Research Article Vol. 4, No. 2 / 25 April 2026 / Optica Quantum 89

OPTICA QUANTUM

High-speed phase-encoded quantum key distribution over a 1.4-km free-space channel

Li Zhang,[1,2] Fang-Xiang Wang,[1,3,4,*] Hai-Yang Fu,[1,3,4,5] Xin-Cai Tang,[2] Guo-Wei Zhang,[1,3,4] Hong-Yan Song,[2] Yong-Jun Qian,[2] Da-Wei Li,[2] Da-Chuang Li,[1] Dong Pan,[6,8] Guang-Can Guo,[1,3,4,5] Zheng-Fu Han,[1,3,4,5,9] and Gui-Lu Long[7]

[1]Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China
[2]Anhui Asky Quantum Technology Co., Ltd., Wuhu, 241000, China
[3]Anhui Province Key Laboratory of Quantum Network, University of Science and Technology of China, Hefei 230026, China
[4]CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China
[5]Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China
[6]Beijing Academy of Quantum Information Sciences, Beijing 100193, China
[7]State Key Laboratory of Low-Dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, China
[8]pandong@baqis.ac.cn
[9]zfhan@ustc.edu.cn
*fxwung@ustc.edu.cn

Received 22 August 2025; revised 26 January 2026; accepted 5 February 2026; published 3 March 2026

Quantum Key Distribution (QKD) represents a groundbreaking cryptographic technology that enables theoretically unconditionally secure key generation between communication parties. With recent advancements in network integration, QKD systems have been successfully deployed across diverse complex scenarios. For last-mile access network applications, free-space optical channels emerge as an optimal transmission medium. In this work, we implement a free-space QKD system employing a high-repetition-rate phase-encoding BB84 protocol. The experimental setup incorporates a simplified, highly integrable synchronization apparatus and self-compensating phase drift correction mechanism, which enhances both system stability and secure key generation rate. Experimental results demonstrate robust performance over a 1.4-km free-space channel with approximately 13 dB attenuation, achieving a secure key rate (SKR) of 160.19 kbps while maintaining a quantum bit error rate (QBER) of 2.3%. These findings establish the feasibility and efficiency of phase-encoded free-space QKD for last-mile access network applications.

https://doi.org/10.1364/OPTICAQ.577031

1. INTRODUCTION

Quantum Key Distribution (QKD) technology was first proposed in the 1980s [1]. Based on fundamental physical principles [2,3], it has been theoretically proven to provide unconditionally secure key generation. Over four decades of development, QKD has evolved from laboratory prototypes to engineered implementations [4–9]. Practical QKD systems are categorized into fiber-optic and free-space channels according to their operational environments. Given the extensive existing fiber-optic infrastructure, fiber-based QKD solutions have witnessed rapid technological advancement and commercialization. Since the completion of the first quantum network in 2004 [10,11], pilot applications such as the Quantum Government Network [12], the Beijing-Shanghai Quantum Dedicated Line, and metropolitan quantum networks have been successively deployed [13]. In recent years, fiber-based point-to-point transmission distances have been extended to 1000 km [14,15] using the TF-QKD protocol [16]. Free-space channels differ significantly from fiber-optic channels due to their flexibility in configuration and heightened susceptibility to environmental factors. Free-space-based QKD has achieved remarkable progress in long-distance transmission beyond intercity scales. Ground-based free-space experiments have continuously refined methodologies and extended channel distances [17–19]. By 2016, the world's first satellite-to-ground quantum communication link was established, preliminarily forming an "integrated space-earth" quantum secure communication system [20]. Subsequent applications have enabled key distribution across 12,900 km [21]. Demonstrations and technological breakthroughs in QKD across both fiber-optic and free-space channels have propelled QKD networks into an integrated space-terrestrial development phase [22]. Within such integrated networks, short-range free-space links hold substantial application value for addressing critical "last mile" scenarios where fiber deployment proves impractical.

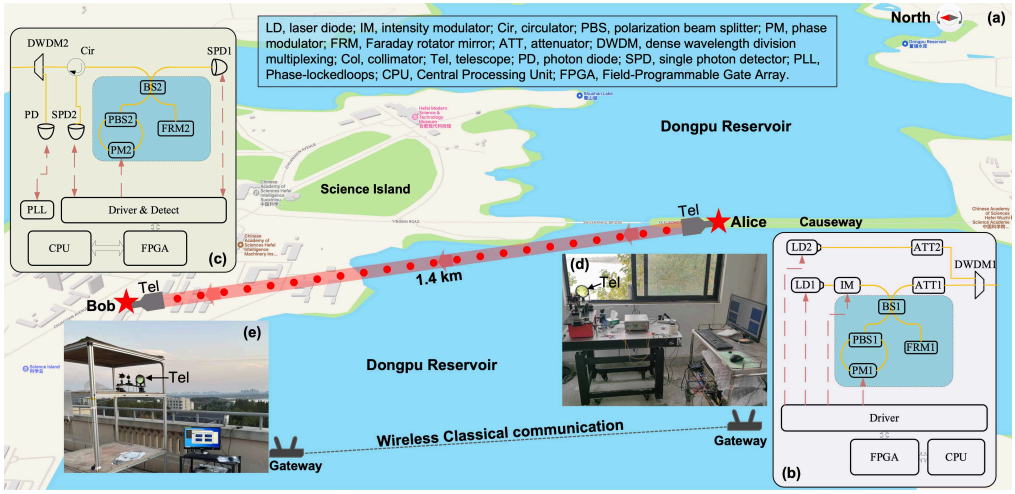

Fig. 1. Schematic diagram of the experimental setup. (a) The field-deployed experimental setup of the QKD system, where Alice and Bob are deployed on the causeway and Science Island, respectively. (b) The encoding setup of Alice. (c) The decoding setup of Bob. (d) and (e) The field deployment scenarios of Alice and Bob, respectively.

Research on QKD in short-range free-space channels mainly contains entanglement distribution, polarization encoding, time-bin encoding QKD scheme. In 2009, Kurtsiefer's group experimentally demonstrated daylight QKD using entanglement distribution over a 350-meter channel [23]. In subsequent experiments, entanglement distribution achieved key rates of 500 bps over a 1.3-km free-space channel [24], 1.7 kbps over 200 m [25], and 5.7 kbps over 1.7 km [26]. Polarization-encoded QKD was also extensively studied experimentally over short-distance free-space channels. Pan's group achieved a secure key rate (SKR) of 0.5 kbps over a 17 km [27], and they shifted the operating wavelength to 1550 nm over an 8 km urban free-space channel [28,29]. To enhance the operational efficiency of QKD systems, Han Zhengfu's group designed and experimentally demonstrated an RFI-BB84-QKD system using joint encoding with the polarization and orbital angular momentum states of photons [30]. Concurrently, researchers implemented BB84 polarization encoding on a silicon-based integrated chip. They achieved 701.22 kbps over a 275-m channel [31] and achieved 65 kbps over 145 m [32]. Polarization encoding has also been implemented in drone-to-ground scenarios, achieving an 8 kbps SKR over a 200-m distance [33]. QKD in hybrid fiber-optic and space channel applications, Picciariello's group realized a three-node urban network involving a 17-km fiber channel and a 620-m free-space channel [34]. Time-phase encoding has also been researched for short-distance free-space channels. Researchers implemented a reference-frame-independent (RFI) time-bin QKD system over a 2-km free-space channel [35], which validated the feasibility of time-bin QKD systems in free-space channels. In 2023, based on a time-phase encoding/decoding unit, researchers used the asymptotic key rate formula at a 1 GHz repetition rate under 15 dB, they calculated an SKR of 107 kbps [36]. From the aforementioned progress, it is evident that QKD is advancing toward an integrated space-ground network. Researchers are proposing QKD solutions and conducting field experiments for various application scenarios. While QKD based on fiber-optic channels has already been commercialized [37–39], there remains a critical need for mature, stable, and high-rate QKD solutions utilizing space channels in scenarios where fiber resources are unavailable for the "last mile" connectivity. Faraday-Michelson-Interferometer (FMI) type phase-encoded system is perfectly immune to polarization variations and thus become a most important implementation form of practical QKD systems [40–42]. However, phase-encoded free-space QKD remains to be validated. It obstructs the deployment of integrated space-to-fiber quantum network.

