



OPEN ACCESS

EDITED BY

Laszlo Gyongyosi,
Budapest University of Technology and
Economics, Hungary

REVIEWED BY

Aarón Adrián Aguilar Cardoso,
University of Ottawa, Canada
German Granados,
ESPOL Polytechnic University, Ecuador

*CORRESPONDENCE

Urbasi Sinha,
✉ usinha@rri.res.in

RECEIVED 26 April 2026

REVISED 09 August 2026

ACCEPTED 13 August 2026

PUBLISHED 14 September 2026

CITATION

Behera SR, George M and Sinha U (2026)
Round-the-clock QKD over a free-space-
fiber channel with passive polarization-
basis compensation.

Front. Quantum Sci. Technol. 5:1865541.
doi: 10.3389/frqst.2026.1865541

COPYRIGHT

© 2026 Behera, George and Sinha. This is
an open-access article distributed under
the terms of the [Creative Commons
Attribution License \(CC BY\)](#). The use,
distribution or reproduction in other
forums is permitted, provided the original
author(s) and the copyright owner(s) are
credited and that the original publication
in this journal is cited, in accordance with
accepted academic practice. No use,
distribution or reproduction is permitted
which does not comply with these terms.

Round-the-clock QKD over a free-space-fiber channel with passive polarization-basis compensation

Saumya Ranjan Behera¹, Melvee George¹ and Urbasi Sinha^{1,2*}

¹Light and Matter Physics Group, Raman Research Institute, Bengaluru, Karnataka, India, ²Department of
Physics and Astronomy, University of Calgary, Calgary, AB, Canada

Quantum key distribution (QKD) enables information-theoretically secure communication by exploiting the quantum properties of single photons. Real-world deployment of QKD, however, requires reliable operation under uncontrolled environmental conditions where background illumination, atmospheric loss, coupling fluctuations, and polarization drift can significantly degrade performance. In this work, we experimentally demonstrate entanglement-based free-space QKD over an atmospheric channel with a passive, low-bandwidth polarization-correction strategy that avoids high-bandwidth real-time polarization tracking during the QKD acquisition. Using a 50-m free-space optical link implementing the BBM92 protocol, we compensate polarization scrambling arising from fiber birefringence and reference-frame misalignment by optimizing Bob's measurement bases through quantum state tomography. QKD performance is evaluated across three 24-h acquisition campaigns spanning daylight and nighttime conditions, where high background noise, atmospheric fluctuations, and polarization drift pose significant challenges for secure key generation. By combining spectral, temporal, and spatial filtering with optimized coincidence-window selection, threshold-compatible average QKD performance is maintained across these acquisition campaigns. The optimized daylight key rate and QBER are $(6.39 \pm 0.81 \text{ kHz}, 8.05 \pm 1.48\%)$, while nighttime operation yields $(6.98 \pm 0.81 \text{ kHz}, 8.25 \pm 0.85\%)$. Under representative operating conditions with 8.3% QBER, we obtain a final secure key rate of 351 Hz after reconciliation and privacy amplification. To assess loss tolerance, we further emulate attenuation equivalent to a 1 km free-space link using controlled attenuation, demonstrating approximately 6 kHz raw key rate under 30% additional link loss. This attenuation study reproduces the additional loss budget only and does not constitute a physical kilometer-scale free-space demonstration. These results demonstrate that tomography-assisted measurement-basis correction can enable stable free-space entanglement-based QKD without high-bandwidth polarization tracking during key acquisition, providing a basis for future studies of more dynamic terrestrial and satellite-relevant quantum communication links.

KEYWORDS

BBM92, daytime QKD, entanglement, key rate, MUB, passive polarization correction, QBER, quantum communication

1 Introduction

Advances in quantum information science have enabled new approaches to secure communication that rely on the fundamental laws of physics rather than computational complexity. Quantum key distribution (QKD) is one of the most prominent examples of such protocols. Unlike classical cryptographic schemes whose security relies on computational assumptions [Rivest et al. \(1978\)](#), QKD offers information-theoretic security against adversaries with arbitrary computational power. Translating this theoretical security advantage into practical cryptographic infrastructure, however, requires quantum communication systems that remain stable under realistic environmental conditions. In particular, free-space QKD links are subject to atmospheric turbulence, background illumination, temperature fluctuations, and polarization drift, all of which can significantly increase the quantum bit error rate (QBER) and degrade secure key generation.

Free-space quantum channels are especially important for extending QKD beyond metropolitan fiber networks [Toyoshima et al. \(2011\)](#). Because optical fibers suffer from exponential transmission loss, long-distance terrestrial quantum communication often relies on free-space links and satellite relays to distribute entanglement across large distances [Bedington et al. \(2017\)](#). Landmark demonstrations of satellite-based QKD have already established quantum channels spanning thousands of kilometers [Yin et al. \(2017\)](#), [Yin et al. \(2020\)](#). Practical deployment of free-space QKD systems must manage several distinct effects: atmospheric absorption, scattering, turbulence-induced loss and coupling fluctuations, background illumination, and polarization transformations arising from optical fibers, source and receiver optics, and reference-frame misalignment between transmitter and receiver. Most existing polarization-stabilization implementations rely on active tracking systems that continuously monitor a beacon signal and dynamically adjust optical elements to restore the correct polarization basis. While effective, such active feedback architectures increase system complexity and introduce additional hardware requirements that may complicate large-scale deployment.

Before introducing our earlier work, we clarify the terminology adopted throughout this manuscript. The term “passive polarization correction” is used here specifically to distinguish the proposed methodology from the “active” polarization-compensation schemes commonly reported in the QKD literature, which employ continuous real-time monitoring of channel-induced polarization evolution together with closed-loop modulation of optical elements during key distribution. In contrast, our protocol does not modify the polarization state of the transmitted photons during the QKD run. Instead, it employs an intermittent tomography-assisted calibration step between acquisition intervals to determine the measurement basis, after which the measurement settings remain fixed throughout the corresponding BBM92 data acquisition. We acknowledge that the protocol uses prior tomographic information to determine the measurement basis; however, no continuous polarization tracking, beacon-assisted feedback, or real-time polarization correction is performed during key distribution. We introduced this terminology in our earlier work [Chatterjee et al. \(2023\)](#) and retain it here for consistency. The detailed

operational distinction between our methodology and active polarization-compensation schemes is discussed in [Section 2.1](#).

In earlier work from our group [Chatterjee et al. \(2023\)](#), we introduced a measurement-basis optimization technique that compensates polarization rotations by appropriately choosing the measurement bases rather than actively correcting the polarization state during transmission. In that work, the concept was demonstrated in a controlled laboratory setting. The new contribution of the present study is the extension of this tomography-derived measurement-basis compensation method to a stationary atmospheric free-space QKD link, together with day/night acquisition campaigns, environmental robustness analysis, and finite-size post-processing of experimentally generated keys. Using quantum state tomography of the distributed entangled state, we determine the nearest pure state and derive optimized mutually unbiased measurement bases that maximize correlations between Alice and Bob. By projecting measurements onto these corrected bases, the net polarization transformation of the implemented source–fiber–free-space–receiver system can be compensated without high-bandwidth real-time polarization tracking during the BBM92 acquisition. This measurement-based strategy reduces the hardware complexity associated with continuous beacon-assisted polarization tracking, while remaining best suited to links in which the relevant polarization transformation is slow compared with the tomography/calibration cadence. In addition, we report measurements spanning three 24-h acquisition campaigns under varying atmospheric and illumination conditions, and we evaluate the resulting secure key rates using the adopted finite-size security model. We also assess loss tolerance up to an attenuation-equivalent 1 km link by emulating additional loss with a variable optical attenuator in the free-space transmission path.

Our method is designed to achieve a reduced Quantum Bit Error Rate (QBER), which quantifies the rate of errors occurring during the transmission and reception of qubits, as well as an optimized key rate, representing the rate of successfully transmitted qubits over the quantum channel. The experimental prototype of BB84 [Bennett and Brassard \(1984\)](#), the first free-space QKD protocol, was demonstrated over a 32-cm optical link [Bennett and Brassard \(1989\)](#). Our experiment employs the BBM92 protocol [Bennett et al. \(1992\)](#), a variant of BB84 utilizing entangled photons. Unlike BB84, where single photons are prepared in two mutually unbiased bases (MUB), here we measure two photons of an entangled pair at Alice’s and Bob’s ends, projecting them onto the same MUBs.

Instead of an active feedback mechanism to compensate for the polarization scrambling, we perform a quantum state tomography to arrive at optimal measurement bases for any one party, resulting in maximal (anti-)correlation in measurement outcomes of both parties. Taking into account polarization fluctuations in the implemented source–fiber–free-space–receiver system, we show that the optimized measurement bases substantially reduce the QBER and improve the key rate relative to a fixed conventional-basis reference, even when the measured state has low fidelity with the target maximally entangled state. Future work will be required to evaluate this technique in moving-platform or satellite-relevant scenarios where reference-frame changes occur on faster timescales.

Furthermore, we tested the feasibility of QKD using our methods during both day and night. Measurements were carried

out across three 24-h acquisition campaigns. We discuss in detail a representative dataset corresponding to one complete day from the three cycles of data acquisition. The remaining datasets, obtained under different light and weather conditions, are presented and discussed in the [Supplementary Material](#). In this period of time, our location in Bangalore, India, allowed us to experience a dynamic weather pattern, featuring bright sunlight, rain, and partly cloudy conditions. Throughout the period, the rate of pairs detected and background events varied depending on ambient conditions.

A notable outcome of our filtering strategy is that the QBER achieved during daylight operation is comparable to nighttime performance. This near-equivalence arises because the combined spectral, temporal, and spatial filtering suppresses background photons sufficiently that residual errors are dominated by source imperfections and polarization scrambling rather than ambient illumination. This is a desirable property for practical deployment: it implies that daytime performance is not significantly degraded relative to nighttime and that the system does not require reconfiguration between operating regimes.

The significance of this work is that it experimentally tests the corrected-MUB approach outside a controlled laboratory setting, over a stationary atmospheric link connecting two separate facilities. The present experiment does not reproduce moving-platform or satellite dynamics; rather, it establishes a terrestrial baseline for evaluating how tomography-derived measurement-basis compensation performs under realistic daylight, nighttime, weather, and filtering conditions. Future implementations with faster state estimation, reduced calibration overhead, and controlled motion will be needed to assess applicability to rapidly varying links.

