presence and absence of eavesdropping is substantial, allowing for reliable detection of eavesdropping. The E91 protocol stipulates that keys are valid only if QBER is below 11%, necessitating low-noise conditions for effective entanglement distribution.

Moreover, the influence of randomly selecting measurement bases in contrast to the use of a fixed measurement basis within the E91 protocol was also investigated. Figure 13 demonstrates these options. When Alice and Bob randomly select their bases between the computational basis (Z-basis) and the diagonal basis (X-basis), the presence of an eavesdropper is significantly indicated by an increase in the QBER, which allows Alice and Bob to detect the eavesdropper. However, if Alice and Bob use a predetermined fixed basis (Z-basis or X-basis), and Eve is aware of this basis, there is no significant change in QBER, regardless of whether or not Eve is eavesdropping. This scenario demonstrates the potential security risk associated with the use of a fixed basis, which may prevent Alice and Bob's ability to detect the eavesdropper and thereby compromise the inherent security of quantum communications.

7.4 Defense Strategy Effectiveness

To quantify the practical benefits of our defense strategies, we evaluate three deployment scenarios against increasingly sophisticated adversaries: Baseline, Stealthy Deployment, and

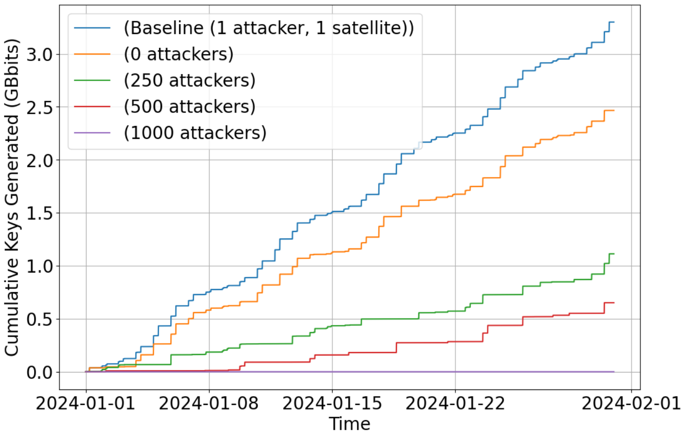


Figure 14 Probability of successful eavesdropping in Baseline vs. Stealthy Deployment Scenarios for a constellation of 6174 satellites.

Dynamic Re-Routing.

7.4.1 Theoretical Security Analysis

In the **Baseline Scenario**, no defense strategies are employed. The quantum-enabled satellite is distinguishable from the rest of the constellation due to its unique hardware configuration, communication scheduling, or orbital parameters. This allows an adversary with modest observational capability to consistently identify and target the satellite during its effective QKD windows. Figure 14 shows the probability of a successful eavesdropping attack under the Baseline and Stealthy Deployment Scenarios. Even minimal adversarial resources (single eavesdropper) can achieve 100% compromise rates, rendering QKD completely ineffective.

In contrast, the **Stealthy Deployment Scenario** conceals quantum-enabled satellites within a large constellation of visually and behaviorally indistinguishable nodes. Under this configuration, the attacker can no longer deterministically target the QKD satellite and must resort to random or exhaustive eavesdropping across the constellation. In a 6,174-satellite constellation, the probability of successful targeting drops to approximately 0.016% per attempt, increasing the adversary's resource requirements by orders of magnitude. As illustrated in Figure 14, this randomized targeting significantly lowers the success rate of eavesdropping, especially when the constellation size is large.

Nevertheless, under high attacker density or persistent adversaries, even randomized eavesdropping may succeed with non-negligible probability. To address this, we introduce a third scenario: **Dynamic Re-Routing Scenario**. Dynamic re-routing provides active defense through spatial and temporal redundancy. In this scenario, quantum satellites leverage the inherent properties of quantum communication to detect eavesdropping attempts. When a rise in QBER or other indicators suggests potential compromise, the current QKD session is aborted, and entanglement distribution is re-established using a backup satellite. Thus, an adversary must eavesdrop on all quantum-enabled satellites simultaneously to successfully disrupt the distribution.