This work demonstrates QKD over a 1.4-km free-space channel using phase encoding BB84 protocol [1] in short-range scenarios. The proposed scheme employs phase-encoded QKD with a 1.25 GHz repetition rate and 1550 nm light source, enabling both daytime and nighttime operation. Furthermore, it integrates a simplified, low-cost yet stable synchronization mechanism along with a phase tracking and compensation system, achieving a key rate of 160.19 kbps in the 1.4-km free-space channel. This scheme enhances system security by employing a single quantum light source at the transmitter and implementing active basis selection at the receiver [43,44]. This implementation provides valuable insights for deploying and applying integrated space-ground QKD networks, particularly addressing access scenarios for the last mile.

2. EXPERIMENTAL SETUPS

The experimental system's transmitter and receiver terminals were deployed at two distinct locations: the Dongpu Reservoir Observatory Station on the Causeway and the rooftop of a six-story experimental building on Hefei Science Island, separated by a 1.4-km line-of-sight link over the reservoir surface. As illustrated in Fig. 1(a), the transmitter and receiver includes the phase-encoded QKD, the fiber-to-free-space telescope system, and a free-space-to-fiber telescope system. Classical communication between terminals was implemented through a wireless bridge connection. The QKD scheme employs a phase encoding scheme to implement quantum key distribution over fiber and free-space channels. As shown in Fig. 1(b), quantum light source (LD1) utilizes a distributed feedback (DFB) laser to generate pulsed light with a repetition rate of 1.25 GHz, a wavelength of 1549.32 nm, and a pulse full width at half maximum (FWHM) of 60 ps. The use of a single laser for the quantum light source effectively prevents the security vulnerabilities

arising from practical operational differences inherent in multi-laser systems [43]. The intensity modulator (IM) enables decoy-state modulation.

For the encoding end Alice, PM1 randomly modulates four phases $\{0, \pi, \pi/2, 3\pi/2\}$ to prepare two sets of mutually unbiased bases ($|Z\rangle = |s\rangle \pm |l\rangle$, and $|X\rangle = |s\rangle \pm i|l\rangle$), where $|s\rangle$ and $|l\rangle$ are the short and long arms, respectively. As shown in Fig. 1(b), a Faraday-Michelson Interferometer (FMI) is employed to achieve phase modulation and active basis selection at the receiver end [45], which can effectively defend passive basis-choice attacks [44]. In this system, the designed arm-length difference of the FMI is 400 ps. The pulse emitted from LD1, attenuated to the single-photon level after passing through the transmitter-side FMI unit, is wavelength-division multiplexed with the synchronization signal and transmitted through the channel.

As shown in Fig. 1(c), upon reaching the receiver Bob, the photon state enters port 1 of circulator (Cir1), exits from port 2, and is directed to the receiver-side FMI unit, where PM2 randomly modulates between phases 0 and $\pi/2$ to project the photon into Z and X bases, respectively. After undergoing interference, the two optical pulse paths pass through a 50:50 beam splitter (BS2). One path propagates directly to the single-photon detector (SPD1), while the other travels through an optical fiber to port 2 of circulator (Cir2), then exits from port 3 to SPD2. The interference outcome (I) is primarily determined by the phase difference ($\Delta\phi$) between Alice's and Bob's ends. Ignoring the SPDs' detection efficiency and dark counts, the correspondence between the phase encoding scheme and the detector results is summarized: when $\Delta\phi = 0$, the interference pulse has a 100% probability of being detected by SPD2 and a 0% probability of being detected by SPD1. When $\Delta\phi = \pi$, the interference pulse has a 0% probability of being detected by SPD2 and a 100% probability of being detected by SPD1. When $\Delta\phi = \pi/2$ or $3\pi/2$, the interference pulse has a 50% probability of being detected by SPD2 and a 50% probability of being detected by SPD1.

The clock synchronization method between the two ends of the QKD system is shown in Figs. 1(b) and 1(c). LD2 serves as the synchronization laser with a wavelength of 1550.52 nm. After being wavelength-division multiplexed with the quantum optical signal via a dense wavelength-division multiplexer (DWDM1), the synchronization signal is connected via a fiber jumper to collimator (COL1, TC18FC-1550, Thorlabs). It then transitions from fiber to free space through telescope (Tel1, transmission aperture of 120 mm, beam expansion ratio exceeding 20×) and is transmitted over the free-space channel. At the receiver end, the transmitted signal is collected via telescope (Tel2, reception aperture of 120 mm) and collimator (Col2), then fed into dense wavelength-division multiplexer (DWDM2). The synchronization signal is separated and directed to the high-power photodetector (PD), where it undergoes photoelectric conversion and is sent to the receiver's main control system to serve as the baseline clock synchronization for the receiving end.

The QKD main control module and post-processing unit are illustrated in Figs. 1(b) and 1(c). These components include a radio frequency (RF) amplification driver module, a timing processing FPGA (xcku060, Xilinx), and an x86-architecture CPU (Intel Core i5-7442 @ 2.1 GHz, 16 GB RAM). The RF amplification module amplifies high-speed small-signal amplitudes for driving optoelectronic devices, operating within a bandwidth range of 1 MHz to 10 GHz and delivering an amplitude range of 8 Vp-p. The FPGA handles high-speed digital signal modulation, signal triggering, and detector signal acquisition, achieving a maximum input/output rate of 16.3 Gbps via its GTX interface. Raw sampled data from the FPGA is transferred to the CPU through a PCIe 2.0 × 4 interface for post-processing. The CPU processes the raw data for basis reconciliation, error correction, and privacy amplification. The error correction employs low-density parity-check (LDPC) algorithm [46], achieving a tested correction rate of 26.2 Mbps, though the system utilizes a practical rate of approximately 600 kbps. Privacy amplification is implemented using a universal class of hash functions based on modular arithmetic [47], with an optimized multiplication algorithm for adaptive length adjustment and accelerated processing, achieving a maximum algorithmic rate of 14.8 Mbps.

3. KEY TECHNOLOGY

A. Synchronization

In this experiment, we use a wavelength of 1550.52 nm to transmit the synchronization signal (*A_Sync_clk*) with a frequency of 500 kHz and an output optical power of 300 nW. With a full width at half maximum of 60 ps and a luminous duty cycle of 6:200,000, the synchronization signal's optical pulse parameters are designed to minimize interference with the quantum signal, as shown in Fig. 2(a). A start signal with a pulse width of 5 ns is transmitted at fixed intervals Δt, serving as the initiation marker for QKD and triggering the quantum signal (*A_LD_Q*) to work at 1.25 GHz. The clock signal (*A_Sync_clk*), the start signal, and quantum signal (*A_LD_Q*) are jointly transmitted through the spatial channel to the receiver.

Upon reaching the receiver, wavelength demultiplexing separates the synchronization signal to enter an avalanche photodiode (APD). After photoelectric conversion, these signals are processed through signal discrimination and clock generation circuits. The start signal is identified to the arrival of quantum signals, while the 500 kHz clock signal from the transmitter is converted into a 250 kHz clock signal (*B_Sync_clk*) with a 1:1 duty cycle. The signal (*B_Sync_clk*) then enters the phase-locked loop (PLL) circuit at the receiver for phase recognition, locking, and frequency multiplication. The multiplied 125 MHz clock serves as the reference clock for the receiver-side FPGA, achieving clock synchronization between both ends. As shown in Fig. 2(b), the synchronized clock jitter in this scheme is approximately 60 ps.