The remainder of the paper is organized as follows. [Section 2](#) presents the theoretical background and polarization-compensation framework, [Section 3](#) describes the experimental implementation of the free-space QKD system, [Section 4](#) reports the experimental results together with secure key analysis, and [Section 5](#) concludes with discussion and outlook.

2 Background

2.1 MUB approach

In a recent work from our group [Chatterjee et al. \(2023\)](#), we devised and demonstrated a technique for choosing measurement bases that compensate the net polarization transformation experienced by the distributed entangled state. Instead of performing high-bandwidth active polarization tracking, the method uses quantum state tomography to determine modified measurement bases, thereby improving visibility, reducing QBER, and increasing key rate in the corrected-basis protocol.

To implement this correction, the following steps are executed.

1. We start with a density matrix ρ^{AB} obtained through quantum state tomography. The entangled state which we intended to share between Alice and Bob is given by:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle^A|V\rangle^B + |V\rangle^A|H\rangle^B). \quad (1)$$

2. From the experimentally obtained density matrix ρ^{AB} , we can find the nearest pure state by doing an eigen decomposition such that $\rho^{AB} = \sum \lambda_i |\lambda_i\rangle \langle \lambda_i|$, where $\{\lambda_i\}$ are the eigenvalues and $\{|\lambda_i\rangle\}$ are the corresponding eigenvectors. The eigenvector corresponding to the maximum eigenvalue represents the nearest pure state, as it will have the maximum overlap with ρ^{AB} . This can be quantified by defining fidelity as $F = \langle \lambda_i | \rho^{AB} | \lambda_i \rangle$.
3. It is well known that for a maximally entangled system as shown in [Equation 1](#), unitaries acting on two different subsystems can be reduced to an identity acting on one subsystem and a modified unitary operating on the other subsystem [Coecke \(2010\)](#). Considering this, we can express this nearest pure state in the following form:

$$|\psi\rangle_\rho^{AB} = \frac{1}{\sqrt{2}}(|H\rangle^A|\phi_H\rangle^B + |V\rangle^A|\phi_V\rangle^B). \quad (2)$$

4. In this scenario, while performing coincidence measurements between Alice and Bob, if Alice has measured in $\{|H\rangle, |V\rangle\}$ basis, Bob's measurement in $\{|\phi_H\rangle, |\phi_V\rangle\}$ basis will result in a maximum correlation. From the nearest pure state, we find that the obtained $|\phi_H\rangle$ and $|\phi_V\rangle$ are nearly orthogonal, because of the very high Concurrence of $|\psi\rangle_\rho^{AB}$. So, as our modified measurement settings, we derive one of the orthogonal basis vectors $|\phi_H\rangle$ and find the angles of the waveplates to create a projection corresponding to this basis vector.
5. Similarly, if we consider the state in $\{|D\rangle, |A\rangle\}$ basis, the nearest pure state can be expressed as:

$$|\psi\rangle_\rho^{AB} = \frac{1}{\sqrt{2}}(|D\rangle^A|\phi_D\rangle^B + |A\rangle^A|\phi_A\rangle^B), \quad (3)$$

6. To obtain these modified bases as shown in [Equations 2, 3](#) we can do an inner product of the first qubit with the conventional basis with identity operated on the second. We then derive:

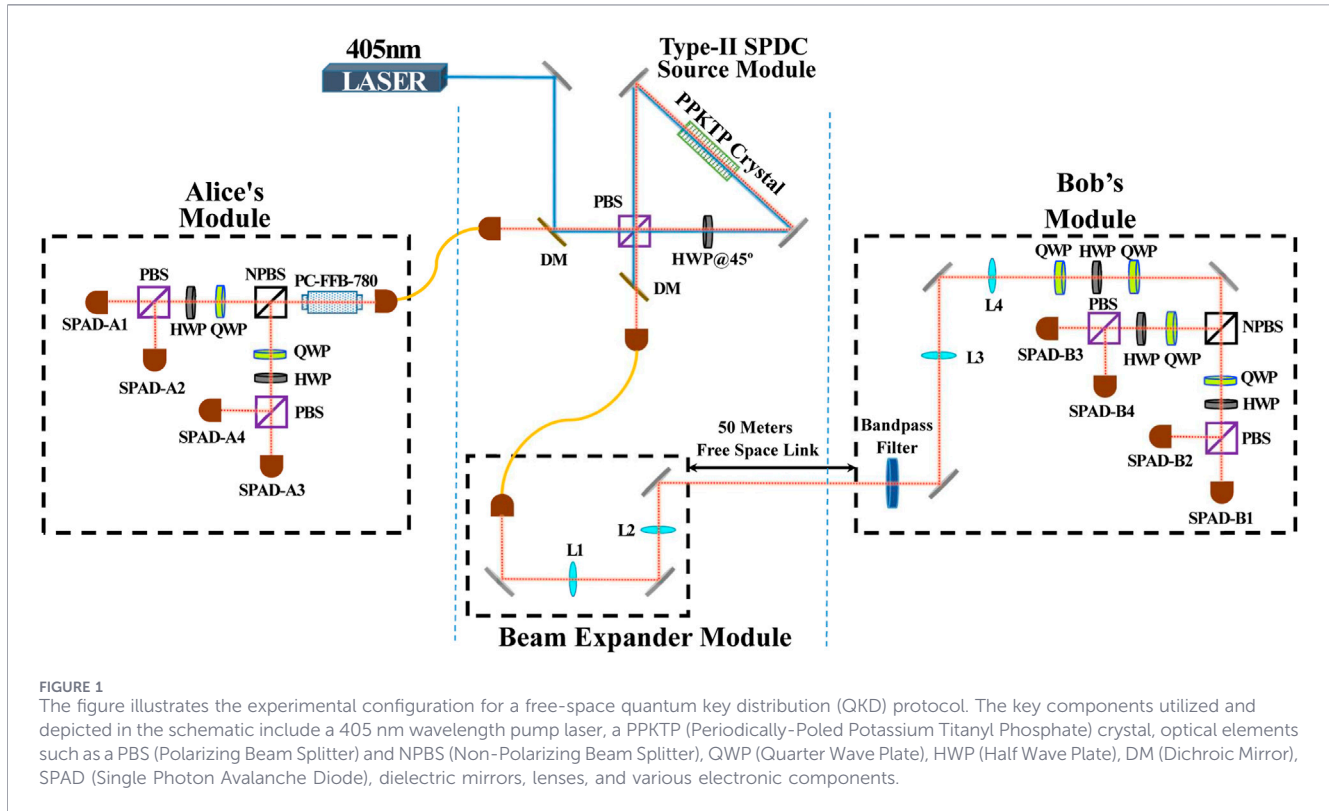
$$|\phi_X\rangle_{Unnormalized} = (\langle X| \otimes I) |\psi\rangle_\rho^{AB}, \quad (4)$$

where $|X\rangle$ is the conventional basis vector.

7. After normalizing the modified basis vector, we create the projection for measurement in the same basis. Experimentally, to measure the photon state in a certain basis we use a combination of quarter-wave plate (QWP), half-wave plate (HWP) and polarization beam splitter (PBS). Jones matrices corresponding to HWP and QWP are given by [Hecht \(2017\)](#):

$$HWP = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix},$$

$$QWP = \begin{pmatrix} \cos^2 \beta + i \sin^2 \beta & (1-i) \sin \beta \cos \beta \\ (1-i) \sin \beta \cos \beta & \sin^2 \beta + i \cos^2 \beta \end{pmatrix},$$



where α and β are the angles between the fast axis of the waveplates and the horizontal plane of reference.

- We know that a measurement at the transmitted port of the PBS, projects the state to $|H\rangle$. Using the newly obtained basis vector $|\phi_X\rangle$ information with the following equation, we can determine our new HWP and QWP angles i.e., α' and β' corresponding to the projection for $|\phi_X\rangle$:

$$|\phi_X\rangle = \text{QWP}(\beta')\text{HWP}(\alpha')|H\rangle. \quad (5)$$

As can be seen in Figure 1, we have positioned detectors on both the transmitted and reflected ports of the PBS. Using Equation 5 we find α' and β' corresponding to projection $|\phi_H\rangle$ in the transmitted port at SPAD-B1. The same angles of the waveplates also create a projection of $|\phi_V\rangle$ in the reflected port of the PBS at SPAD-B2. Similarly, we measure the photons in $\{|\phi_D\rangle, |\phi_A\rangle\}$ basis at detectors B3 and B4, respectively. By doing so, we counter any polarization scrambling that may have happened because of the transmission through the quantum channel. Without any active feedback-based correction, by choosing the correct MUB for measurement, we can now achieve secure communication protocols with low QBER and high key rate.

In this manuscript, the term passive refers specifically to the absence of high-bandwidth, real-time polarization tracking during the BBM92 acquisition. Active feedback systems typically manipulate the polarization state of photons during the run of the experiment using external components such as wave plates, polarizers, and modulators. In such a case, another classical beacon signal may be used on which polarization measurements are performed to obtain the required feedback Xavier et al. (2009); Li et al. (2018). Other approaches include robotized polarization

correction based on an active control system Lee et al. (2022), active polarization tracking, and polarization-basis tracking using the sifted key Toyoshima et al. (2011). Hence, such systems continuously monitor the polarization state of the incoming signal or beacon and apply corrective actions in real time to maintain the desired polarization state of the signal photons. Unlike the methodology for finding modified MUBs to project the photon's state for measurement as given in Equation 4, for active feedback, the unitary transformation that caused the state to change is determined using another beacon source and its polarization state, i.e., $U_{\text{Transformation}}|X\rangle = |\phi_X\rangle$. With this unitary-transformation information, active polarization correction has to be employed using one of the above-discussed processes to reverse the transformation.