To further quantify defense robustness, we evaluate two metrics: (1) the *attack success rate* given a fixed number of adversaries, and (2) the *required adversarial scale* needed to sustain disruption. Figure 15 illustrates the change in attack success rate with differ-

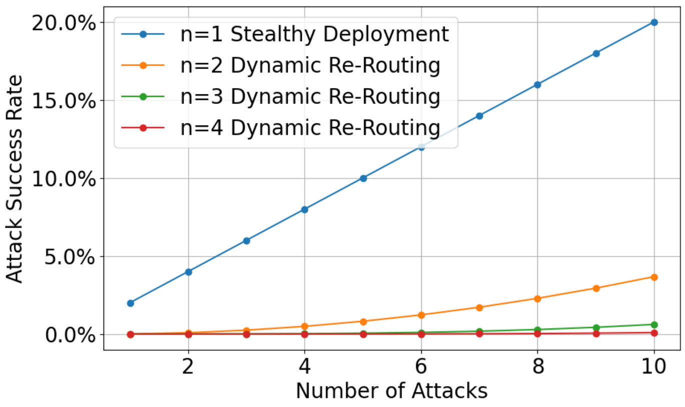


Figure 15 Attack success rate for different numbers of quantum-enabled satellites n in a constellation of 50 satellites.

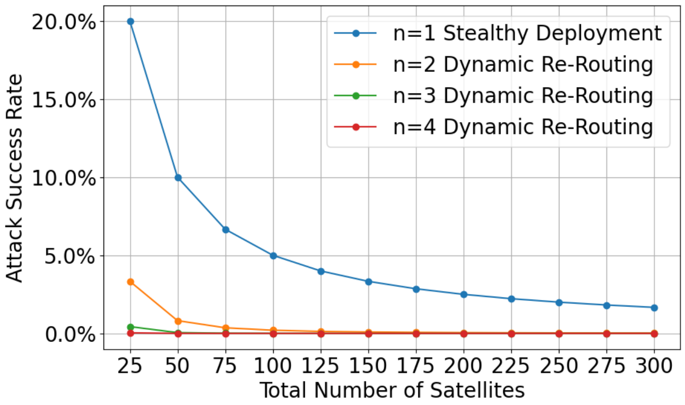


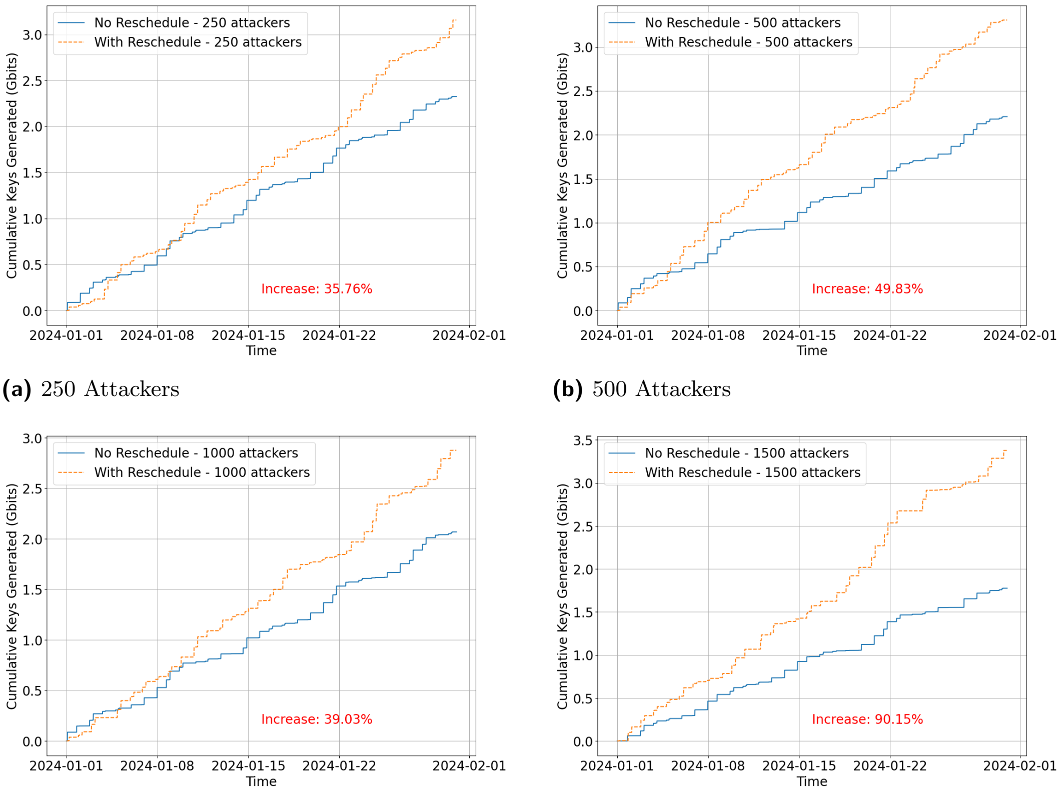
Figure 16 Attack success rate with different total number of satellites in the constellation and 10 eavesdroppers.

