

Feasibility of multi-gigahertz satellite-to-ground secure quantum communication

Oliver M. Crampton^{1,2,*}, Thomas Roger¹, Chithrabhanu Perumangatt¹, Ravinder Singh¹, Robert I. Woodward¹, Davide G. Marangon¹, Ross J. Donaldson², R. Mark Stevenson¹, and Andrew J. Shields¹

¹*Toshiba Europe Ltd., Cambridge, United Kingdom*

²*Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh, United Kingdom*



(Received 12 September 2025; accepted 9 May 2026; published 8 June 2026)

We investigate the feasibility of satellite-to-ground quantum key distribution (QKD) at multi-GHz clock rates, where secure key generation time is constrained, due to low-Earth orbit (LEO) satellite overpasses (≈ 300 s). Higher repetition rates offer a direct route to increased secure key rate (SKR), though system performance is fundamentally limited by detector timing jitter, optical coupling losses, and atmospheric turbulence, depending on receiver architecture. We combine finite-key modeling, detailed detector timing characterization, adaptive optics (AO) modeling, and real-time free-space QKD experiments at 1 GHz to evaluate practical receiver configurations based on multi-mode fiber-coupled avalanche photodiodes (MMF-APDs) and single-mode fiber-coupled superconducting nanowire single-photon detectors (SMF-SNSPDs), at projected rates > 1 GHz. The results indicate clear operating regimes across a range of atmospheric conditions: MMF-APDs maximize secure key rates below ~ 1 GHz, mainly due to their low coupling loss. However, low-jitter SMF-SNSPDs are required to obtain positive key rates at higher clock rates—with modeling and measured timing responses of our hardware indicating an estimated optimal operating point near ~ 7.2 GHz—though AO correction is required for effective single-mode coupling under turbulence. The experimental and projected results provide quantitative performance bounds and realistic design targets for future high-rate satellite QKD systems, while highlighting the technological requirements needed to achieve end-to-end operation beyond the GHz regime.

DOI: [10.1103/y12y-yk88](https://doi.org/10.1103/y12y-yk88)

I. INTRODUCTION

Global quantum communication networks are an essential technology for the future of secure data transfer, especially as quantum computing threatens the security of traditional cryptographic protocols [1]. Quantum key distribution (QKD) provides a means for generating symmetric encryption keys, which is provably secure against any future technology. The fiber-based implementation of QKD is a mature technology. However, the scalability of fiber-based QKD is constrained by linear attenuation in optical fibers, restricting secure transmission to a few hundred kilometers without trusted nodes or quantum repeaters [2]. A promising way to extend this range is to use satellites as trusted nodes, by implementing satellite-to-ground QKD links [3]. Many studies have been performed to test the requirements for such links [4–6].

Since the concept of satellite QKD was first introduced [7], many works have investigated ways to increase the total key generation rate under high loss [4,8,9]. This can be done by improving the transmission and receiving optics, reducing pointing and tracking losses, or using specialized receiver optics to maximize coupling, such as adaptive optics (AO)

[10]. Another way to achieve higher secure bit rates and thus enable higher quantum-secure communication bandwidths in point-to-point, prepare-and-measure QKD is to increase the clock rate. As the clock rates of QKD transmitters are pushed into the GHz regime, the timing accuracy of photon detection will quickly become a bottleneck. It is therefore relevant to understand the practical impact of higher clock rates on the performance of QKD systems. Considering the limited time for an overpass to generate keys with an optical ground station (OGS), we opt to focus on increasing the clock rate of systems beyond 1 GHz, which is typical of modern QKD systems.

Since the demonstrations performed by the Micius satellite [11–13], many small satellite QKD missions are being planned around the world. Most recently, Jinan-1 performed satellite-to-ground QKD with real-time postprocessing at a clock rate of 625 MHz [3]. In-laboratory setups have demonstrated 1 GHz clocked free-space QKD with real-time optical postprocessing [14]. In fiber, polarization-based QKD has been achieved at clock rates of 5 GHz [15]. On the transmitter side, recent works have pushed the rates of polarization modulation to up to 10 GHz [16], but the detection at these rates is still predominantly a bottleneck. Two main devices are often chosen for photon detection: single-photon avalanche diodes (APDs) [17], and increasingly, superconducting nanowire single-photon detectors (SNSPDs). As the clock rates of QKD systems move toward the GHz regime [18,19], the need for SNSPDs is increasing due to their high timing accuracy [20], low dark count rates, and higher detection efficiencies [21].