We co-propagate the synchronization signal and the quantum signal over the same channel using wavelength-division multiplexing (WDM) technology and separate them in the time domain (achieved by adjusting the relative delay of the optical pulses). As a result, the noise measured at the quantum signal port due to the synchronization light is 100 counts per second (cps). In this experiment, the quantum signal count rate is approximately 2×10^6 cps. Therefore, the additional bit error rate introduced by synchronization is about 0.5 per ten thousand, which is negligible.

B. Phase Drift Compensation

The phase drift in our high-speed spatial phase-encoding system primarily arises from slow drift in fiber-optic interferometric loops and turbulence-induced disturbances in free space. Due to the 400-ps-length delay employed in this system, the phase drift

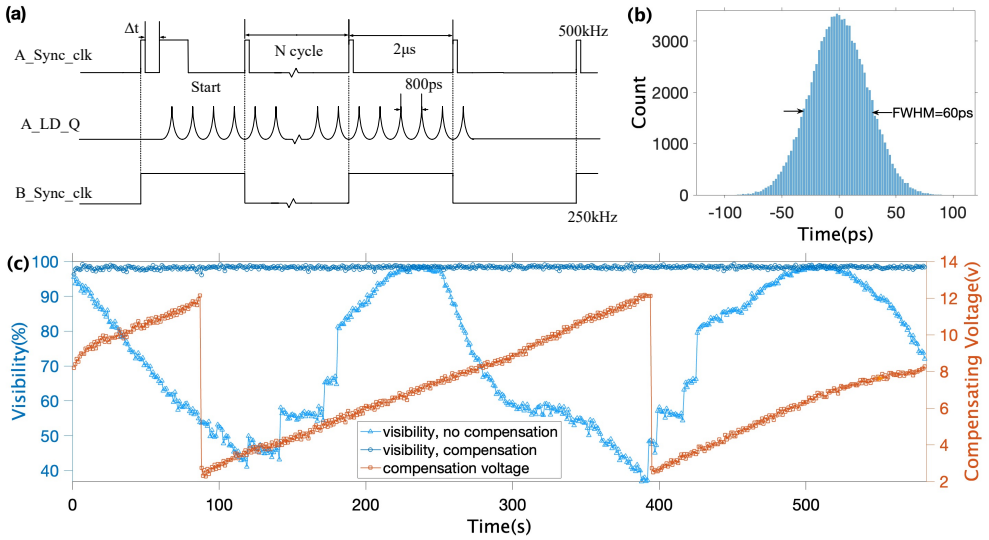

Fig. 2. Synchronization mechanism and phase tracking compensation. (a) Synchronization mechanism. (b) Synchronous clock jitter. (c) Phase compensation vs. no compensation comparison diagram.

induced by turbulence in the free space is significantly smaller than that caused by temperature variations between the long and short arms in the fibers at both the transmitter and receiver ends. To address this without introducing additional system overhead, we employ a self-calibration method.

This approach utilizes the raw key data (originally intended for public error rate estimation) to analyze and compensate for phase drift. Specifically, based on detection counts from single-photon detectors, a balanced matrix of counts is generated, reflecting the interference outcomes of the four phase differences between the two parties. Using the interference formula $I = \frac{1}{2}(1 + \cos\Delta\phi)$, the actual phase $\Delta\phi$ difference is derived. Comparing these results with the ideal phase differences $(0, \pi/2, \pi, 3\pi/2)$, the deviation is calculated to estimate the phase offset and corresponding voltage adjustment. The computed offset voltage is applied to the original phase voltages, dynamically tracking and compensating for drift. We utilized interference fringe visibility as a metric for the stability of phase interference, according to Eq. (1):

$$V = (C_{\max} - C_{\min})/(C_{\max} + C_{\min}). \quad (1)$$

V is interference fringe visibility, $C_{\max}$ is the cumulative count of constructive interference, and $C_{\min}$ is the cumulative count of destructive interference.

We recorded and compared the performance of the system over approximately 10 minutes under two conditions: without phase compensation and with active phase compensation applied. As shown in Fig. 2(c), the blue curve represents the interference fringe visibility. Without phase voltage compensation, the interference fringe visibility drifts from 35% to 99%. When phase voltage compensation is applied, as shown by the orange curve, with a compensation voltage range of 2 V to 12 V, the interference fringe visibility stabilizes at 99%.

Designed for QKD systems, this algorithm continuously monitors quadrature-phase voltage drift and executes dynamic compensation. It maintains stable and efficient system performance during voltage drift episodes by utilizing quantum bit error rate (QBER) estimation data for synchronization correction, achieving zero-overhead operation.

4. RESULTS AND DISCUSSION

The experiment adopts the decoy-state method [48,49], involving random switching between signal states, decoy states, and vacuum states. The transmission ratios for these three states are 29:2:1, with intensities of 0.6 photons/pulse for the signal state, 0.2 photons/pulse for the decoy state, and 0.0037 photons/pulse for the vacuum state. The presence of the vacuum state primarily arises from the limited extinction ratio of the intensity modulator, resulting in residual light. The experiment employs the asymptotic [50,51] and finite-length [52,53] key generation rate formulas:

$$R \geq qp_{\mu}\left\{-Q_{\mu}f(E_{\mu})H_2(E_{\mu}) + Q_1[1 - H_2(e_1)]\right\}, \quad (2)$$

$$l \leq s^{l}_{Z,0} + s^{l}_{Z,1}(1 - H_2(\phi^{u}_{Z})) - \lambda_{EC} - 6\log_2\left(\frac{19}{\epsilon_{sec}}\right) - \log_2\left(\frac{2}{\epsilon_{cor}}\right), \quad (3)$$

where q is the basis reconciliation factor (1/2 for balanced sifting BB84 protocol). p_{μ} is the probability of emitting signal states, Q_{μ} is the yield of the signal states with the average photon number of u, E_{μ} is the overall QBER, Q_1 and e_1 are, respectively, the yield and error rate of the single-photon states, and $f(x)$ is error correction efficiency. $H_2(x)$ is the binary Shannon entropy, given by $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$. $s^{l}_{Z,0}$ and $s^{l}_{Z,1}$ are the lower bound on the vacuum and single-photon events, respectively, ϕ^{u}_{Z} is the estimated upper bound on the phase error rate of Z basis, λ_{EC} is the key consumption during post-processing procedure, and $\epsilon_{sec} = 1 \times 10^{-9}$ and $\epsilon_{cor} = 1 \times 10^{-15}$ are the secrecy and correctness parameters.