ent numbers of quantum-enabled satellites n within a constellation of 50 satellites. When $n = 1$, representing the Stealthy Deployment Scenario, the success rate of eavesdropping increases linearly with the number of attacks. However, for $n = 2, 3, 4$, representing Dynamic Re-Routing Scenarios, the success rate decreases, demonstrating the effectiveness of redundancy in mitigating eavesdropping. Figure 16 further demonstrates that larger constellations substantially decrease attack success probability. Integrating multiple quantum-enabled satellites into mega-constellations can provide practical security enhancement.

7.4.2 Operational Performance Under Attack

In this section, we evaluate the practical effectiveness of our proposed defense strategies over the Starlink satellite constellation under adversarial conditions. Our experiments consider three deployment scenarios: Baseline, Stealthy Deployment, and Dynamic Re-Routing, capturing their respective resilience to varying levels of eavesdropping activity over a one-month simulation window.

Baseline Scenario: In this setting, a single satellite is designated for QKD, and it is continuously monitored by an adversary. As indicated by the baseline curve in Figure 14,



(a) 250 Attackers

(b) 500 Attackers

(c) 1000 Attackers

(d) 1500 Attackers

Figure 17 Comparison of cumulative keys generated with varying numbers of attackers and scenarios.

eavesdropping frequency directly reduces valid key generation, collapsing to zero at 100% coverage, highlighting the critical vulnerability of current approaches.

Stealthy Deployment Scenario: Stealthy deployment provides substantial resilience, maintaining service availability even against hundreds of adversaries. Under this scenario, the adversary can no longer distinguish quantum-enabled nodes a priori and must resort to randomly selecting satellites for interception. As shown in Figure 14, even under full-time adversarial coverage, stealthy deployment significantly reduces the attack effectiveness compared to the baseline. However, as the number of attackers increases, the probability of inadvertently intercepting an active QKD link also increases.

Dynamic Re-Routing Scenario: To further strengthen the system, we incorporate *Dynamic Re-Routing* as an adaptive defense layer. Upon detection of potential eavesdropping, the system seamlessly switches QKD operations to one of several backup satellites. This approach transforms the attacker's challenge from targeting a single node to simultaneously disrupting all redundant QKD links within a narrow time window.

Dynamic re-routing demonstrates good robustness across all tested attack intensities. We conducted simulations under adversarial scales of 250, 500, 1000, and 1500 eavesdropping attempts. Figures 17a–17d illustrate the cumulative key generation over a one-month window, comparing scenarios with and without Dynamic Re-Routing. Compared to Stealthy Deployment, Dynamic Re-Routing consistently preserves a higher cumulative key generation rate.

As the number of eavesdropping attempts increases, overall key generation declines in both settings. However, dynamic re-routing consistently yields substantial gains: +35.8% at 250 eavesdropping attempts, +49.8% at 500 eavesdropping attempts, +39.0% at 1000 eavesdropping attempts, and +90.2% at 1500 eavesdropping attempts. Even under the extreme 1500-eavesdropping-attempts scenario, the system preserves nearly 70% of its potential key generation capacity. This performance stems from the spatial diversity of quantum nodes and rapid failover capabilities, which transform the security challenge from node hardening to network resilience.

Overall, the simulation results validate the efficacy of both stealthy deployment and dynamic re-routing strategies in enhancing the security and reliability of QKD over satellite constellations. Specifically, Stealthy Deployment offers a passive, low-cost enhancement that obscures quantum satellite identities. Dynamic Re-Routing adds a proactive, adaptive mechanism that mitigates attacks even when stealth fails. Together, they provide a layered defense architecture capable of maintaining secure QKD operations across large-scale satellite constellations under a range of adversarial scenarios.