*Contact author: omc2000@hw.ac.uk

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

One important consideration in choosing a detector is how efficiently the light can be coupled onto its active area to maximize the total detection efficiency. Although SNSPDs have high photon detection efficiency, due to their relatively small active area ($<20\ \mu\text{m}$), the signal needs to be coupled to a single-mode fiber before sending it to the detector. On the other hand, most commercial APDs for single-photon detection have larger active area ($>150\ \mu\text{m}$) and the signal can be coupled to either a single-mode or multimode fiber at the receiver. Multimode collection is particularly helpful, when you need to detect photons after atmospheric propagation. An advantage of single-mode fiber coupling is spatial filtering, meaning that the background light seen by the field of view of the receiving telescope is significantly reduced, when compared to larger field of view multimode fibers [22,23].

To use SNSPDs for satellite-to-ground QKD, one must consider adaptive optics for coupling the signal onto a single-mode fiber [24–29]. Studies have looked at the ability to couple light into single-mode fibers after propagation through turbulence, using AO [24–29]; however, this still remains an active area of research for free-space optical channels. Recently, progress has been made in multimode coupled SNSPDs [30,31] and nanowire arrays [32]. However, these devices are still in their infancy and tend to have lower detection efficiencies and higher jitter, when compared to their single-mode counterparts [33].

SNSPD detection efficiency also depends on the polarization of incoming photons; this means that polarization control is required at the detectors. SNSPDs also require space for cryogenic cooling, while APDs are available in small form factors that can be mounted to the telescope, and have much lower cost.

This study compares the use of different receiver configurations, for performing real-time polarization-based QKD at GHz clock rates, comparing the advantages and disadvantages of each detector type with each fiber coupling method. We provide an analysis of the feasibility of performing satellite-to-ground polarization-based QKD at rates well beyond 1 GHz with these commercially available detectors. Section II provides an experimentally validated analysis of the feasibility of multi-GHz clock-rate satellite-based QKD, as well as system-level AO requirements. In Sec. III, we describe an experimental setup that allows us to emulate a free-space satellite link, and directly compare detector configurations. In Sec. IV, we give an outlook on the future of satellite-based quantum communication at high bandwidths. We consider a relatively large optical ground station (OGS) telescope diameter of 100 cm, and LEO orbit of 500 km altitude.

II. SATELLITE-TO-GROUND EFFICIENT DECOY-STATE BB84 MODEL

In this section, we present both simulation and experimental results for a satellite-to-ground quantum communication link modeled using weak coherent pulses within a decoy-state BB84 framework [34,35]. This is the simplest and most likely scenario for a satellite QKD link in a future global-scale quantum network. The analysis that we present here can be readily adapted to also evaluate entanglement-based (E91 [36]) or up-link protocols. This analysis is also useful for applications

TABLE I. Detector parameters: η_{coupling} , coupling efficiency, η_{rx} , receiver optics efficiency, η_{turb} , efficiency after AO correction, NA, numerical aperture of fiber, fiber core diameter, η_{det} , loss due to detection efficiency, DCR, dark-count rate per detector, BGCR, background counts per detector, τ , detector dead-time, $\delta\tau_{\text{jitter}}$, detector jitter (quoted), measured FWHM (using gain-switched laser), τ_{decay} , measured decay constant, Z QBER_{Baseline}, intrinsic Z QBER, and X QBER_{Baseline}, intrinsic X QBER (measured, including 1 GHz jitter contribution).

Parameter	APD (MMF)	SNSPD (SMF)
Coupling efficiency, η_{coupling}	−0.5 dB	−2.5 dB
Rx optics efficiency, η_{rx}	−1.1 dB	−1.1 dB
Residual AO efficiency, η_{turb}	−0.1 dB	−2.0 dB
Numerical aperture (NA)	0.22	0.1
Fiber core diameter	50 μm	5 μm
Detection efficiency, η_{det}	0.56	0.85
DCR	~25 cps	15 cps
BGCR (estimated)	~185 cps	~6 cps
Detector dead time, τ_{dead}	22 ns	10 ns
$\delta\tau_{\text{jitter}}$	250–350 ps	<15 ps
Measured FWHM	350 ps	40 ps
Measured tail constant, τ_{decay}	0.15 ns	0.02 ns
Z QBER _{Baseline}	1.8%	0.8%
X QBER _{Baseline}	2.8%	1.8%

that directly couple the quantum signal into single-mode fiber and then forward to a QKD receiver elsewhere, in an untrusted ground station configuration. We also experimentally verify our results by performing real-time polarization-based QKD across a 3 m free-space link.