Our approach instead uses a tomography-derived calibration step between acquisition blocks to set Bob's measurement bases. Thus, it is not passive in the sense of requiring no calibration information; rather, it is passive during the QKD acquisition because no continuous beacon-assisted tracking or real-time polarization actuation is applied while the BBM92 data are collected. Quantum state tomography is used only to determine the corrected-MUB settings for the polarization-compensated protocol. It is not required for conventional-basis BBM92 measurements, which are performed in fixed Pauli/polarization bases.

A natural question concerns the security of the passive MUB approach under adversarial conditions. In particular, one might ask whether an eavesdropper Eve performing a unitary intercept-resend attack could cause the system to adapt its measurement bases to Eve's resent states rather than the legitimate channel transformation. We note that in the BBM92 protocol, security is guaranteed by the

monogamy of entanglement: any eavesdropping that disturbs the quantum state introduces detectable errors. The MUB correction is derived from quantum state tomography performed prior to the QKD protocol run, and photons used for tomography are not included in the key-generating dataset. If Eve were to intercept and resend, the resulting mixed state detected during tomography would exhibit reduced concurrence and elevated QBER during the protocol, making the attack detectable. The security analysis we apply via the finite-size key rate formula (Equation 8) accounts for this through the QBER-dependent entropy term, which automatically reduces the extractable secure key length as the error rate increases. Thus, the passive correction does not circumvent standard BBM92 security; it operates within the same security framework while reducing hardware complexity.

2.2 Daylight QKD

In traditional QKD experiments, photons are sent over optical fibers or free space in a controlled laboratory environment with low levels of ambient light. However, extending QKD to senders and receivers located at large distances from each other and to daytime scenarios presents unique challenges such as high background noise, atmospheric turbulence, etc. Some major sources of noise for QKD under daylight conditions are:

Background Noise: Daytime environments are inherently brighter due to sunlight, which introduces a significant amount of background noise. This complicates the detection of the single photons, which serve as our quantum signals.

Atmospheric Interference: Earth's changing atmospheric conditions lead to scattering and absorption of quantum signals, further reducing their fidelity and efficiency of being detected.

Temperature Fluctuations: Unlike controlled laboratory temperature conditions, in an outside environment, and particularly in the daytime, we record major temperature variations, which can affect the stability of any optical or optomechanical components, potentially degrading the performance of QKD systems.

The QBER of the system increases significantly during the daytime, much higher than the information-theoretic secure threshold, if there is no adequate noise-filtering system. Daylight QKD was first demonstrated over a distance of 1.6 km in the year 2000 Buttler et al. (2000). Various noise reduction methods must be employed across the spectral, temporal, and spatial domains to successfully remove background photons from sunlight Hughes et al. (2002); Peloso et al. (2009). This comprehensive approach is necessary to reduce QBER, which is a critical factor in ensuring the security and reliability of these systems. Some other approaches include the study of optimal wavelengths that are less affected by background noise from the Sun Avesani et al. (2021); Abasifard et al. (2023); Liao et al. (2017b). The development of entanglement-based daylight QKD systems is still in its early stages, but it is a rapidly growing field of research. The first entanglement-based QKD during the day was performed over several days under varying light and weather conditions Peloso et al. (2009). Recently, entanglement-based QKD in daylight using a quantum dot-based photon source has also been implemented Basset et al. (2023).

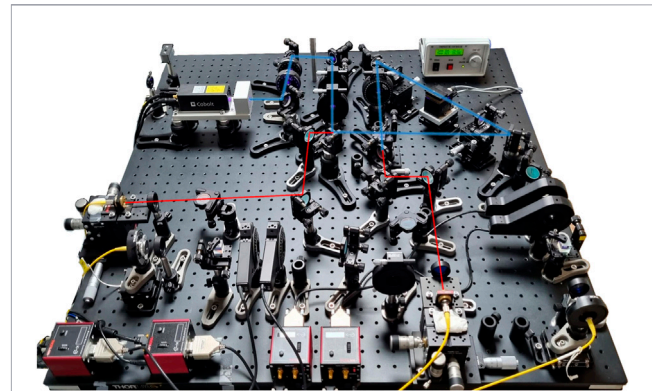


FIGURE 2
Type-II Entangled Photon source with PPKTP crystal under bidirectional pumping within a Sagnac Interferometer. The blue shaded line, a guide for the eye, illustrates the path of the pump beam both before and inside the interferometer. The red dashed line, also a visual guide, represents the trajectories of the entangled photon pair.

2.3 Nighttime QKD

Night-time conditions often lead to lower background noise levels, creating a more favorable signal-to-noise ratio for QKD protocols. It benefits from relatively stable nighttime temperatures, levels of turbulence, and atmospheric interference compared to daytime. Hence, the practical implementation of QKD during night is relatively easier and was successfully achieved in 1998 Buttler et al. (1998) over 1 km of free space distance. The follow-up work by the same group demonstrated 10 km of QKD at night Hughes et al. (2002). Many other experimental demonstrations were performed for nighttime QKD, including hot air balloon experiment Wang et al. (2013), 20 km free space experiments Cai et al. (2024) etc.

Our work reports QKD measurements spanning three 24-h acquisition campaigns under changing atmospheric conditions. We discuss three representative datasets for daytime and nighttime QKD obtained on three alternate days, under varying weather and filtering conditions.

3 Experimental detail and procedure

3.1 Entangled source

Our experimental setup for implementing the BBM92 protocol involves a bipartite source entangled in polarization. This source generates polarization-entangled photon pairs through the spontaneous parametric down-conversion (SPDC) process. It uses a doubly pumped Type-II Periodically-poled Potassium Titanyl Phosphate (PPKTP) crystal configured in a Sagnac arrangement (see Figure 2). We used a set of waveplates to switch between bidirectional and unidirectional pumping of the crystal. Lenses are placed on either side of the crystal to focus and collimate the input and output beams, respectively. As can be seen in Figure 2 we collect the entangled photons from the PBS's output ports and direct them into the single-mode fibers. We also have the

setup for quantum state tomography for initial-state characterization, on the same optical table as the photon source. Our source yields single-photon pairs entangled in polarization with a measured fidelity of 89% with the Bell state $|\Psi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 + |V\rangle_1|H\rangle_2)$ and a Concurrence of 0.9. The entangled source was operated under practical laboratory conditions without active vibration isolation, allowing slow environmental perturbations and alignment drifts representative of realistic deployment scenarios. We transmit these degenerate entangled single photons, at 810nm, to the Alice and Bob modules via optical fibers and free-space quantum channels. On average, the source produces pairs of entangled photons at a rate of 2 MHz. Each optical fiber is accompanied by a Thorlabs fiber-bench polarization controller kit (PC-FFB-780). We do synchronized tomography and obtain almost the same Concurrence and varying fidelity because of the polarization scrambling that occurs due to changing experimental conditions between Alice and Bob, located in facilities separated by 50 m. The observed fidelity degradation over the 24-h cycle arises from two main causes. First, thermal fluctuations throughout the day affect the alignment of the Sagnac interferometer, modifying the relative phase between the two pump directions and thereby degrading the entanglement quality of the prepared state. Second, since a complete tomography requires approximately 30 min and 36 projection measurements, the channel conditions evolve during each tomography run, introducing systematic errors into the density matrix reconstruction. Despite these effects, the MUB correction remains effective because it derives measurement bases from the nearest pure state of the reconstructed density matrix, which retains high concurrence (~ 0.84 on average across all days) even when fidelity with the target Bell state is low. In the implemented stationary free-space link, the dominant polarization drift timescale was experimentally observed to be substantially slower than the 30-min tomography acquisition time, allowing the tomography-derived corrected MUB settings to remain operationally stable for approximately 2–3 h before recalibration was required. Accordingly, during each 24-h measurement campaign, state tomography was repeated at approximately 2-h intervals, resulting in a total of 12 tomography runs per campaign.

3.2 Stationary transmitter and receiver

Our experimental configuration involves two separate facilities, each hosting specialized modules for Alice and Bob. These facilities are located at a distance of 50 m from each other. The process begins with the generation of entangled photon pairs in the same facility as Alice's equipment. These entangled photons are subsequently distributed to both Alice and Bob. Alice's photons are transmitted from the source to Alice via a fiber patch cable, whereas Bob's photons undergo a more complex transmission process. They are first collected through a fiber optic cable and then pass through a series of refractive optics implementing a telescopic arrangement. Finally, they traverse a 50-m free-space link to reach Bob's location.

Furthermore, by including a variable attenuator just before the telescopic arrangement, with the physical 50-m distance that is available, we emulated additional attenuation corresponding to longer-link loss budgets up to an equivalent distance of 1 km.

This controlled-loss study tests the tolerance of the implementation to reduced signal levels; it does not reproduce the full spatiotemporal dynamics of a physical kilometer-scale free-space channel, such as turbulence-driven beam wander, scintillation, or pointing fluctuations over an extended path. For an attenuation setting corresponding to the 1000 m loss budget, we recorded approximately 6 kHz key rate with nearly 30% additional link loss. The specific designs of the transmitter and receiver are described next:

Transmitter: The transmitter module includes the entangled photon source, two 5m single-mode fibers (SMF), and a refractor telescope arrangement for beam expansion between the source and Bob to achieve the free space link. The pair of entangled photons is distributed between Alice and Bob. Photon 1 goes to Alice's detection module, guided by the SMF, whereas Photon 2 is guided through another SMF and evolves into the telescopic arrangement. This is where we perform beam expansion using a combination of two lenses with focal lengths 50mm and 200mm to have 4X magnification. This counters the beam divergence because of the free-space transmission. At the initial alignment stage, we use 633nm and 810nm continuous-wave lasers to establish the link and verify the magnification after the lens combination.

Receiver: Alice, as one of the receivers, has the optics aligned for the state tomography and QKD protocol experiments. Output photons from the SMF go through the polarization controller, followed by a combination of QWPs, HWPs, and PBSs, as shown in Figure 1. These optics help in creating different projections to measure the single photons. There are four different single-photon detectors at the end.

Similarly, Bob has the same polarization optics arrangement at its end, followed by four more single photon detectors. Apart from this, Bob's module also has an 8X demagnification setup consisting of two lenses of focal lengths 200mm and 25mm respectively. A polarization controller setup with two QWPs and one HWP is placed after the lenses for any desired polarization correction (see Figure 1). We use time tagger TT20 and TTULTRA from Swabian instruments at Alice and Bob's ends, respectively, to record the timestamps.