7.5 Discussion and Practical Implications

Our experimental results demonstrate that the combination of stealthy deployment and dynamic re-routing creates a layered defense architecture. Specifically, Stealthy Deployment offers a passive, low-cost enhancement that obscures quantum satellite identities. Dynamic Re-Routing adds a proactive, adaptive mechanism that addresses service continuity when stealth fails. This approach leverages the inherent properties of large-scale satellite constellations (such as spatial diversity and orbital predictability) to create security guarantees that scale with constellation size.

Moreover, our simulations indicate that equipping only a modest fraction of satellites within a large constellation with quantum capability can already yield meaningful redundancy for robust defense while maintaining cost efficiency. In this setting, the dominant additional cost arises from coordinating and scheduling these quantum nodes effectively, rather than from replicating specialized payloads across every satellite. This makes the approach amenable to incremental deployment and compatible with existing constellation architectures.

Most importantly, our strategies transform the fundamental security model of satellite QKD from vulnerable point-to-point links to resilient network-based security, addressing the critical system-level vulnerability that has been largely overlooked in previous work.

8 Conclusion

In this paper, we investigate a comprehensive evaluation of the security risks and mitigation strategies for satellite-based QKD systems operating in LEO scenario. Our analysis shows that predictable orbital dynamics expose such systems to targeted eavesdropping, creating system-level vulnerabilities that cannot be addressed by traditional point-to-point defenses. To address these vulnerabilities, we introduced a two-layer defense framework: *Stealthy Deployment*, which conceals quantum-enabled satellites within large constellations, and *Dynamic Re-Routing*, which ensures service continuity through rapid channel switching when eavesdropping is detected. Large-scale simulations confirm that these strategies substantially reduce attack effectiveness and preserve up to 90% improvement in cumulative key generation under adversarial conditions. By integrating stealth with active resilience, we shift security paradigm from hardening individual point-to-point links to building a robust, network-level defense, thereby enabling truly secure satellite-based QKD.

References

1 Mark Ballard, Guanqun Song, and Ting Zhu. Chain reactions in space: Analyzing the impact of satellite collisions and debris accumulation, 2025. URL: `https://arxiv.org/abs/2512.22429`, `arXiv:2512.22429`.

2 Mark Ballard, Guanqun Song, and Ting Zhu. Satellite cybersecurity across orbital altitudes: Analyzing ground-based threats to leo, meo, and geo, 2025. URL: `https://arxiv.org/abs/2512.21367`, `arXiv:2512.21367`.

3 Charles H Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of cryptology*, 5:3–28, 1992.

4 Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussières, Ming-Jun Li, et al. Secure quantum key distribution over 421 km of optical fiber. *Physical review letters*, 121(19):190502, 2018.

5 Wolfgang Dür, H-J Briegel, J Ignacio Cirac, and Peter Zoller. Quantum repeaters based on entanglement purification. *Physical Review A*, 59(1):169, 1999.

6 Artur K Ekert. Quantum cryptography based on bells theorem. *Physical review letters*, 67(6):661, 1991.

7 Nicolas Gisin and Rob Thew. Quantum communication. *Nature photonics*, 1(3):165–171, 2007.

8 Sumeet Khatri, Anthony J Brady, Renée A Desporte, Manon P Bart, and Jonathan P Dowling. Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet. *npj Quantum Information*, 7(1):4, 2021.

9 Zeqi Lai, Hewu Li, Yikun Wang, Qian Wu, Yangtao Deng, Jun Liu, Yuanjie Li, and Jianping Wu. Achieving resilient and performance-guaranteed routing in space-terrestrial integrated networks. In *IEEE INFOCOM 2023 - IEEE Conference on Computer Communications*, pages 1–10, 2023. `doi:10.1109/INFOCOM53939.2023.10229104`.

10 Yuanjie Li, Hewu Li, Wei Liu, Lixin Liu, Wei Zhao, Yimei Chen, Jianping Wu, Qian Wu, Jun Liu, Zeqi Lai, et al. A networking perspective on starlink's self-driving leo mega-constellation. In *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking*, pages 1–16, 2023.

11 Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, et al. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, 2017.

12 David Luong, Liang Jiang, Jungsang Kim, and Norbert Lütkenhaus. Overcoming lossy channel bounds using a single quantum repeater node. *Applied Physics B*, 122:1–10, 2016.

13 Ji-Gang Ren, Ping Xu, Hai-Lin Yong, Liang Zhang, Sheng-Kai Liao, Juan Yin, Wei-Yue Liu, Wen-Qi Cai, Meng Yang, Li Li, et al. Ground-to-satellite quantum teleportation. *Nature*, 549(7670):70–73, 2017.