A. System parameters

The choice of detectors and coupling method at the optical ground station significantly impacts system performance, affecting quantum bit error rate (QBER), receiver losses, system complexity, background counts, achievable clock rates, and ultimately finite-key rates. We make use of three detection configurations for our comparison, SMF-coupled silicon(Si)-APDs (SMF-APDs), MMF-coupled Si-APDs (MMF-APDs), and SMF-coupled SNSPDs (SMF-SNSPDs); the detector parameters are shown in Table I. For the majority of the investigation, however, the interesting comparisons are between MMF-APDs and SMF-SNSPDs, because the total loss due to coupling and detector efficiency for SMF-APDs is greater than in any other case.

B. Key rates

We first model the finite-key rates and QBER, for each detector setup, given the parameters in Table I. The finite-key rate is calculated for an input raw sifted key of size 16 Mbit. The results of this simulation are shown in Fig. 1. The total receiver efficiency when coupled to single-mode and multimode fiber is −5.6 and −1.6 dB, respectively. We take the receiver loss to be a combination of fiber coupling efficiency, η_{coupling} , and receiver optics loss, and for single-mode coupling we assume a residual loss after adaptive optics correction, η_{turb} of −2 dB, as in Ref. [14], based on realistic measurements

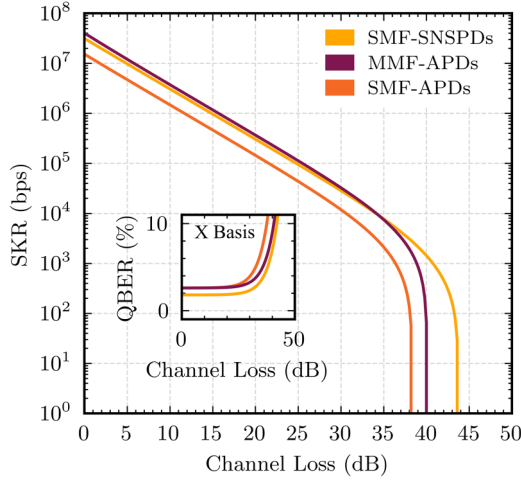


FIG. 1. Secure key rate analysis. Finite-key rates for three detectors and coupling configurations; SNSPDs, MMF-APDs, and SMF-APDs. The inset shows the X QBER for each detector setup.

of the Fried parameter, r_0 , in the East of England, detailed in Sec. II F. The detection efficiencies for the APDs and SNSPDs used are 56% and 85%, respectively.

For these simulations, the background counts for MMF-APDs (~ 185 cps) are typical of a suburban ground station as measured by the Jinan mission [3]. The background for SMF-SNSPDs is estimated based on measurements in the laboratory to be ~ 6 cps, which is approximately proportional to the ratio of fiber core areas. The other parameters used are experimentally obtained for our detectors. It is clear that SMF-APDs are outperformed by both MMF-APDs and SMF-SNSPDs. The secure key rate for MMF-APDs is marginally higher than for SNSPDs, until high loss (~ 40 dB), where SNSPDs can obtain higher positive secure key rates than MMF-APDs, due to lower QBER and background counts.

C. Jitter model

Many studies have developed models for the response of APDs [37–40] and SNSPDs [41], and compared the jitter of both types of detectors [42]. Thorough models for the response of APDs have been developed [43]; however, these models rely on complex numerical calculation of the probability distribution function (PDF). In this section, we use an exponentially modified distribution (ex-Gaussian) to model the detector response of both APDs and SNSPDs, using a similar method to that described in Ref. [44]. The response of SNSPDs is usually modeled as a simple Gaussian distribution; however, we observe a tail in our data, which is likely due to the shape of the laser pulse.