The experimental data (collected on November 26, 2024) recorded the operation of the high-speed phase-encoded BB84 protocol over a 1.4-km free-space channel, as shown in Fig. 3. In order to verify the impact of different times of the day on the channel, the jitter of the channel loss during the day and at night was measured respectively. As shown in Figs. 3(a) and 3(b), the channel loss measured by this experimental system at night was approximately 2 dB. In contrast, the channel loss measured during daytime reached 10 dB. This significant increase

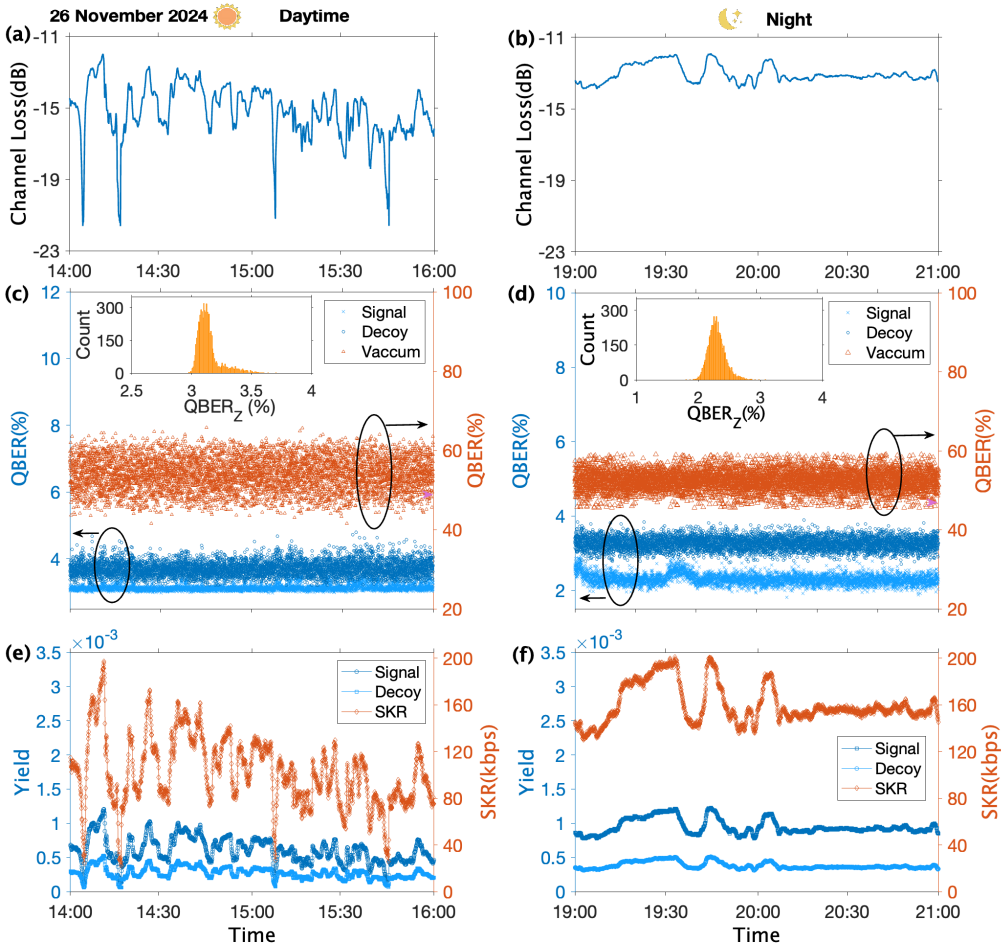

Fig. 3. The result of phase-encoded QKD system in a 1.4-km free-space channel. The three graphs on the left present results from the two-hour daytime test, the three graphs on the right display those from the two-hour nighttime test. (a) and (b) Channel loss and jitter. (c) and (d) QBERs of the signal, decoy, and vacuum states. The inset is a QBER frequency histogram for the signal states. (e) and (f) Test of yields and SKR.

was attributed to the combined effects of higher daytime temperatures causing water vapor evaporation from the lake surface, coupled with wind forces of 4–5 magnitude grades that generated substantial turbulent airflow, resulting in greater channel instability. The QKD parameters of this experimental system are listed in Table 1. The measured total attenuation of the 1.4 km spatial channel (including coupling losses at both ends) averaged 15 dB in day and 13 dB at night, with 4 dB attenuation observed at Bob's end. The single-photon detectors operated in Geiger mode with a working frequency of 1.25 GHz, featuring 20% detection efficiency, a dark count rate of 1×10^{-6} counts/gate, and an after-pulse probability below 1% per gate.

The quantum bit error rates (QBERs) of the signal state and two decoy states recorded over a 2-hour period are shown in Figs. 3(c) and 3(d). The corresponding gains of the signal, decoy, and vacuum states, along with real-time secure key generation rates, are shown in Figs. 3(e) and 3(f). The average yields of the signal during daytime and nighttime were 5.92×10^{-4} and 9.48×10^{-4}, respectively. The average yields of the decoy during daytime and nighttime were 2.67×10^{-4} and 3.8×10^{-4}, respectively. The average yields of the vacuum during daytime and nighttime were 5.63×10^{-6} and 4.81×10^{-6}, respectively. Under favorable nighttime channel conditions Fig. 3(f), the average QBER of the signal state was 2.3% with an average SKR of 160.19 kbps. During daytime channel degradation Fig. 3(e), the average QBER increased to 3.14% with a reduced SKR of 102.53 kbps. We further conducted a modeling and numerical study of turbulence effects using time-evolving phase screens [54] and split-step propagation [55], incorporating the receiver optics and the single-mode fiber coupling process. The results indicate that for the 1.4-km link under weak-to-moderate turbulence, beam wander is much smaller than the receiver aperture, geometric loss remains minor, and the excess QBER induced by background noise is negligible, consistent with our experimental observations. However, strong turbulence poses a major challenge for efficient fiber coupling, and adaptive optics represents a promising solution [56]. For longer distances, simulations suggest that our QKD system can be maintained up to 5 km in clear days, whereas operation at 10 km becomes increasingly limited by geometric loss, thereby requiring active tracking and a larger receiver aperture.

The post-processing of QKD data include error correction, SKR calculation (in this experiment, calculated using Eqs. (2) and (3), respectively), and privacy amplification. Table 1 presents detailed experimental results at several time points. The LDPC algorithm is used for error correction,

Table 1. Parameters for the QKD Experiment[a]

Parameter	Asymptotic				Finite-Length			
Time	14:30	15:30	20:00	21:00	14:30	15:30	20:00	21:00
N_{send} ($\times 10^9$)	6	6	6	6	125	125	125	125
n_Z	863661	603543	1307631	1189069	17992989	12573827	27242341	24772299
C_u	837279	584913	1272703	1157324	17443331	12185700	26514656	24110925
C_v	26090	18375	34631	31462	543554	382812	721484	655468
C_0	292	255	297	283	6104	5315	6201	5906
E_u	25913	17904	28737	25160	539871	373004	598700	524171
E_v	906	664	1111	1003	18893	13846	23138	20916
E_0	152	151	153	148	3184	3160	3194	3097
e_{obs}	0.031232	0.031018	0.022943	0.022129	0.031232	0.031018	0.022943	0.022129
$s^l_{Z,0}$	0	878	0	0	0	0	0	0
$s^l_{Z,1}$ ($\times 10^5$)	7.46	5.25	9.12	8.27	138	94.2	168	151
ϕ^u_Z	0.0271	0.0244	0.029	0.0283	0.0463	0.0474	0.0464	0.0463
f	1.221	1.119	1.221	1.22	1.221	1.119	1.221	1.22
S_{dc}	0.68229	0.68941	0.82458	0.84407	-	-	-	-
R ($\times 10^{-5}$ bit/pulse)	8.488	6.041	12.53	11.63	3.074	2.080	4.617	4.318
K (bits)	106094	75515	156632	145396	38429.532	25998.504	57715.076	53970.948

[a] N_{send} is the number of transmitted pulses, n_Z is the sifted key of Z base, C_u, C_v, and C_0 are the sifted counts of the signal, decoy, and vacuum states, respectively. E_u, E_v, and E_0 are the QBERs of the signal, decoy, and vacuum states, respectively. e_{obs} is the total observed error rate. f is the error correction efficiency. S_{dc} is the QKD system duty cycle. K is the SKR per second, while R is the SKR per pulse.