14 Davy Romine, Andrew Kingery, Guanqun Song, and Ting Zhu. Slash: Simulation of lisls aboard leo satellite shells, 2025. URL: `https://arxiv.org/abs/2601.02396`, `arXiv:2601.02396`.

15 Muskan Shergill, Zach Thompson, Guanqun Song, and Ting Zhu. Energy efficient lorawan in leo satellites, 2024. URL: `https://arxiv.org/abs/2412.20660`, `arXiv:2412.20660`.

16 Peter W Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical review letters*, 85(2):441, 2000.

17 Yan-Lin Tang, Hua-Lei Yin, Si-Jing Chen, Yang Liu, Wei-Jun Zhang, Xiao Jiang, Lu Zhang, Jian Wang, Li-Xing You, Jian-Yu Guan, et al. Measurement-device-independent quantum key distribution over 200 km. *Physical review letters*, 113(19):190501, 2014.

18 Rupert Ursin, Felix Tiefenbacher, T Schmitt-Manderbach, Henning Weier, Thomas Scheidl, M Lindenthal, Bibiane Blauensteiner, Thomas Jennewein, J Perdigues, Pavel Trojek, et al. Entanglement-based quantum communication over 144 km. *Nature physics*, 3(7):481–486, 2007.

19 Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, et al. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

20 Tianyu Zhang, Hewu Li, Jun Liu, Lu Lu, Qian Wu, Shaowen Zheng, Zeqi Lai, and Yuanjie Li. High-risk leo satellite network path detection based on spatial and temporal delay anomaly analysis. *China Communications*, 20(7):57–71, 2023. doi:10.23919/JCC.fa.2023-0077.202307.

21 Wei Zhao, Yuanjie Li, Hewu Li, and Yimei Chen. A first look at networking-aware leo maneuvers. In *Proceedings of the 1st ACM Workshop on LEO Networking and Communication*, LEO-NET '23, pages 25–30, New York, NY, USA, 2023. Association for Computing Machinery.

A Appendix A: QKD Protocol

In this section, we provide a detailed and self-contained description of the entanglement-based quantum key distribution (QKD) process employed in our system. The protocol follows the standard E91 framework and is adapted to a satellite-based setting. We describe the generation of entangled photon pairs, measurement basis selection, measurement outcomes, key sifting, and security verification. This appendix is intended to provide sufficient background for readers who may not be experts in quantum cryptography, while maintaining consistency with the experimental evaluation presented in the main body of the paper.

A.1 Generation of Entangled Photon Pairs

The satellite acts as a quantum source that generates entangled photon pairs and temporarily stores them in quantum memory before distribution. Each photon pair is transmitted to two distant ground stations, commonly referred to as Alice and Bob. Due to quantum entanglement, the quantum states of the two photons are intrinsically correlated regardless of the spatial separation between the receivers.

The entangled photon pair is initialized in a maximally entangled Bell state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{22}$$

where $|0\rangle$ and $|1\rangle$ represent the computational basis states of a qubit.

In a two-qubit system, the joint state $|00\rangle$ denotes that both photons are in the state $|0\rangle$, while $|11\rangle$ denotes that both are in the state $|1\rangle$. The superposition in Eq. (22) implies that neither photon possesses a definite individual state prior to measurement. Instead, measurement outcomes are probabilistic but perfectly correlated. When Alice measures her photon and obtains $|0\rangle$, Bobs photon instantaneously collapses to $|0\rangle$, and similarly for $|1\rangle$. This correlation property underpins both key generation and security verification in entanglement-based QKD.

A.2 Selection of Measurement Bases

Upon receiving their respective photons, Alice and Bob independently and randomly choose a measurement basis for each photon. In the E91 protocol, two complementary bases are used:

- **Z-basis (computational basis):** $\{|0\rangle, |1\rangle\}$,
- **X-basis (diagonal basis):** $\{|+\rangle, |-\rangle\}$.

The Z-basis corresponds to the classical binary representation and is defined by the states $|0\rangle$ and $|1\rangle$. Measuring a qubit in this basis yields outcomes that can be directly interpreted as classical bits. The X-basis consists of superposition states defined as

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{23}$$

Measurements in the X-basis are essential for detecting disturbances introduced by an eavesdropper. While Z-basis measurements are primarily used for key generation, X-basis measurements allow Alice and Bob to test the integrity of the entangled state and verify whether the quantum channel has been compromised.