Time Synchronization in QKD: Precise time synchronization is crucial for detecting coincidences in entangled photon pairs, especially in scenarios where detectors are situated at varying distances from the source, as in our experiment where Alice's detectors are closer than Bob's. Synchronization with GPS ensures that Alice's and Bob's systems are properly aligned in time for reliable coincidence identification across unequal path lengths.

Alice and Bob employ highly accurate GPS clocks to establish a common time reference. Pulse Per Second (PPS) signals generated from the GPS units serve as reference points for synchronization. These clocks synchronize with signals from multiple satellite GPSs, providing exceptionally accurate time measures. To achieve this synchronization, we utilize two time-tagging units—TTUltra and TT20 from Swabian Instruments, each with jitters of 34ps and 8ps, respectively, along with two GPS units featuring onboard OCXO (Oven Controlled Crystal Oscillators) from Trimble.

The TTUltra requires a 10 MHz clock signal, whereas TT20 is stabilized with a 167 MHz clock signal from an arbitrary waveform generator (AWG). The stability of each component is essential for

achieving the required synchronization. Each time tagger unit ensures that the photon timestamps recorded on one of its channels are set to a common reference point by using the PPS signal from the respective GPS unit, which is recorded on another channel of the time tagger. The two PPS signals from Alice and Bob's module are then compared to obtain coincidence between single photon detection events. Thus, we maintain robust time synchronization, facilitated by GPS-based clocks and careful calibration of components during the entire experimental run.

Our initial alignment and optimization for the experiment involve the following steps: We establish the link between two laboratories using a visible 633nm laser. As our single photons are of 810nm, we use a laser of the same wavelength to verify magnification and collimation. Also, the optimization of coupling with all four couplers at Bob's end is done using the same laser. As we switch to single photons, we check for coupling efficiencies of all the couplers again and optimize them to have the best possible single photon count detected. With these initial tests, we consider the free-space link ready to be used as our quantum channel. The link is manually aligned and remains static during the acquisition campaigns; no active pointing or tracking system is used. Then, with bidirectional pumping of the PPKTP crystal inside the Sagnac interferometer, we generate and transmit entangled photon pairs to Alice and Bob, and we conduct quantum state tomography, thoroughly characterizing the initial quantum states involved in our experiment. On every incoming photon, both parties measure the polarization in H/V , D/A , and R/L bases to generate the timestamps using which coincidence analysis is then carried out. For a complete tomography, measurement is done in 36 different projections. The main link and filtering parameters available from the experiment are summarized in Table 1.

Table 2 summarizes the distinction between the controlled laboratory demonstration of the MUB correction method in Chatterjee et al. (2023) and the present outdoor implementation and the adaptations used in this work to mitigate operational challenges.

The visibilities in Figure 3 are operational visibilities measured after the full source–fiber–free-space–receiver chain and are therefore not expected to be identical to the source-only Bell-state fidelity and concurrence. These correspond to experimentally measured correlations in the implemented QKD bases. The observed reduction arises from the combined effect of source imperfection, accidental coincidences, analyzer and coupling imperfections, residual polarization transformation, and environmental drift during the acquisition. The visibility data are used here as an operational indicator of basis-dependent correlations for the implemented link, rather than as a source-only characterization metric.

For the corrected-MUB QKD protocol, using the nearest pure state analysis, we determine the new MUBs. Once identified, we adjust the waveplates within Bob's module accordingly to align with the projection associated with these new MUBs (See 2.1) i.e., ϕ_H/ϕ_V and ϕ_D/ϕ_A . Meanwhile, at Alice's station, we perform photon measurements using the conventional H/V and D/A bases. Quantum state tomography is used only to determine the corrected-MUB settings applied at Bob's station; it is not required for conventional-basis BBM92 measurements. In the conventional-basis reference case, Alice and Bob measure in the

TABLE 1 Experimental link and filtering parameters used in the free-space QKD experiment.

Parameter	Value or implementation
Physical free-space distance	50 m
Photon wavelength	810 nm
Transmitter beam expansion	4 × telescope using 50 mm and 200 mm lenses
Receiver collection optics	8 × demagnification using 200 mm and 25 mm lenses
Receiver aperture used in attenuation study	One-inch aperture
Alignment procedure	Manual alignment using 633 nm and 810 nm continuous-wave lasers
Pointing/tracking during campaigns	Static link; no active pointing or tracking
Spectral filtering	10 nm FWHM bandpass filter; 3 nm FWHM filter used for Day 2
Temporal filtering	Fixed 1 ns baseline window and adaptive optimized coincidence window
Acquisition per plotted point	Five BBM92 runs over 5 minutes; each run uses 10 s of data
Spatial filtering	Pinhole-based spatial filtering at Bob, aligned to the incoming beam

Quantities not independently calibrated in the experiment are stated qualitatively rather than assigned numerical values.

fixed laboratory H/V and D/A bases without applying tomography-derived basis corrections. The conventional-basis data are therefore included as a fixed-basis reference under the same implemented link conditions, while the corrected-MUB data correspond to the tomography-assisted measurement-basis compensation protocol. The choice of corrected MUBs results in lower QBER and improved key rate relative to this fixed conventional-basis reference because the modified MUBs at Bob's end restore stronger correlations with the conventional basis choices at Alice's end. The signal-to-noise ratio is consistently higher for the corrected basis, as expected. The visibility in each respective basis served as an indicator of these characteristics. Therefore, for all runs of the protocol, we have chosen these two bases to measure the photons in.

For QKD protocol data acquisition using our SPAD combinations, coincidence measurements are performed in 8 different projections. Among these, 4 projections yield high coincidence counts corresponding to the actual signal, while the remaining 4 produce low coincidence counts representing noise contributions in the system. The sum of all coincidence detections divided by the protocol runtime defines the raw key rate (see Equation 6) Chatterjee et al. (2023). After basis reconciliation, the key rate corresponds to the sifted key rate, i.e., the rate of coincidence detection events where Alice and Bob have chosen the same measurement bases. The final secure key rate is obtained from the sifted key rate after accounting for error correction and privacy amplification. We compute the sifted key rate as

TABLE 2 Comparison between the laboratory demonstration of the MUB correction method in Chatterjee et al. (2023) and the present outdoor free-space implementation, highlighting the experimental challenges and the adaptations introduced in this work.

Experimental aspect	Chatterjee et al. (2023)	Present outdoor free-space experiment	Adaptation in this work
Background illumination	Indoor darkroom environment with no solar background	Daytime operation under solar background	Spectral bandpass filtering and pinhole-based spatial filtering
Temperature variation	Thermally stable laboratory environment	Uncontrolled ambient temperature variations during day–night operation	Repeated tomography and MUB recalibration at approximately 2-h intervals
Polarization transformation	Controlled polarization transformation for studying passive polarization correction	Unknown transformation arising from the combined effects of the source, fiber, free-space channel, and receiver reference frame	Tomography-derived corrected MUBs re-estimated at each calibration interval
Reference-frame alignment	Common laboratory reference frame	Independent Alice and Bob reference frames separated by the free-space span	Initial beacon-assisted alignment using refractive telescope assemblies
Timing synchronization	Single time-tagging unit recording timestamps, requiring only delay adjustment	Alice and Bob operated as separate stations with independent time-tagging units	GPS-disciplined PPS synchronization
Long-duration operation	Short controlled measurement runs	Three 24-h atmospheric measurement campaigns	Round-the-clock data acquisition with repeated calibration cycles

$$\text{Sifted Key rate} = \frac{C(A1, B1) + C(A1, B2) + C(A2, B1) + C(A2, B2) + C(A3, B3) + C(A3, B4) + C(A4, B3) + C(A4, B4)}{T} \text{ (Hz)}. \quad (6)$$

Throughout this manuscript, key rates reported in Hz or kHz denote generated key bits per second, whereas detector count rates and coincidence rates are explicitly identified as count or coincidence rates.

The error contribution in the key distribution is obtained by summing the four undesired coincidence projections. The QBER is then computed by dividing these error bits by the total number of coincidence detections and multiplying by 100, as shown in Equation 7.

$$\text{QBER} = \frac{[C(A1, B2) + C(A2, B1) + C(A3, B4) + C(A4, B3)] \times 100}{C(A1, B1) + C(A1, B2) + C(A2, B1) + C(A2, B2) + C(A3, B3) + C(A3, B4) + C(A4, B3) + C(A4, B4)}. \quad (7)$$

Here, A1, A2, A3, A4 and B1, B2, B3, B4 denote the detectors at Alice's and Bob's stations respectively (see Figure 1), and $C(A, B)$ represents coincidence detection events between the corresponding SPAD pair. T denotes the acquisition time for the protocol. Each point in Figure 4 corresponds to five BBM92 protocol runs conducted over a 5-min interval, with each run comprising 10 s of data acquisition. Using a 1 ns coincidence window together with high-resolution time-tagging electronics, we obtain a high signal-to-noise ratio (SNR) in the coincidence measurements. The reported values of key rate (in kHz) and QBER (in %) are derived from coincidence detections on the order of 10^4 within 10 s of acquisition time.

The identification of coincidence peaks requires precise delay calibration and optimization of the coincidence window. By carefully adjusting the timing offsets and window width, we maximize true photon-pair detections while suppressing accidental coincidences. In order to enhance the practical utility of the QKD system under varying daylight and atmospheric conditions, we employ spectral, temporal, and

spatial filtering combined with the optimized measurement-basis method for polarization correction. Spectral filtering is implemented using bandpass filters with 10 nm FWHM transmission bandwidth, and performance is also evaluated using a narrower 3 nm FWHM filter. Temporal filtering is achieved by optimizing the coincidence window to reject background photons arriving outside the correlated detection window. The optimization strategy, discussed in the Supplementary Material and in Chatterjee et al. (2020), Chatterjee et al. (2023), iteratively adjusts the coincidence window to target threshold-compatible QBER while maximizing the key rate. Spatial filtering is implemented using pinhole apertures at the entrance of Bob's setup and in front of the detectors, aligned with the incident beam diameter to suppress stray background photons. With these combined filtering techniques, our MUB-based polarization compensation method enables stable daylight entanglement-based QKD.