Table 2. Performance Comparison of QKD over Short-Range Free-Space Channels

Ref	Encoding Type	Wavelength (nm)	Operating Rate	Distance	SKR	Finite-Size Effect
[26]	Entanglement, BBM92	810	–	1.7 km	5.7 kbps	Finite
[33]	Polarization, Drone-based	850	50 MHz	200 m	8 kbps	Asymptotic
[27]	Polarization	671	100 MHz	17 km	0.5 kbps	Asymptotic
[28]	Polarization	1550	100 MHz	8 km	98–419 bps	Asymptotic
[30]	Polarization-OAM, RFI	1550	50 MHz	416 m	7 kbps	Asymptotic
[32]	Polarization, on-chip	1550	50 MHz	145 m	65.8 kbps/33 kbps	Asymptotic/finite
[34]	Polarization, fiber-space	1550	50 MHz	620 m	1.5 kbps	Finite
[35]	Time bin-phase, RFI	1550	20 MHz	2 km	–	–
This work	Phase	1550	1.25 GHz	1.4 km	160 kbps/104 kbps	Asymptotic/finite

processing accumulated sifted key in blocks of 1 Mbit. After calculation via the asymptotic rate formula or finite-length rate formula, the error-corrected data enters the privacy amplification process to generate a secure key. In this experiment, the sifted key peaked at approximately 400 kbps, and the processing speed of the privacy amplification algorithm meets the requirements for both asymptotic and finite-length rate scenarios. Under the asymptotic rate formula, the secure key generation rate can be generated in real time. When using the finite-key formula, we calculate the key rate once per transmission block of 1.25×10^{11} pulses from the transmitter. Considering the system duty cycle (factoring in time for parameter adjustments, data uploading, etc.), which is about 69% during daytime, calculations with the finite-key formula require waiting approximately 145 seconds per block.

The synchronization mechanism and wireless network employed in this system handle classical communication, thereby preventing continuous optical signals from entering the quantum channel. The wavelength-division multiplexing (WDM) component in the system provides inherent filtering capabilities, complemented by the gated single-photon detectors' effective gating window of 200 ps, which further suppresses noise outside the signal bandwidth. This configuration ensures the system exhibits strong immunity to external noise.

As shown in Table 2, we have listed representative works on short-distance spatial channels from the past decade, all of which provide detailed experimental parameters and post-processing methods with security proofs. As can be seen from the table, our experimental results demonstrate advantages in both the asymptotic regime and the finite-size regime. In our experiment, post-processing adopts the asymptotic rate, where sifted keys are accumulated for 3–4 seconds to generate secure keys. When considering the finite-size regime with a block length of 1.25×10^{11} pulses, the average SKR reached about 104 kbps at night and 49 kbps during daytime.

In practical applications of QKD, it is essential to address the identity authentication between Alice and Bob. Currently, we employ pre-shared secret keys for identity authentication. As the keys are consumed, a portion of the new keys generated by QKD is used to replenish and extend the pre-shared seed keys, enabling the renewal of authentication keys. In the future, digital signature-based authentication, particularly using Post-Quantum Cryptography (PQC) digital signature algorithms, can be adopted. QKD can leverage PQC digital signatures to authenticate the classical channel, thereby reducing or even eliminating the reliance on pre-shared keys in QKD. The integration of QKD and PQC can further enhance security in the field of information technology.

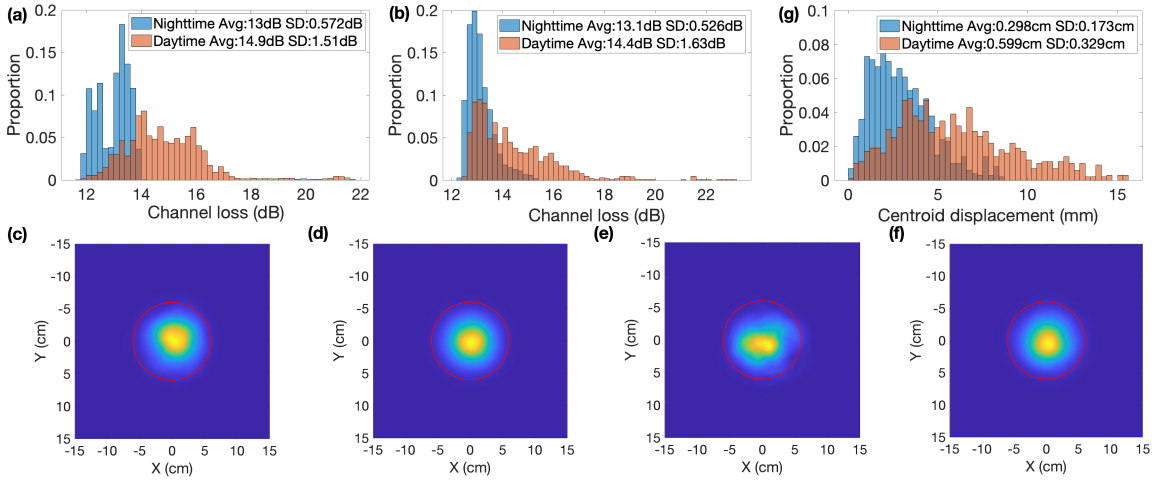

Fig. 4. Analysis of 1.4-km free-space channel. (a) The channel losses measured from the experiment. (b) The channel losses calculated from simulation. (The refractive index structure constant C_N^2 in simulation is 4×10^{-16} $m^{-2/3}$ at night and 1.5×10^{-15} $m^{-2/3}$ in the daytime.) (c) and (d) Transient and cumulative light intensity distribution at the receiver at night. (e) and (f) Transient and cumulative light intensity distribution at the receiver in the daytime. (The aperture of the receiving system is indicated by a red circle.) (g) The beam centroid displacement calculated from simulation.

5. CONCLUSION

Our work experimentally demonstrates, for the first time, the feasibility of applying phase-encoding BB84 protocol QKD systems in space channels. This experiment achieved a secure key generation rate of 160.19 kbps with an average QBER of 2.3% for phase-encoding QKD at a 1.25 GHz repetition rate over a 1.4 km free-space channel. Notably, daytime secure key generation was successfully realized at the same transmission distance. The system integrates a cost-effective synchronization mechanism to mitigate instability-induced parameter re-calibration in free-space channels, significantly enhancing operational efficiency. Real-time phase drift compensation ensures robust system stability, while the phase-encoding architecture—employing a single quantum light source at the transmitter and active basis selection at the receiver—strengthens security by minimizing potential attack surfaces. As a free-space optical communication system (FSO), the future QKD-FSO system requires integrated design of the internal modules of QKD itself, as well as optical integration with the acquisition, tracking, and pointing (ATP) system. This will thereby enable the realization of a compact and lightweight QKD-FSO system and is expected to extend operational stability. While phase-encoding BB84 protocol QKD has historically excelled in fiber-optic channels, this work validates its feasibility for high-speed free-space applications over short distances, offering a viable solution for bridging the "last mile" in ground-space integrated quantum networks.

APPENDIX A: ANALYSIS OF 1.4-km FREE-SPACE CHANNEL

We conducted a modeling and analytical study on the impact of atmospheric turbulence based on time-evolving turbulent phase screen [54] and split-step propagation [55]. Numerical simulations of the free-space channel were performed by incorporating the optical receiving system and fiber-coupling process. In the experiment, the optical transceiver system employed an aperture diameter of 120 mm, and the transmitted Gaussian beam had a waist radius of 80 mm. At the receiver, single-mode fiber coupling and DWDM filtering were applied to suppress background radiation.