The effects of jitter caused by different fibers and their impact on QBER have been studied in Ref. [45]. However, these studies considered only APDs, which have comparatively higher jitter than SNSPDs. The ex-Gaussian distribution is characterized by its full width at half maximum (FWHM) δt and exponential decay rate λ . Assuming the Gaussian standard deviation is given by $\sigma_t \approx 2\sqrt{2 \ln 2} \approx \delta t/2.355$, and optimizing the position of the pulse within T , we can numerically

calculate the intersymbol interference ($\text{ISI}_{\text{jitter}}$)

$$\begin{aligned} \text{ISI}_{\text{jitter}} &= \frac{1}{2}(P(t < 0) + P(t > T)) \\ &= \frac{1}{2}[\text{CDF}(0) + (1 - \text{CDF}(T))], \end{aligned} \quad (1)$$

where the cumulative distribution function (CDF) is

$$\text{CDF}(T) = \int_{-\infty}^T \text{PDF}(t; \mu, \sigma_t, \lambda) dt. \quad (2)$$

$$\text{PDF}(t) = \frac{\lambda}{2} \exp\left[\frac{\lambda}{2}(2\mu + \lambda\sigma_t^2 - 2t)\right] \text{erfc}\left(\frac{\mu + \lambda\sigma_t^2 - t}{\sqrt{2}\sigma_t}\right) \quad (3)$$

is the probability distribution function.

This corresponds to the tail probability outside the gate window, $[0, T]$ for a Gaussian centered at $T/2$, where μ is the Gaussian center, $\sigma = \delta t/2.355$, and $\lambda = \frac{1}{\tau}$ is the exponential decay rate. The decay constant τ is chosen as a fit parameter to reproduce the empirically measured single-pulse timing distribution of each detector.

D. Clock rate projections

The $\text{ISI}_{\text{jitter}}$ represents the probability of photon arrival outside the gate, effectively the probability of a bit flip given that a photon lands in the neighboring bin. The factor of $1/2$ accounts for the symmetric probability of a photon detection leading to an error, due to the randomly selected bit.

This model allows for the estimation of QBER due to detector and system jitter as a function of repetition rate and FWHM, and allows us to calculate estimated projections of the finite-key rates for >1 GHz repetition rate. Figure 2(a) shows the impact on Z $\text{QBER}_{\text{jitter}}$ as the clock rate is increased when using APDs and SNSPDs with 350 and 40 ps FWHM, respectively (solid line). These pulses were measured using a 25 GS/s arbitrary waveform generator to electrically gain-switch a vertical-cavity surface-emitting laser (VCSEL), which is typical of other gain-switched VCSELs [46–48]. Far narrower pulses, on the order of 10 ps have been achieved [49–51]. Histograms of a single pulse from a fixed random pattern are shown for each type of detector in the inset of Fig. 2(a). Single-mode coupling was used for measuring the response of both detectors, to avoid any contribution from using a different fiber. The data shown in Fig. 2(a) were obtained from the measured single-pulse response of each detector by varying the temporal bin width to match the clock rate and calculating the fraction of counts falling outside the bin; further details are provided in the Supplemental Material [52].

It should be noted that the method assumes a transmitter that is capable of generating Gaussian optical pulses, with <40 ps FWHM; the results will vary with the width and shape of the transmitted pulses [46]. We also performed these measurements using fixed pulse trains (010101 ...), to estimate the QBER due to ISI up to 12.5 GHz. However, at higher rates, ISI extends across multiple time bins, causing the measured QBER to be underestimated relative to the model. These results are included in the Supplemental Material [52].

One challenge in satellite-based QKD is the accurate synchronization of the transmitter and receiver clocks. State-