The sifted key generated from the above coincidence analysis is subsequently subjected to error correction and privacy amplification. The expected length of the secure key N_f can be estimated using the finite-size key rate expression Ma et al. (2007); Ecker et al. (2021).

$$N_f \geq N_s [1 - H_2(E) - f(E)H_2(E)] - 2 \log_2 \left(\frac{1}{\epsilon} \right), \quad (8)$$

where N_s is the sifted key length, E denotes the measured QBER, and $H_2(E) = -E \log_2 E - (1 - E) \log_2 (1 - E)$ is the binary entropy function. The term $f(E)$ represents the error correction efficiency, defined as

$$f(E) = \frac{\text{total leakage}}{N_s H_2(E)}, \quad (9)$$

quantifying the ratio between the practical information revealed during reconciliation and the Shannon limit. In our implementation, the security parameter is chosen as

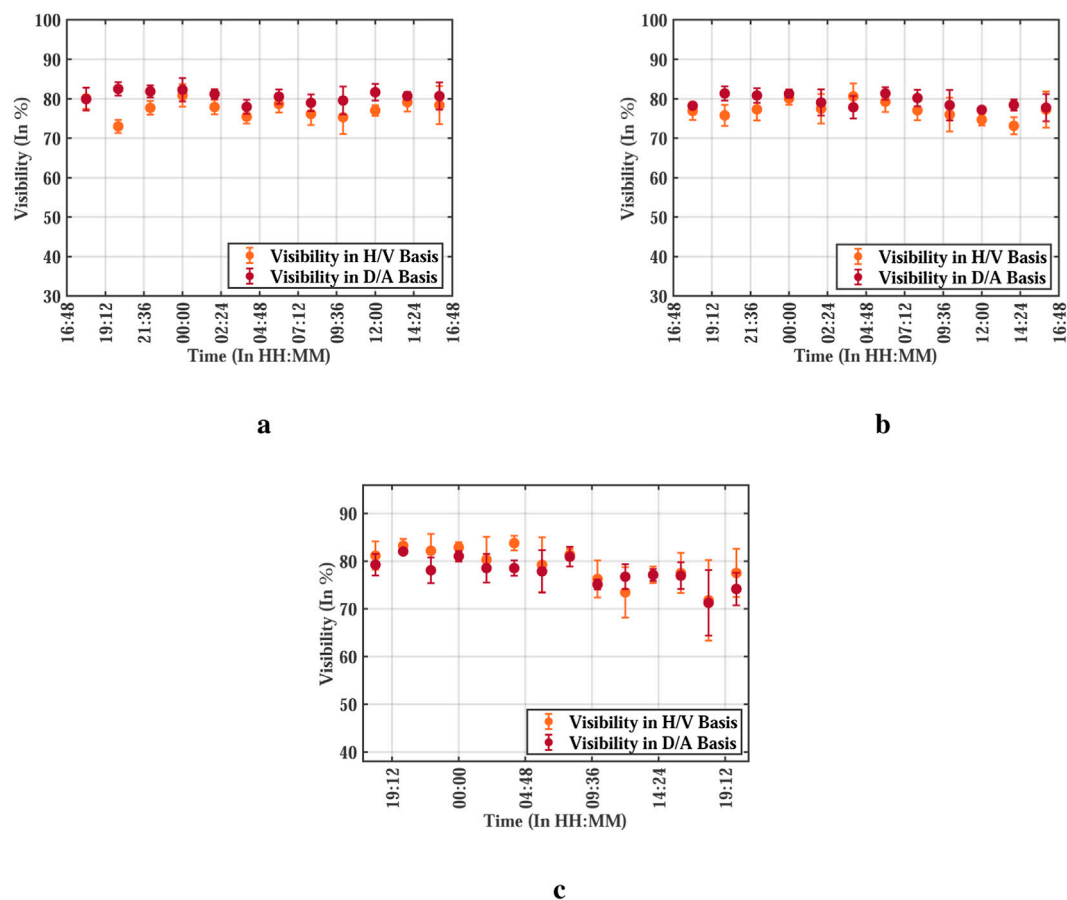


FIGURE 3

Visibility in H/V and D/A basis. (a–c) correspond to data taken on the first, second and the third day, respectively. Each point with the error bar in the plots corresponds to visibility data obtained from five iterations of the QKD protocol done for a single corrected MUB. (a) Day 1 visibility data. (b) Day 2 visibility data. (c) Day 3 visibility data.

$\epsilon = 2 \times 10^{-40}$. The entropy term $N_s H_2(E)$ provides an estimate of the information potentially accessible to an eavesdropper based on the observed QBER, while the term $N_s f(E) H_2(E)$ accounts for the information disclosed during error correction. The subtraction term $2 \log_2(\frac{1}{\epsilon})$ reflects the privacy-amplification security penalty associated with two-universal hashing and is most directly justified in the QKD setting by the Leftover Hash Lemma Tomamichel et al. (2011); Bennett et al. (1988) against quantum side information. The parameter ϵ quantifies the maximum deviation of the generated key from an ideal uniform key in trace distance. In this work, the reported secure-key values are obtained from the adopted Shannon-entropy-based finite-size model applied to the experimentally measured data.

The experimentally measured coincidence statistics determine the sifted key rate and the average QBER used in Equation 8. In the implemented post-processing pipeline, the sifted key is partitioned into fixed-size 6000-bit blocks, each block is assigned an effective error estimate, and a rate-adaptive LDPC code is selected from a predefined candidate set. Accepted blocks are concatenated before privacy amplification, while blocks that fail reconciliation are excluded from the final key. This establishes a direct quantitative link between the physical channel performance, post-processing efficiency, and the achievable secure-key output under the adopted

approximation. For the block-wise reconciliation analysis reported here, the effective error level of each 6000-bit block was estimated offline from the recorded sifted data and used to guide code-rate selection.

Successful block acceptance requires both syndrome consistency and CRC32 verification of the reconstructed block. A Cascade-based fallback is available in the implementation for blocks that fail LDPC decoding; however, it was not invoked in the representative dataset reported in Section 4.1. In Equation 9, total leakage denotes the sum of disclosed syndrome bits and any publicly revealed verification bits.

4 Results

We performed the free-space QKD experiments on different days under changing weather conditions. We now discuss results from three 24-h acquisition campaigns, each comprising repeated BBM92 runs collected during both daytime and nighttime operation. We focus primarily on the dataset shown in Figure 4. During the nighttime portion of the first 24-h acquisition campaign, the experiment was conducted under clear weather conditions, while the daytime session experienced bright sunlight. As illustrated in