The fluctuating channel losses measured during daytime and nighttime are shown in the Fig. 4(a). Based on time-evolving turbulent phase screens, we evaluated the intensity distribution of optical field at the receiver, the beam centroid displacement, and the total channel loss. Figure 4(b) shows that the simulation results are statistically consistent with the experimental data, thereby validating the effectiveness of our modeling and analysis. At a link distance of 1.4 km and a receiving aperture of 120 mm, the theoretical geometric loss when the beam is aligned is 0.1 dB. Under weak turbulence conditions at night, as Fig. 4(c) shows, the beam essentially remains in the fundamental Gaussian mode and is well aligned with the receiver aperture, which is favorable for subsequent fiber coupling. Figure 4(d) shows the intensity distribution accumulated over 1000 samples, the beam remains entirely within the receiver aperture, resulting in an average geometric loss of 0.14 dB. Under moderate turbulence conditions during daytime, Fig. 4(e) indicates that although most of the optical power is still collected by the receiver aperture, noticeable modal distortion and beam displacement emerge, which leads to increased fiber-coupling loss. The accumulated intensity distribution shown in Fig. 4(f) also remains within the aperture, with an average geometric loss of 0.20 dB. As shown in Fig. 4(g), the beam-wander extent is very small compared with the receiver aperture (with an average displacement of 3.0 mm at night and 6.0 mm during daytime), and thus does not introduce significant geometric loss. These results demonstrate that over a 1.4 km link under weak-to-moderate turbulence conditions, tracking system or adaptive optics is not strictly required, which is consistent with our experimental observations.

As for background noise, for the 1550 nm band, the background noise in a free-space channel mainly originates from atmospheric scattering of solar radiation [57] and, to a lesser extent, artificial light sources. Since both the solar emission and the atmospheric scattering spectrum are broadband and contin-

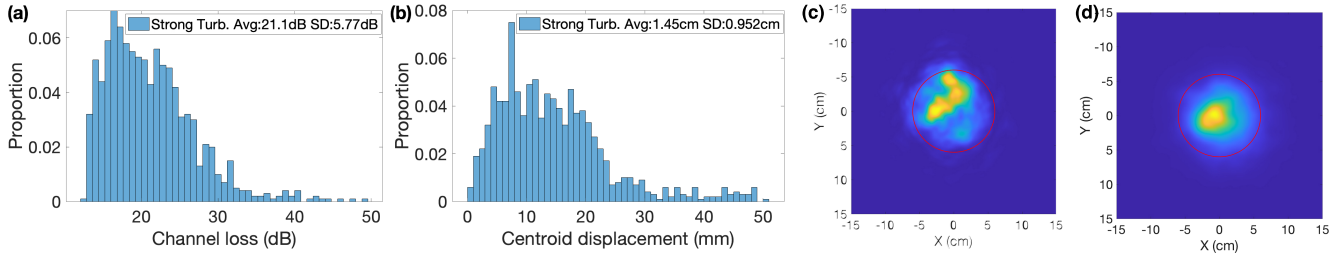

Fig. 5. Analysis of 1.4-km free-space channel under strong turbulence ($C_N^2 = 1 \times 10^{-14}$ m$^{-2/3}$). (a) The channel losses calculated from simulation. (b) The beam centroid displacement calculated from simulation. (c) and (d) Transient and cumulative light intensity distribution at the receiver. (The aperture of the receiving system is indicated by a red circle.)

Table 3. Achievable QKD Performance under Different Channel Loss

Channel loss (dB)	12	14	16	18	20	22	24	26
Asymptotic SKR (kbps)	197.3	126.0	82.64	54.51	35.37	21.82	11.93	4.506

uous, spectral filtering can effectively suppress the associated noise counts. In addition, the spectra of commonly used LED lighting are primarily concentrated in the visible range. Only legacy halogen and incandescent lamps exhibit broadband continuous spectra extending into the near-infrared; however, their contribution can likewise be mitigated by narrow-band spectral filtering. Our experiment was conducted near a reservoir, far from the downtown area, where artificial illumination was limited. Therefore, the background noise was dominated by the sky background. In our system, the single-photon detector (SPD) exhibits a dark count rate of 1250 cps. The additional counts induced by sky background were measured to be 200 cps at night and 500 cps during daytime. Meanwhile, the signal-state count rate reaches as high as 1 Mcps. Consequently, the excess QBERs introduced by background radiation are negligible in our system.

Thus, through modeling and analysis of the free-space channel, we discussed turbulence-induced beam wander, the optical receiving system and fluctuating channel loss, as well as the impact of background radiation. These results demonstrate that our system is capable of 24-hour operation over a last-mile link under weak-to-moderate turbulence conditions.

APPENDIX B: SYSTEM PERFORMANCE UNDER STRONGER TURBULENCE

Firstly, we calculated the achievable SKR of our QKD system under different channel losses in the asymptotic regime based on experimental results, as summarized in Table 3. Then, we investigated the impact of stronger turbulence over a 1.4-km link. For $C_N^2 = 1 \times 10^{-14} m^{-2/3}$, Fig. 5(a) shows the channel loss distribution obtained from numerical simulations. It can be seen that the channel loss is mainly within 30 dB, with an average value of 21 dB, under which our QKD system is still capable of secure key distribution, achieving an asymptotic SKR of 28 kbps. However, the loss exhibits considerable fluctuations, with the maximum exceeding 40 dB. This may lead to the loss of synchronization pulses, causing the QKD protocol to be interrupted until the synchronization clock is re-established. As shown in Fig. 5(b), although turbulence becomes stronger, the beam-centroid drift (15 mm on average) at 1.4 km distance link remains small compared with the receiver aperture. As the cumulative intensity distribution shown in Fig. 5(d), the beam is still mainly concentrated within the receiver aperture, resulting in an average geometric loss of 0.72 dB, these results indicate that the tracking system cannot significantly reduce the channel loss over short distances. In contrast, the intensity distribution in Fig. 5(c) suggests that the beam is no longer in the fundamental mode and exhibits multiple spots, which significantly increases the coupling loss. In this case, compensating high-order aberrations using an adaptive optics system can effectively reduce the coupling loss by 3–5 dB and improve the overall system performance [56].

APPENDIX C: SYSTEM PERFORMANCE AT LONGER DISTANCE

For longer link distances, turbulence-induced beam wander and beam broadening become pronounced, making alignment accuracy and the receiver aperture becomes limitation. Figure 6(a) shows the simulated channel-loss results for nighttime links over distances of 5 km and 10 km, with average losses of 16 dB and 21 dB, respectively. Since the turbulence is relatively weak at night, the loss fluctuations are not significant. Under these conditions, our system can still perform QKD, achieving asymptotic SKR of 84 kbps and 28 kbps. The distribution of beam-centroid displacement is shown in Fig. 6(b), where the mean displacement is comparable to the receiver aperture. Figures 6(c) and 6(d) show the intensity distributions at a distance of 5 km, indicating that the beam modal distortion remains limited and that most of the optical power is still collected within the 120-mm receiver aperture. In contrast, at a distance of 10 km, the intensity distributions in Figs. 6(e) and 6(f) reveal substantial beam broadening and beam wander. Moreover, the energy distribution becomes asymmetric, suggesting that a larger receiver aperture and tracking system is required to mitigate the geometric loss. Figure 7(a) presents the simulated link-loss results under moderate turbulence in the daytime. The average losses are 22 dB and 31 dB, respectively, with pronounced fluctuations. This indicates that even under clear daytime conditions, our system cannot operate over longer distances unless a tracking system and a larger receiver aperture are introduced. As shown in Fig. 7(b), beam wander becomes more severe during the daytime, reaching up to 25 cm at a distance of 10 km,