A.3 Measurement Process and Correlations

The measurement operators corresponding to the two bases are given by the Pauli matrices:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad X = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{24}$$

Z-basis measurements. If both Alice and Bob choose the Z-basis, the joint measurement operator $(Z \otimes Z)$ is applied to the entangled state:

$$(Z \otimes Z)|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle). \tag{25}$$

The resulting outcomes are perfectly correlated: Alice and Bob both obtain 0 or both obtain 1, each with probability 1/2.

X-basis measurements. If both parties choose the X-basis, the measurement can be equivalently analyzed by applying the Hadamard transform

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{26}$$

to each qubit prior to a Z-basis measurement. Using $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$, the state evolves as

$$(H \otimes H)|\psi\rangle = \frac{1}{\sqrt{2}}(|+\rangle \otimes |+\rangle + |-\rangle \otimes |-\rangle) \tag{27}$$

$$= \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle). \tag{28}$$

Thus, X-basis measurements also yield perfectly correlated outcomes. Regardless of the chosen basis, the entanglement guarantees strong correlations between Alices and Bobs results, forming the foundation of shared key generation.

A.4 Key Sifting Process

Following the transmission and measurement phases, Alice and Bob proceed to the key sifting stage to distill a shared bit sequence. This process is conducted over an authenticated public classical channel.

It is crucial to note that during sifting, Alice and Bob announce only the sequence of *measurement bases* (e.g., Z-basis or X-basis) they employed for each photon. They strictly keep their specific *measurement outcomes* (0 or 1) private. The sifting logic operates as follows:

1. **Basis Matching:** If Alice and Bob chose the same basis for a given photon pair (both Z or both X), quantum mechanics guarantees their results are correlated. These bits are retained as part of the raw key.
2. **Basis Mismatch:** If they chose different bases (e.g., Alice used Z, Bob used X), the measurement outcomes are uncorrelated and random. These bits provide no information and are permanently discarded.

Table 1 presents a concrete example of this sifting protocol applied to a subset of transmitted photons.

Table 1 Detailed example of the key sifting process. Mismatched bases result in the discarding of the corresponding bits.

Photon Pair	**1**	**2**	**3**	**4**	**5**	...	**1000**
Alice's Basis	X	Z	X	Z	X	...	Z
Alice's Result	0	1	1	0	1	...	0
Bob's Basis	X	X	X	Z	Z	...	Z
Bob's Result	0	0	1	0	1	...	0
Action	**Keep**	Drop	**Keep**	**Keep**	Drop	...	**Keep**

Based on the data in Table 1, we can analyze specific instances:

- For **Photon Pair 1**, both parties independently selected the X-basis. Consequently, their measurement results (0 and 0) are correlated and form valid key bits.
- Conversely, for **Photon Pair 2**, Alice measured in the Z-basis while Bob measured in the X-basis. Due to this mismatch, the results are uncorrelated, and the bit is dropped.
- Similarly, **Photon Pairs 3, 4, and 1000** feature matching bases, contributing to the final key, while **Photon Pair 5** is discarded due to a basis mismatch.

By aggregating the results from all instances where the "Keep" action was triggered, the final sifted key is extracted as:

$$\text{Sifted Key} = \{0, 1, 0, 0, \ldots\} \tag{29}$$

This raw sifted key serves as the input for the subsequent post-processing stages, specifically error estimation and privacy amplification, to ensure unconditional security.

A.5 Security and Error Detection

By comparing a subset of their keys, Alice and Bob can estimate the quantum bit error rate (QBER). If the QBER exceeds a certain threshold, it indicates the presence of an eavesdropper, and they discard the keys. If the QBER is below the threshold, they proceed with error correction and privacy amplification to produce a secure final key.

The final key generation rate R after privacy amplification can be calculated as:

$$R = S \cdot \left[1 - f(Q)H_2(Q)\right], \tag{30}$$

where S is the sifted key rate, $f(Q)$ is the error correction inefficiency factor (commonly $f(Q) \approx 1.1$), and $H_2(Q)$ is the binary entropy function:

$$H_2(Q) = -Q\log_2 Q - (1-Q)\log_2(1-Q). \tag{31}$$

This post-processing step compresses the sifted key to remove any partial information that may have been leaked to an adversary, ensuring that the final shared key is information-theoretically secure.