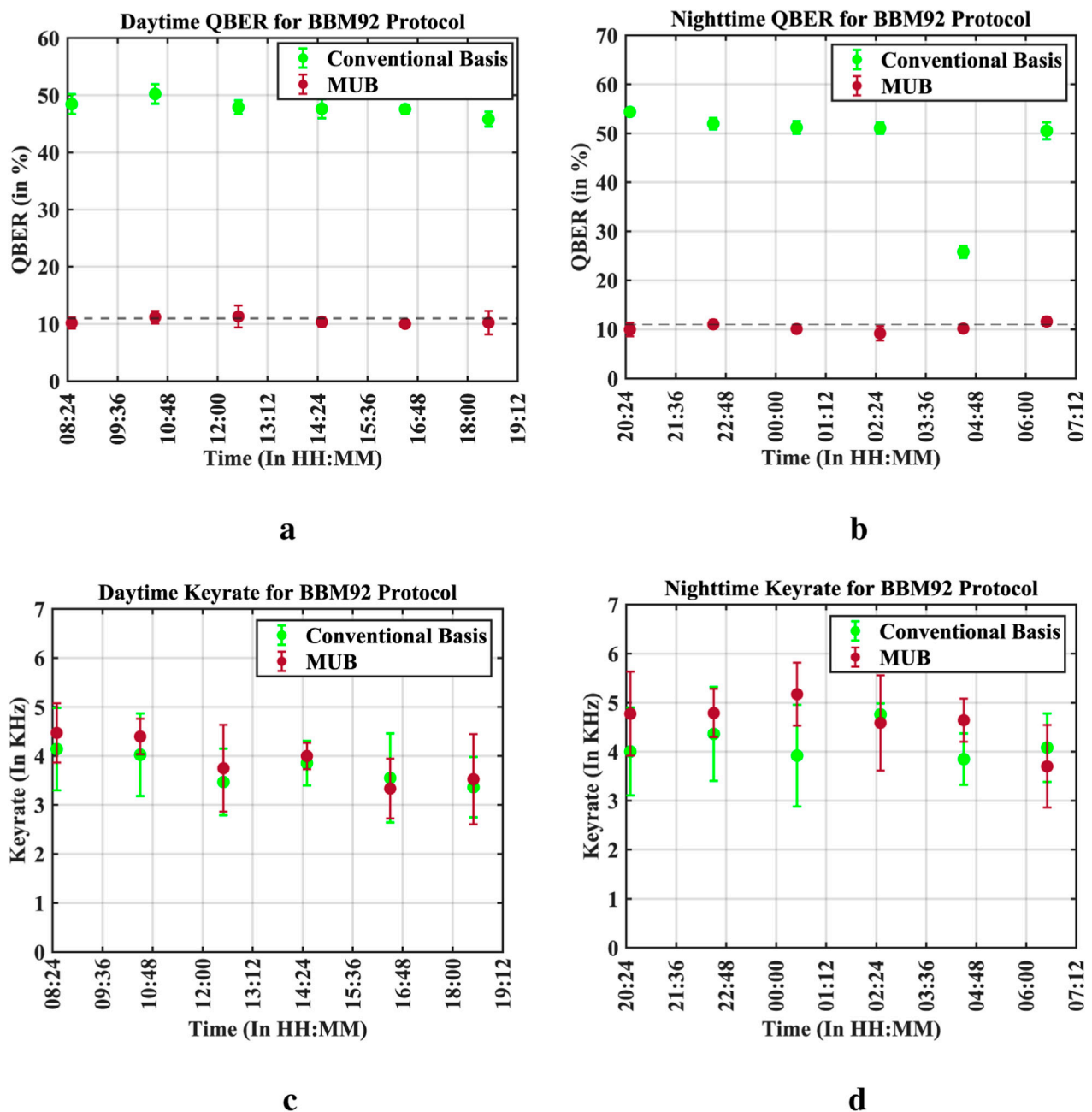


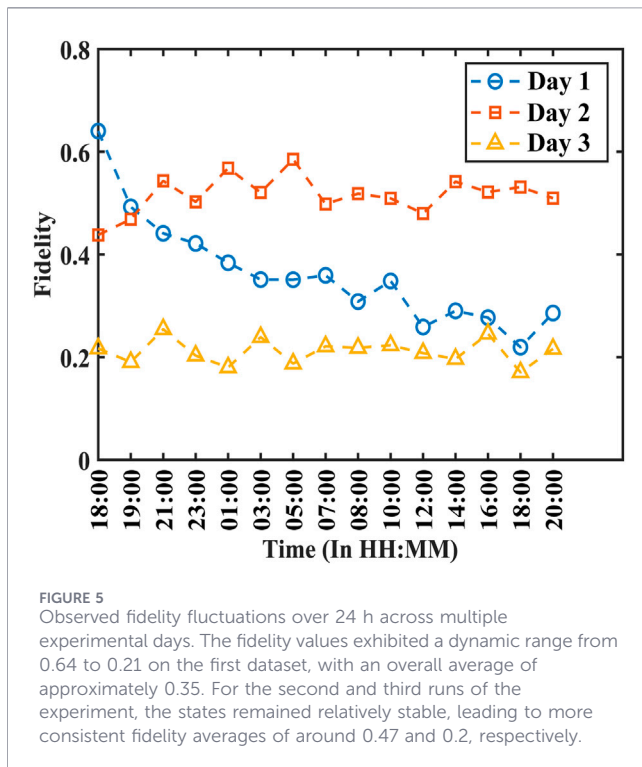
FIGURE 4 Experimental free-space QKD data for Day 1 were analyzed using a fixed coincidence window of 1 ns. (a,c) compare the QBER and key rate for daytime operation using the fixed conventional-basis reference and the corrected MUB. (b,d) show the corresponding comparison for nighttime operation. This dataset represents the baseline analysis under identical coincidence-determination conditions for both basis choices. Average daylight key rate and QBER = $(3.91 \pm 0.73 \text{ kHz}, 10.55 \pm 1.34\%)$. Average nighttime key rate and QBER = $(4.61 \pm 0.81 \text{ kHz}, 10.35 \pm 1.25\%)$. (a) Daytime QBER. (b) Nighttime QBER. (c) Daytime keyrate. (d) Nighttime keyrate

Figure 4, the fixed-window baseline analysis provides the reference performance before coincidence-window optimization.

We obtained an average daylight key rate and QBER of $(3.91 \pm 0.73 \text{ kHz}$ and $10.55 \pm 1.34\%)$ and nighttime key rate and QBER of $(4.61 \pm 0.81 \text{ kHz}$ and $10.35 \pm 1.25\%)$, respectively. Although comparable performance is achieved in both regimes due to filtering techniques, nighttime operation naturally provides a slightly improved signal-to-noise ratio. The near-

equivalence of daytime and nighttime QBER confirms that the dominant error contributions in our system are polarization scrambling and source imperfections rather than background illumination, validating the effectiveness of our multi-domain filtering approach.

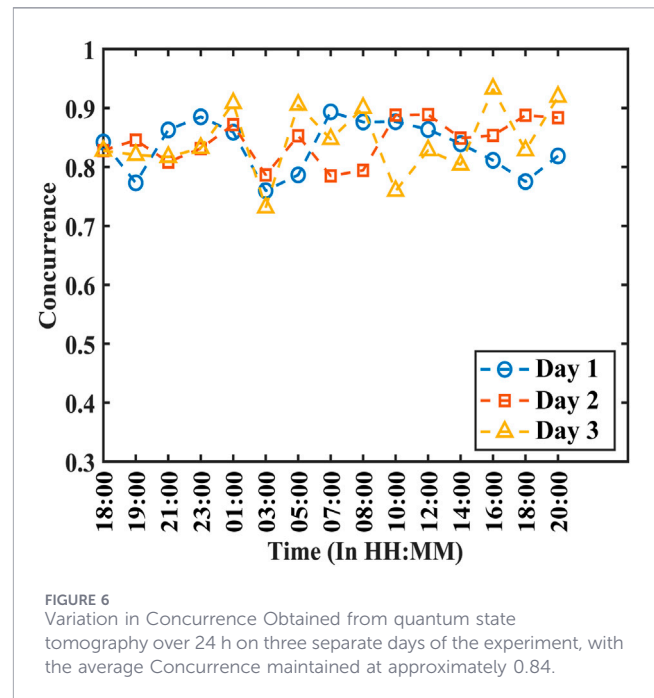
In a similar manner, experiments were repeated on two more alternate days under different spectral filtering and weather conditions (see the [Supplementary Material](#) for additional data).



We found that our system works the same with different spectral filtering at the receiver's end. This is primarily due to the filtering applied at the source using bandpass filters of FWHM of 3 nm around 810 nm of central wavelength. As a result, the number of single photons transmitted through free space remains largely unaffected by the narrower bandpass filter at the receiver. Despite the variability in weather conditions, our results consistently reveal robust performance, with both good key rate and QBER that generally maintain information-theoretic security.

Also, it is worth noting that on the last day we measured a fidelity of approximately 0.2 with the Bell state $|\Psi^+\rangle$, as shown in Figure 5. This is reflected in the conventional-basis data, where the QBER exceeds 70% for some points. For the corrected-MUB analysis, the nighttime data generally remain below the 11% threshold, while daytime points require the coincidence-window optimization discussed below. Although the reconstructed states maintain relatively high concurrence, the fidelity with respect to the target Bell state is reduced under the implemented experimental conditions. Consequently, the fixed laboratory H/V and D/A measurement bases are no longer optimally aligned with the dominant correlation basis of the shared entangled state. This effective basis rotation leads to reduced experimentally observed visibility and correspondingly increased QBER in the conventional basis implementation, despite the underlying entanglement remaining preserved. The corrected-MUB approach compensates for this basis mismatch by determining the effective correlation basis from the reconstructed density matrix.

Since a complete state tomography takes around half an hour to perform and requires measurements from 36 different projections, the data for these projections are collected under varying coupling conditions due to the dynamic nature of the free space channel given by thermal fluctuations and changing weather conditions



throughout the day. This leads to fluctuating coincidence values for each projection across different tomography runs, as reflected in the concurrence data (see Figure 6), which shows slight variations in the concurrence for each tomography. This can be regarded as an error in characterizing the state accurately across the channel. Nevertheless, during the course of the experiment, we were able to obtain close approximations for the corrected MUB choices because the distributed state retained high entanglement. The present data, therefore, support the use of the MUB approach for slowly varying changes in the implemented link. The fixed-window baseline analysis, therefore, shows occasional QBER excursions above the information-theoretic security threshold.

All the data shown in Figure 4 represent QBER and key rate extracted from raw timestamps using a fixed 1 ns coincidence window. Under this baseline analysis, local fluctuations and accidental coincidences can occasionally drive the estimated QBER above the 11% threshold. We therefore apply the adaptive coincidence-window optimization described in Chatterjee and Sinha (2023) to the raw timestamps. This protocol-relevant analysis suppresses accidental coincidences and yields average daytime and nighttime QBER values of $8.05 \pm 1.48\%$ and $8.25 \pm 0.85\%$, with corresponding key rates of 6.39 ± 0.81 kHz and 6.98 ± 0.81 kHz for the Day 1 corrected-MUB dataset. Figure 7 displays the optimized key-rate and QBER values for various iterations of QKD, where measurements are conducted in the corrected MUB. These results are compared with the unoptimized fixed conventional-basis reference. The comparison is therefore intended to quantify the benefit of tomography-derived measurement-basis compensation under the implemented link transformation, not to claim that a separately optimized standard-BBM92 system requires tomography.

Throughout all the presented plots, the fixed conventional-basis reference is compared with the corrected-MUB protocol. Previous