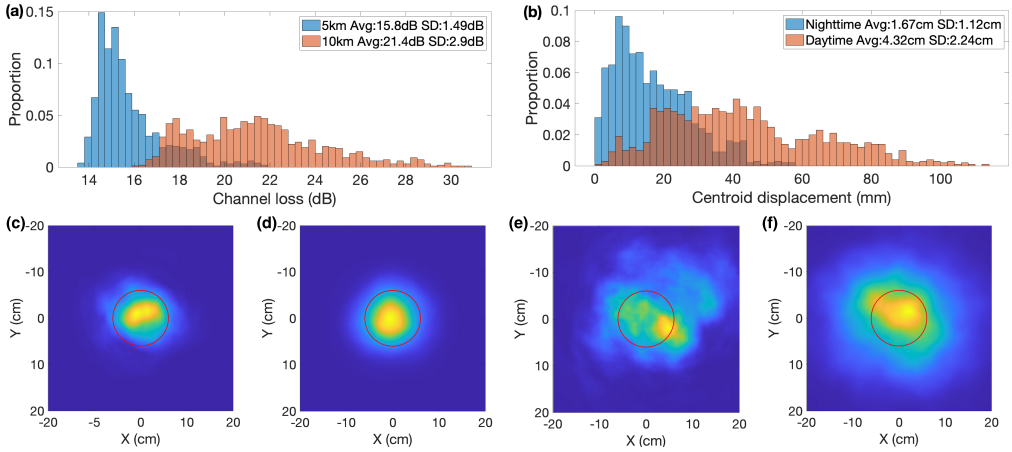

Fig. 6. Analysis of 5-km and 10-km free space channels at night ($C_N^2 = 4 \times 10^{-16}$ m$^{-2/3}$). (a) The channel losses calculated from simulation. (b) The beam centroid displacement calculated from simulation. (c) and (d) Transient and cumulative light intensity distribution at 5-km-away receiver. (e) and (f) Transient and cumulative light intensity distribution at 10-km-away receiver. (The aperture of the receiving system is indicated by a red circle.)

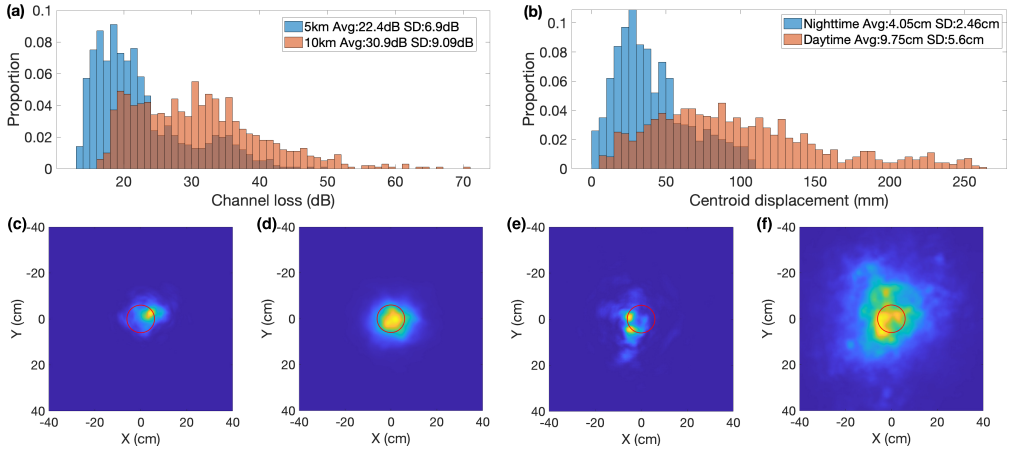

Fig. 7. Analysis of 5-km and 10-km free space channels in the daytime ($C_N^2 = 1.5 \times 10^{-15}$ m$^{-2/3}$). (a) The channel losses calculated from simulation. (b) The beam centroid displacement calculated from simulation. (c) and (d) Transient and cumulative light intensity distribution at 5 km-away receiver. (e) and (f) Transient and cumulative light intensity distribution at a 10-km-away receiver. (The aperture of the receiving system is indicated by a red circle.)

which is far beyond our receiver aperture. The intensity distributions in Figs. 7(c) and 7(d) show that, at a distance of 5 km, beam wander is no longer negligible; however, the optical energy is still mainly concentrated around the geometric center, thereby limiting the fiber-coupling loss. Meanwhile, the cumulative intensity distribution already extends beyond the receiver aperture, leading to increased geometric loss. At a distance of 10 km, the intensity distributions in Figs. 7(e) and 7(f) indicate that the Gaussian mode is substantially distorted, and the energy is no longer concentrated, resulting in a significant increase in coupling loss. Moreover, the cumulative intensity distribution spreads over an area of up to 40 cm × 40 cm, implying that geometric loss constitutes the dominant contribution to the overall channel loss.

Hence, our system is capable of performing QKD throughout the day for link distances up to 5 km, whereas operation over longer distances requires the introduction of a tracking system and a larger receiver aperture. For links within 5 km, the system performance is not primarily limited by turbulence-induced beam wander or beam broadening, but rather by the increased coupling loss resulting from beam modal distortion under moderate-to-strong turbulence. Adaptive optics therefore represents a promising solution to mitigate this effect and extend the applicability of free-space QKD systems to more challenging environments.

Funding. National Natural Science Foundation of China (62371437, 11974205, 12205011), Quantum Science and Technology-National Science and Technology Major Project (2021ZD0300701), Young Elite Scientists Sponsorship Program by CAST (2024-2026QNRC001).

Acknowledgement. The authors have been supported by National Natural Science Foundation of China (Grant No. 62371437) and Quantum Science and Technology-National Science and Technology Major Project (Grant No. 2021ZD0300701). Dong Pan and Gui-Lu Long have been supported by the Young Elite Scientists Sponsorship Program by CAST (2024-2026QNRC001) and the National Natural Science Foundation of China (Grant Nos. 11974205 and 12205011).

Disclosures. The authors declare no conflicts of interest.