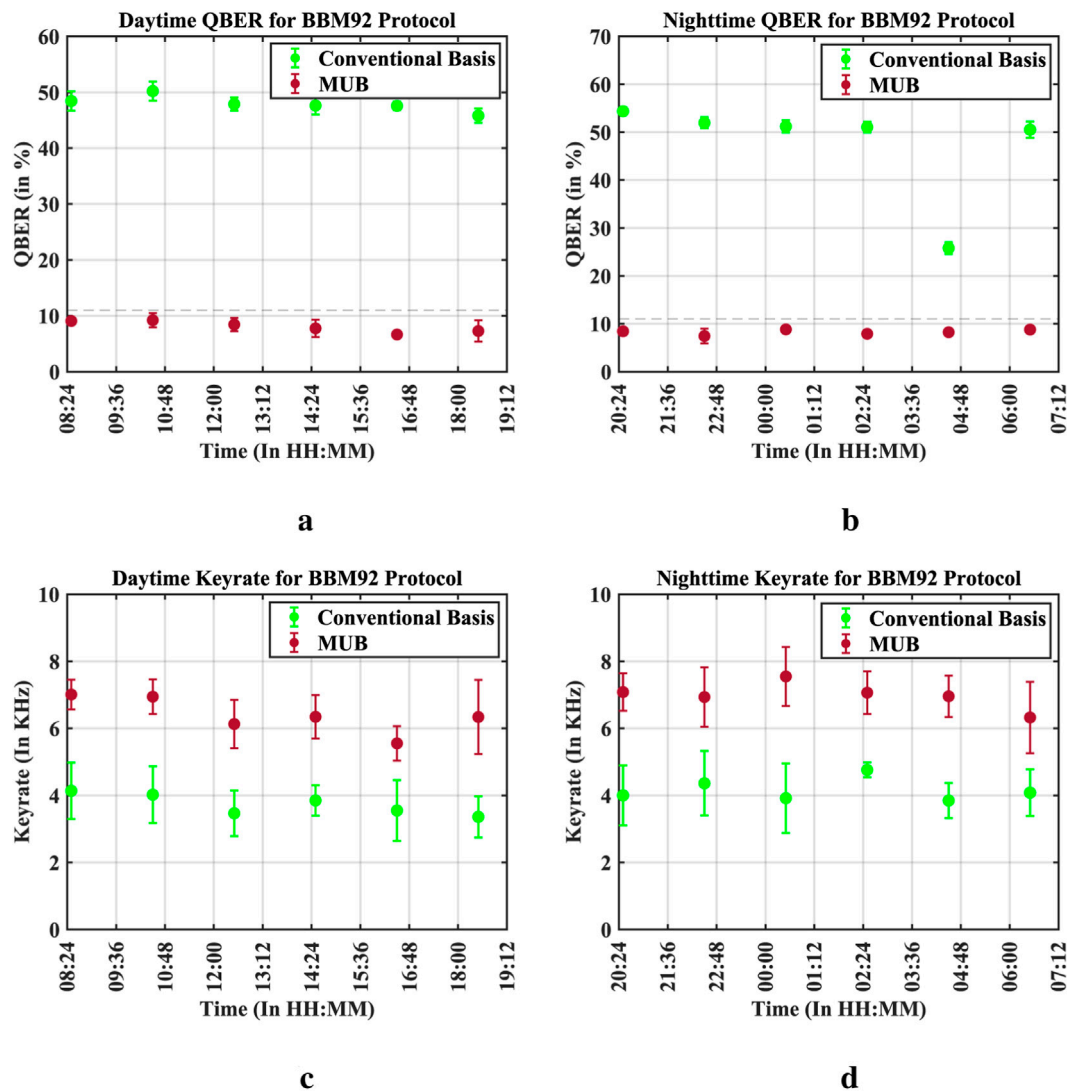


FIGURE 7 Optimized analysis of free-space QKD data for Day 1. Here, the coincidence window is adaptively varied to maximize the signal-to-noise ratio for the corrected-MUB protocol. (a,c) compare the optimized QBER and key rate for daytime operation using the corrected MUB with the unoptimized fixed conventional-basis reference. (b,d) show the corresponding comparison for nighttime operation. Average daylight key rate and QBER = $(6.39 \pm 0.81 \text{ kHz}, 8.05 \pm 1.48\%)$. Average nighttime key rate and QBER = $(6.98 \pm 0.81 \text{ kHz}, 8.25 \pm 0.85\%)$. (a) Daytime QBER. (b) Nighttime QBER. (c) Daytime keyrate. (d) Nighttime keyrate.

free-space BBM92 demonstrations have shown that well-aligned conventional-basis implementations can achieve low QBER over short-to-moderate free-space distances [Mishra et al. \(2022\)](#). Our conventional-basis reference is therefore not presented as a separately optimized standard-BBM92 benchmark. It is included to show how the fixed laboratory H/V and D/A bases perform under the net polarization transformation of the implemented source-fiber-free-space-receiver link. Under these same link conditions, selecting the corrected MUB as Bob's measurement basis restores stronger correlations and reduces QBER. The contribution of the present experiment is thus the deployment of the previously proposed MUB correction method over a stationary atmospheric link, together with day/night operation and secure-key post-processing.

4.1 Secure key generation and reconciliation performance

For secure key analysis, we consider a representative optimized run ([Figure 7](#)) yielding a sifted key rate of $R_{\text{raw}} = 6.54 \text{ kHz}$, with an average QBER of $\bar{E} = 8.3\%$.

We analyze a representative sifted key length of $N_s = 1.96 \times 10^6$ bits. Using the finite-size key rate expression introduced in Eq. ([Equation 8](#)), we evaluate the entropy at $E = 8.3\%$:

$$H_2(0.083) \approx 0.413.$$

In the ideal reconciliation limit ($f = 1$), the asymptotic secure fraction excluding the loss from the assumed security parameter ϵ becomes,

$$1 - 2H_2(E) \approx 1 - 2(0.413) = 0.174,$$

yielding an ideal secure key length of approximately

$$N_f^{\text{ideal}} \approx 3.41 \times 10^5 \text{ bits.}$$

However, practical reconciliation efficiency deviates from the Shannon limit. Using LDPC protocol based on belief propagation Gallager (1962); Varnica and Fossorier (2004); Lai and Kuo (2021), we observe.

- Average reconciliation efficiency: $f_{\text{avg}} = 1.31$,
- Best observed block efficiency: $f_{\text{best}} = 1.16$.

These efficiencies summarize the leakage overhead observed across the accepted LDPC-decoded blocks of the representative run. Substituting these into (Equation 8) gives:

$$N_f^{f=1.16} \approx 2.12 \times 10^5 \text{ bits,}$$

$$N_f^{f=1.31} \approx 9.16 \times 10^4 \text{ bits.}$$

These values represent finite-size estimates assuming a uniform reconciliation efficiency across the entire dataset. In contrast, the experimentally obtained secure key length is derived from block-wise adaptive LDPC reconciliation, where the effective global efficiency differs from the average efficiency due to variability in block-wise leakage. The finite-size correction term contributes only ~ 264 bits and is negligible compared to reconciliation leakage. Thus, the reconciliation efficiency constitutes the dominant limitation on the extractable secure key length.

In the implemented post-processing pipeline, the sifted key is divided into 327 blocks of 6000 bits each. Of these, 296 blocks are successfully reconciled using rate-adaptive LDPC decoding, corresponding to a 90.5% block-acceptance rate, while the remaining blocks are rejected.

After reconciliation and block rejection, the accepted blocks contain 1.77×10^6 bits prior to privacy amplification, corresponding to an experimentally realized post-reconciliation key rate of $R_{\text{ec}} = 5.92$ kHz.

Privacy amplification is then performed using a Toeplitz hash function, which is a two-universal hash family. Using Equation 8 with the measured QBER, the reported reconciliation leakage, and $\varepsilon = 2 \times 10^{-40}$, we obtain a final secure key of length 105,258 bits, corresponding to a secure key rate of 351 Hz. The obtained secure key length lies between the two finite-size estimates corresponding to $f = 1.16$ and $f = 1.31$, reflecting an effective reconciliation efficiency that is close to, but not exactly equal to, the average value $f_{\text{avg}} = 1.31$. The reduction from the 6.54 kHz sifted key rate to 351 Hz is dominated by reconciliation leakage and block rejection, whereas the finite-size correction contributes only about 264 bits. Across the representative dataset, the block-wise QBER values for the accepted blocks lie approximately in the 6.3%–9.45% range, with lower-rate LDPC codes selected for noisier blocks.

We note that the finite-size key length estimates via Equation 8 account for privacy amplification based on a Shannon-entropy approximation of the observed block-wise QBER, with a finite-size correction term determined by the security parameter $\varepsilon = 2 \times 10^{-40}$. The experimentally reported secure key rate of 351 Hz corresponds to the output after LDPC reconciliation and

privacy-amplification. The block size considered in the process is 6000, while adapted LDPC code rates are among $\frac{3}{5}$, $\frac{1}{2}$, $\frac{2}{3}$, $\frac{1}{3}$ and $\frac{3}{10}$.

5 Discussion

Using entanglement-based QKD over a free-space atmospheric link between two buildings within our institute campus, we have experimentally validated the effectiveness of our MUB-based passive polarization correction mechanism against the net polarization transformation arising from fiber birefringence, source and analyzer imperfections, and misalignment of reference frames between sender and receiver. The results demonstrate operation across three 24-h acquisition campaigns under varying daylight and weather conditions. While the fixed-window baseline analysis shows occasional local QBER excursions due to accidental coincidences and channel fluctuations, the adaptive coincidence-window optimization yields average QBER values around 8% and sifted key rates approaching 7 kHz for the representative Day 1 corrected-MUB dataset discussed in Section 4. Across the remaining datasets, the optimized corrected-MUB analysis also yields threshold-compatible average QBER values, as reported in the Supplementary Material.

The corresponding secure key rate, after reconciliation and privacy amplification, reaches 351 Hz under realistic reconciliation efficiencies. The finite-size security analysis indicates that reconciliation efficiency, rather than the loss due to security correction, presently limits the achievable secure key fraction. This highlights the importance of improved error correction design for further system enhancement.

The present study considers stationary source and receiver platforms and does not reproduce moving-platform or satellite dynamics. Practical long-distance quantum communication often involves relative motion between nodes. Previous demonstrations have explored QKD with moving terrestrial vehicles Kwiat et al. (2022), drones Carrasco-Casado et al. (2011), aircraft Nauwerth et al. (2013), hot air balloons Wang et al. (2013), and satellites Liao et al. (2017a). Extending our passive measurement-based correction mechanism to scenarios involving dynamic motion constitutes a natural and promising direction for future investigation, but such operation would require faster state estimation or a suitable calibration strategy matched to the reference-frame drift timescale.

A current limitation of our methodology is the requirement of performing quantum state tomography prior to initiating the corrected-MUB QKD protocol. State tomography consumes single-photon resources and requires multiple projection measurements, which can be time-consuming under dynamically varying channel conditions. The present work does not claim operation in a rapidly varying turbulence or moving-platform regime; rather, it demonstrates feasibility for a static, slowly varying link where the polarization transformation is stable on the calibration timescale. Although passive correction reduces the need for high-bandwidth active polarization tracking during key acquisition, photons are inherently sacrificed during characterization. Future work should therefore include a systematic resource-budget analysis comparing passive and active correction strategies under realistic operational constraints,

including QBER degradation as a function of elapsed time since tomography. Another promising direction involves developing faster state estimation techniques—for instance, compressed sensing approaches Gross et al. (2010) could reduce the number of required projections from 36 to roughly 10–15 — as well as adaptive post-processing algorithms capable of dynamically optimizing the signal-to-noise ratio in real time and machine learning-based channel prediction that could allow the MUB to be updated adaptively between full tomography runs. Improvements in LDPC code design and reconciliation efficiency are also expected to significantly enhance the final secure key rate, as reconciliation loss currently constitutes the dominant limitation. Our current demonstration of robustness to slowly varying channel conditions provides a baseline for evaluating such approaches. Overall, the results presented here demonstrate that passive MUB-based correction enables daylight-compatible, entanglement-based free-space QKD over a stationary atmospheric link with finite-size security analysis. The demonstrated stability across environmental conditions supports further development of measurement-based correction strategies for deployable quantum communication networks.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Author contributions

SRB: Data curation, Formal Analysis, Investigation, Methodology, Validation, Visualization, Writing – original draft. MG: Data curation, Formal Analysis, Methodology, Writing – original draft. US: Conceptualization, Funding acquisition, Investigation, Methodology, Project administration, Supervision, Visualization, Writing – original draft, Writing – review and editing.