Data availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

REFERENCES

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," Theor. Comput. Sci. **560**, 7–11 (1984).
2. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature **299**, 802–803 (1982).
3. G. D'Ariano, "Impossibility measuring the wave function of single quantum system," Phys. Rev. Lett. **76**, 28–32 (1996).
4. M. Alan, T. Xiao, M. LiJun, *et al.*, "High-speed quantum key distribution system supports one-time pad encryption of real-time video," Proc. SPIE **6224**, 62440M (2006).
5. M. Lijun, M. Alan, and T. Xiao, "High speed quantum key distribution over optical fiber network system," Proc. SPIE **7092**, 70920I (2009).
6. M. Sasaki, M. Fujiwara, H. Ishizuka, *et al.*, "Field test of quantum key distribution in the Tokyo QKD network," Opt. Express **19**, 10387–10409 (2011).
7. P. Sibson, C. Erven, M. Godfrey, *et al.*, "Chip-based quantum key distribution," Nat. Commun. **8**, 13984 (2017).
8. T. Y. Chen, X. Jiang, S. B. Tang, *et al.*, "Implementation of a 46-node quantum metropolitan area network," Npj Quantum Inf. **7**, 134 (2021).
9. A. Atutxa, A. Sanz, J. Sasiain, *et al.*, "Towards a quantum-safe 5g: quantum key distribution in core networks," Comput. Commun. **224**, 145–158 (2024).
10. C. Elliott, "Building the quantum network*," New J. Phys. **4**, 46 (2002).
11. C. Elliott, A. Colvin, D. Pearson, *et al.*, "Current status of the DARPA quantum network (invited paper)," Proc. SPIE **5815**, 138–149 (2005).
12. F. Xu, W. Chen, S. Wang, *et al.*, "Field experiment on a robust hierarchical metropolitan quantum cryptography network," Chin. Sci. Bull. **54**, 2991–2997 (2009).
13. Q. Zhang, F. Xu, L. Li, *et al.*, "Quantum information research in China," Quantum Sci. Technol. **4**, 040503 (2019).
14. W. Shuang, Y. Z. Qiang, H. D. Yong, *et al.*, "Twin-field quantum key distribution over 830-km fibre," Nat. Photon. **16**, 154–161 (2022).
15. Y. Liu, W.-J. Zhang, C. Jiang, *et al.*, "1002 km twin-field quantum key distribution with finite-key analysis," Quantum Front. **2**, 10716–10723 (2023).
16. M. Lucamarini, Z. L. Yuan, J. F. Dynes, *et al.*, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400–403 (2018).
17. R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, *et al.*, "Entanglement-based quantum communication over 144 km," Nat. Phys. **3**, 481–486 (2007).
18. S.-K. Liao, H.-L. Yong, C. Liu, *et al.*, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," Nat. Photon. **11**, 509–513 (2024).
19. W.-Q. Cai, Y. Li, B. Li, *et al.*, "Free-space quantum key distribution during daylight and at night," Optica **11**, 647–652 (2024).
20. BBC. "China launches world's first quantum satellite, Micius," https://www.bbc.com/news/world-asia-china-37091833 (2016).
21. Y. Li, W. Q. Cai, J. G. Ren, *et al.*, "Microsatellite-based real-time quantum key distribution," Nature **640**, 47–54 (2025).
22. Y.-A. Chen, "Large-scale quantum network: from intra-city to inter-city to global," in *8th International Conference on Quantum Cryptography* (2018).
23. M. P. Peloso, I. Gerhardt, C. Ho, *et al.*, "Daylight operation of a free space, entanglement-based quantum key distribution system," New J. Phys. **11**, 045007 (2009).
24. C. Erven, B. Heim, E. Meyer-Scott, *et al.*, "Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere," New J. Phys. **14**, 123018 (2012).
25. S. Mishra, A. Biswas, S. Patil, *et al.*, "Bbm92 quantum key distribution over a free space dusty channel of 200 meters," J. Opt. **24**, 074002 (2022).
26. A. Kržič, S. Sharma, C. Spiess, *et al.*, "Towards metropolitan free-space quantum networks," Npj Quantum Inf. **9**, 95 (2023).
27. L. Wei-Yue, Z. Xian-Feng, W. Teng, *et al.*, "Experimental free-space quantum key distribution with efficient error correction," Opt. Express **25**, 10716–10723 (2017).
28. C. Ma, W. D. Sacher, Z. Tang, *et al.*, "Silicon photonic transmitter for polarization-encoded quantum key distribution," Optica **3**, 1274–1278 (2016).
29. J. E. Kennard, P. Sibson, S. Stanisic, *et al.*, "Integrated silicon photonics for high-speed quantum key distribution," in *2017 Conference on Lasers and Electro-Optics (CLEO)* (2017), pp. 1–2.
30. Y.-P. Li, W. Chen, F.-X. Wang, *et al.*, "Experimental realization of a reference-frame-independent decoy BB84 quantum key distribution based on Sagnac interferometer," Opt. Lett. **44**, 4523–4526 (2019).
31. H. Ko, J.-S. Choe, B.-S. Choi, *et al.*, "Daylight operation of a high-speed free-space quantum key distribution using silica-based integration chip and micro-optics-based module," in *2019 Optical Fiber Communications Conference and Exhibition (OFC)* (2019), pp. 1–3.
32. M. Avesani, L. Calderaro, M. Schiavon, *et al.*, "Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics," Npj Quantum Inf. **7**, 93 (2021).
33. X.-H. Tian, R. Yang, H.-Y. Liu, *et al.*, "Experimental demonstration of drone-based quantum key distribution," Phys. Rev. Lett. **133**, 200801 (2024).
34. F. Picciariello, I. Karakosta-Amarantidou, E. Rossi, *et al.*, "Intermodal quantum key distribution field trial with active switching between fiber and free-space channels," EPJ Quant. Technol. **12**, 6 (2025).
35. H. Chen, J. Wang, B. Tang, *et al.*, "Field demonstration of time-bin reference-frame-independent quantum key distribution via an intracity free-space link," Opt. Lett. **45**, 3022–3025 (2020).
36. A. T. Castillo, U. Zanforlin, G. S. Buller, *et al.*, "Experimental demonstration of a reconfigurable free-space receiver implementing polarization routing and filtering for daytime quantum key distribution," Opt. Express **31**, 40317–40327 (2023).
37. Anhui Asky Quantum Technology Co., Ltd., http://www.qasky.com (2009).
38. ID Quantique, http://www.idquantique.com (2001).
39. Cambridge Research Laboratory of Toshiba Research Europe Limited, https://www.global.toshiba/ww/products-solutions/security-ict/qkd/why.html (1991).
40. X.-T. Song, D. Wang, X.-M. Lu, *et al.*, "Phase-coding quantum-key-distribution system based on Sagnac–Mach-Zehnder interferometers," Phys. Rev. A **101**, 032319 (2020).
41. P. N. Kumar, C. Sumit, K. Sangeeta, *et al.*, "Phase encoded quantum key distribution up to 380 km in standard telecom grade fiber enabled by baseline error optimization," Sci. Rep. **13**, 15868 (2023).
42. Z. Yue, Y. Junyue, Z. Huiqing, *et al.*, "Experimental demonstration of a local active phase compensation method for a phase encoding quantum key distribution system," Appl. Opt. **61**, 7713–7718 (2022).
43. S. Nauerth, M. Fürst, T. Schmitt-Manderbach, *et al.*, "Information leakage via side channels in freespace BB84 quantum cryptography," New J. Phys. **11**, 065001 (2009).
44. H.-W. Li, S. Wang, J.-Z. Huang, *et al.*, "Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources," Phys. Rev. A **84**, 062308 (2011).
45. X.-F. Mo, B. Zhu, Z.-F. Han, *et al.*, "Faraday–Michelson system for quantum cryptography," Opt. Lett. **30**, 2632–2634 (2005).
46. M. Li, C.-M. Zhang, Z.-Q. Yin, *et al.*, "Simple rate-adaptive LDPC coding for quantum key distribution," arXiv (2015).
47. C.-M. Zhang, M. Li, J.-Z. Huang, *et al.*, "Fast implementation of length-adaptive privacy amplification in quantum key distribution," Chin. Phys. B **23**, 090310 (2014).

48. X.-B. Wang, "Decoy-state protocol for quantum cryptography with four different intensities of coherent light," Phys. Rev. A **72**, 012322 (2005).
49. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
50. D. Gottesman, H.-K. Lo, N. Lutkenhaus, *et al.*, "Security of quantum key distribution with imperfect devices," in *International Symposium on Information Theory (ISIT)* (2004), p. 136.
51. C.-H. F. Fung, X. Ma, and H. F. Chau, "Practical issues in quantum-key-distribution postprocessing," Phys. Rev. A **81**, 012318 (2010).
52. C. C. W. Lim, M. Curty, N. Walenta, *et al.*, "Concise security bounds for practical decoy-state quantum key distribution," Phys. Rev. A **89**, 022307 (2014).
53. D. Rusca, A. Boaron, F. Grünenfelder, *et al.*, "Finite-key analysis for the 1-decoy state QKD protocol," Appl. Phys. Lett. **112**, 171104 (2018).
54. H. Fu, F. Wang, W. Chen, *et al.*, "Atmospheric turbulence time-evolving modeling using spatio-temporal fractal nature," Chin. Opt. Lett. **23**, 020101 (2025).
55. R. Frehlich, "Simulation of laser propagation in a turbulent atmosphere," Appl. Opt. **39**, 393–397 (2000).
56. K.-X. Yang, M. Abulizi, Y-h Li, *et al.*, "Single-mode fiber coupling with a M-SPGD algorithm for long-range quantum communications," Opt. Express **28**, 36600–36610 (2020).
57. A. Scriminich, G. Foletto, F. Picciariello, *et al.*, "Optimal design and performance evaluation of free-space quantum key distribution systems," Quantum Sci. Technol. **7**, 045029 (2022).