Funding

The author(s) declared that financial support was received for this work and/or its publication. This work was supported by the Indian Space Research Organization (ISRO) under the QuEST-ISRO research grant. Partial support was also provided by the National Quantum Mission (NQM) of the Department of Science and Technology (DST), Government of India.

References

- Abasifard, M., Cholsuk, C., Pousa, R. G., Kumar, A., Zand, A., Riel, T., et al. (2023). *The Ideal Wavelength for Daylight free-space Quantum Key Distribution*. arXiv preprint arXiv:2303.02106.
- Avesani, M., Calderaro, L., Schiavon, M., Stanco, A., Agnesi, C., Santamato, A., et al. (2021). Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. *npj Quantum Inf.* 7, 93. doi: 10.1038/s41534-021-00421-2
- Basset, F. B., Valeri, M., Neuwirth, J., Polino, E., Rota, M. B., Poderini, D., et al. (2023). Daylight entanglement-based quantum key distribution with a quantum dot source. *Quantum Sci. Technol.* 8, 025002. doi: 10.1088/2058-9565/acae3d

Acknowledgments

US would like to thank the Indian Space Research Organization for support through the QuEST-ISRO research grant. US and SRB thank the National Quantum Mission of the DST for partial support. We thank S. Chatterjee, K. Goswami, S. Prabhakaran and S. Sujatha for their initial technical assistance and Wenyuan Wang for useful discussions. US would like to thank the Perimeter Institute, Canada, and MIT, USA, for their kind hospitality during the QPV 2023 workshop and the Optics and Quantum Electronics seminar, respectively; discussions during these events led to significant enrichment of the manuscript.

Conflict of interest

The author(s) declared that this work was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declared that generative AI was not used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Supplementary material

The Supplementary Material for this article can be found online at: <https://www.frontiersin.org/articles/10.3389/frqst.2026.1865541/full#supplementary-material>

- Bennett, C. H., Brassard, G., and Robert, J.-M. (1988). Privacy amplification by public discussion. *SIAM J. Comput.* 17, 210–229. doi: 10.1137/0217014
- Bennett, C. H., Brassard, G., and Mermin, N. D. (1992). Quantum cryptography without bell's theorem. *Phys. Rev. Lett.* 68, 557–559. doi: 10.1103/PhysRevLett.68.557
- Buttler, W. T., Hughes, R. J., Kwiat, P. G., Lamoreaux, S. K., Luther, G. G., Morgan, G. L., et al. (1998). "Free-space quantum key distribution at night," in *Photonic Quantum Computing II* (SPIE: International Society for Optics and Photonics), 3385, 14–22. doi: 10.1117/12.312638
- Buttler, W. T., Hughes, R. J., Lamoreaux, S. K., Morgan, G. L., Nordholt, J. E., and Peterson, C. G. (2000). Daylight quantum key distribution over 1.6 km. *Phys. Rev. Lett.* 84, 5652–5655. doi: 10.1103/PhysRevLett.84.5652
- Cai, W.-Q., Li, Y., Li, B., Ren, J.-G., Liao, S.-K., Cao, Y., et al. (2024). Free-space quantum key distribution during daylight and at night. *Optica* 11, 647–652. doi: 10.1364/OPTICA.511000
- Carrasco-Casado, A., Vergaz, R., Sánchez-Pena, J. M., Otón, E., Geday, M. A., and Otón, J. M. (2011). "Low-impact air-to-ground free-space optical communication system design and first results," in *2011 - ICSOS (IEEE)*, 109–112.
- Chatterjee, S., and Sinha, U. (2023). Methods and a system for optimizing performance of a quantum key distribution (QKD) protocol. *Indian Pat. Appl.*, 202341035230.
- Chatterjee, R., Joarder, K., Chatterjee, S., Sanders, B. C., and Sinha, U. (2020). qkdsim, a simulation toolkit for quantum key distribution including imperfections: performance analysis and demonstration of the b92 protocol using heralded photons. *Phys. Rev. Appl.* 14, 024036. doi: 10.1103/PhysRevApplied.14.024036
- Chatterjee, S., Goswami, K., Chatterjee, R., and Sinha, U. (2023). Polarization bases compensation towards advantages in satellite-based qkd without active feedback. *Commun. Phys.* 6, 116. doi: 10.1038/s42005-023-01235-8
- Coecke, B. (2010). Quantum pictorialism. *Contemp. Phys.* 51, 59–83. doi: 10.1080/00107510903257624
- Ecker, S., Liu, B., Handsteiner, J., Fink, M., Rauch, D., Steinlechner, F., et al. (2021). Strategies for achieving high key rates in satellite-based qkd. *npj Quantum Inf.* 7, 5. doi: 10.1038/s41534-020-00335-5
- Gallager, R. (1962). Low-density parity-check codes. *IRE Trans. Inf. Theory* 8, 21–28. doi: 10.1109/TIT.1962.1057683
- Gross, D., Liu, Y.-K., Flammia, S. T., Becker, S., and Eisert, J. (2010). Quantum state tomography via compressed sensing. *Phys. Rev. Lett.* 105, 150401. doi: 10.1103/PhysRevLett.105.150401
- Hecht, E. (2017). *Optics*. Incorporated: Pearson Education.
- Hughes, R. J., Nordholt, J. E., Derkacs, D., and Peterson, C. G. (2002). Practical free-space quantum key distribution over 10 km in daylight and at night. *New J. Physics* 4, 43. doi: 10.1088/1367-2630/4/1/343
- Kwiat, P., Chitambar, E., Conrad, A., and Isaac, S. (2022). *Autonomous Vehicle-based Quantum Communication Network*. I-ACT-21-02.
- Lai, C.-Y., and Kuo, K.-Y. (2021). Log-domain decoding of quantum ldpc codes over binary finite fields. *IEEE Trans. Quantum Eng.* 2, 1–15. doi: 10.1109/TQE.2021.3113936
- Lee, Y. S., Mohammadi, K., Babcock, L., Higgins, B. L., Podmore, H., and Jennewein, T. (2022). Robotized polarization characterization platform for free-space quantum communication optics. *Rev. Sci. Instrum.* 93, 033101. doi: 10.1063/5.0070176
- Li, D.-D., Gao, S., Li, G.-C., Xue, L., Wang, L.-W., Lu, C.-B., et al. (2018). Field implementation of long-distance quantum key distribution over aerial fiber with fast polarization feedback. *Opt. Express* 26, 22793–22800. doi: 10.1364/OE.26.022793
- Liao, S.-K., Cai, W.-Q., Liu, W.-Y., Zhang, L., Li, Y., Ren, J.-G., et al. (2017a). Satellite-to-ground quantum key distribution. *Nature* 549, 43–47. doi: 10.1038/nature23655
- Liao, S.-K., Yong, H.-L., Liu, C., Shentu, G.-L., Li, D.-D., Lin, J., et al. (2017b). Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nat. Photonics* 11, 509–513. doi: 10.1038/nphoton.2017.116
- Ma, X., Fung, C.-H. F., and Lo, H.-K. (2007). Quantum key distribution with entangled photon sources. *Phys. Rev. A* 76, 012307. doi: 10.1103/PhysRevA.76.012307
- Mishra, S., Biswas, A., Patil, S., Chandravanshi, P., Mongia, V., Sharma, T., et al. (2022). BBM92 quantum key distribution over a free space dusty channel of 200 meters. *J. Opt.* 24, 074002. doi: 10.1088/2040-8986/ac6f0b
- Nauerth, S., Moll, F., Rau, M., Fuchs, C., Horwath, J., Frick, S., et al. (2013). Air-to-ground quantum communication. *Nat. Photonics* 7, 382–386. doi: 10.1038/nphoton.2013.46
- Peloso, M. P., Gerhardt, I., Ho, C., Lamas-Linares, A., and Kurtsiefer, C. (2009). Daylight operation of a free space, entanglement-based quantum key distribution system. *New J. Phys.* 11, 045007. doi: 10.1088/1367-2630/11/4/045007
- Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* 21, 120–126. doi: 10.1145/359340.359342
- Tomamichel, M., Schaffner, C., Smith, A., and Renner, R. (2011). Leftover hashing against quantum side information. *IEEE Trans. Inf. Theory* 57, 5524–5535. doi: 10.1109/TIT.2011.2158473
- Toyoshima, M., Takenaka, H., Shoji, Y., Takayama, Y., Takeoka, M., Fujiwara, M., et al. (2011). Polarization-basis tracking scheme in satellite quantum key distribution. *Int. J. Opt.* 2011, 254154–254158. doi: 10.1155/2011/254154
- Varnica, N., and Fossorier, M. (2004). "Belief-propagation with information correction: improved near maximum-likelihood decoding of low-density parity-check codes," in *International Symposium on Information Theory, 2004. ISIT 2004* (Chicago, IL: IEEE), 343. doi: 10.1109/ISIT.2004.1365380
- Wang, J.-Y., Yang, B., Liao, S.-K., Zhang, L., Shen, Q., Hu, X.-F., et al. (2013). Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nat. Photonics* 7, 387–393. doi: 10.1038/nphoton.2013.89
- Xavier, G. B., Walenta, N., de Faria, G. V., Temporão, G. P., Gisin, N., Zbinden, H., et al. (2009). Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation. *New J. Phys.* 11, 045015. doi: 10.1088/1367-2630/11/4/045015
- Yin, J., Cao, Y., Li, Y.-H., Ren, J.-G., Liao, S.-K., Zhang, L., et al. (2017). Satellite-to-ground entanglement-based quantum key distribution. *Phys. Rev. Lett.* 119, 200501. doi: 10.1103/PhysRevLett.119.200501
- Yin, J., Li, Y.-H., Liao, S.-K., Yang, M., Cao, Y., Zhang, L., et al. (2020). Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature* 582, 501–505. doi: 10.1038/s41586-020-2401-y