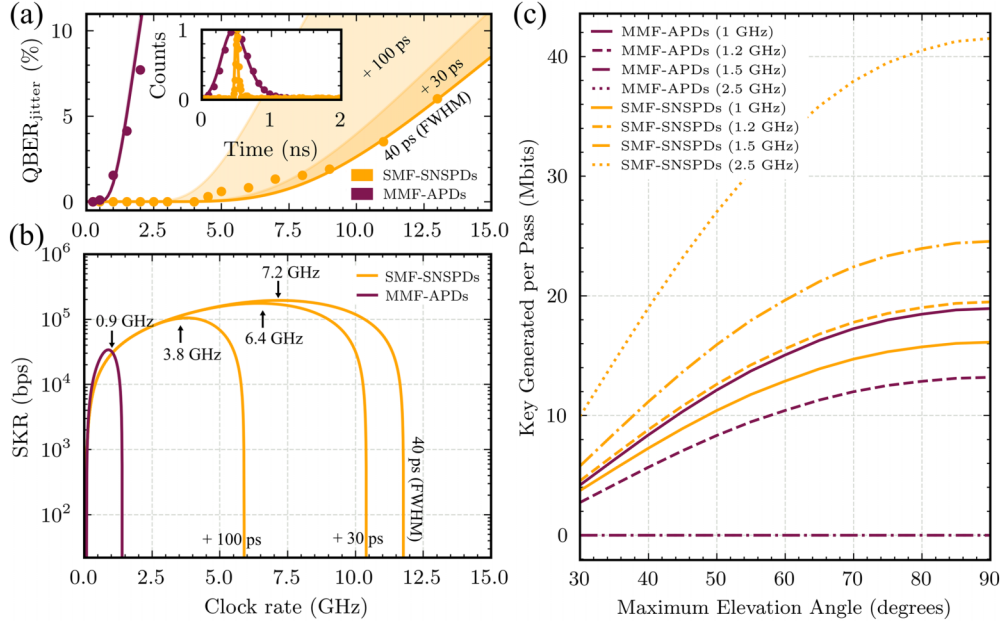


FIG. 2. Jitter analysis results. (a) Experimental data showing the Z QBER increase due to jitter for changing clock rate. The subplot shows the pulse width using SNSPDs vs APDs. The data are collected by binning a single measured pulse on each detector, explained in the Supplemental Material [52]. (b) The finite-key rates against clock rate for multimode APDs and SNSPDs, for a fixed loss of 30 dB, and a fixed session duration of 300 s. (c) The estimated key generated per in an overpass for different maximum elevation angle overpasses. Simulations for MMF-APDs and SMF-SNSPDs are shown at different clock rates. The key generated is calculated using the average loss and the total time for an overpass.

of-the-art demonstrations have achieved sub-100 ps time transfer over turbulent free-space channels [53,54] and real satellite-to-ground links [55,56]. A time-transfer precision of 30 ps was achieved using the Micius satellite [57]. If advanced two-way optical synchronization techniques are used, the error could be reduced to sub-10 ps [58,59], in ideal conditions. We include a conservative 100 ps sensitivity region, as well as a more optimistic 30 ps region, in the projected QBER model, to account for realistic clock synchronization and stability.

Using the estimated increase in Z and X QBER due to jitter (350 and 40 ps FWHM for APDs and SNSPDs, respectively), at higher rates, we calculate the finite-key rate for clock rates, 0.1–15 GHz, for a fixed loss of 30 dB and a fixed session duration of 300 s. The results are shown in Fig. 2(b). The secure key rate initially increases with clock rate, which is expected. However, the secure key rate saturates as the contribution of $\text{QBER}_{\text{jitter}}$ dominates and then starts to decrease rapidly. This effect is reached earlier with MMF-APDs because of the larger $\text{QBER}_{\text{jitter}}$. This clearly shows that for higher clock rates than approximately 1.5 GHz, SNSPDs become essential to be able to obtain a positive key. Based on these projections, the estimated “optimal” clock rates for MMF-APDs and SMF-SNSPDs are 0.9 and 7.2 GHz, respectively. These projections assume an “ideal” transmitter that is capable of producing Gaussian-shaped pulses at these higher clock rates.

To investigate this further, we look at multiple overpasses of different maximum elevations and calculate the secure key rate given the mean loss of the overpass. We use a target block size equal to the maximum sifted bits accumulated in a single overpass. Using the link parameters in Table II, we calculate the expected total key generated per pass for each detector

setup. The results are shown in Fig. 2(c). These results show the clear benefit of SNSPDs at higher clock rates; the coupling efficiency is taken into account. The interesting thing to note here is that at 1 GHz clock rate, MMF-APDs outperform SNSPDs, mainly due to the lower receiver loss. However, when the clock rate is increased to 1.5 GHz, positive secure key rates are no longer possible with MMF-APDs due to jitter effects, while SMF-SNSPDs improve key rates.

The overpass time and average loss are used to calculate a target block size that is used to process the sifted keys. The finite-key length is calculated based on the amount of raw sifted key accumulated during a single overpass, assuming a fixed mean channel loss determined by the maximum elevation angle. Figure 2(c) highlights an important result; that is, at 1 GHz clock rate, more secure key can be obtained per overpass with MMF-APDs than with SMF-SNSPDs. Therefore, it is reasonable to use MMF-APDs for clock rates <1 GHz; this is due to the reduced coupling loss η_{coupling} , when using MMF.

TABLE II. Link model parameters.

Parameter	Value
Transmitter aperture, T_x	0.09 m
OGS aperture, R_x	1 m
Orbital altitude	500 km
Source wavelength	850 nm
OGS central obstruction	30%
Loss after beam-wandering correction	0.4 dB
PAT system accuracy, η_{pat}	3 μrad
Beam divergence, θ	17.2 μrad

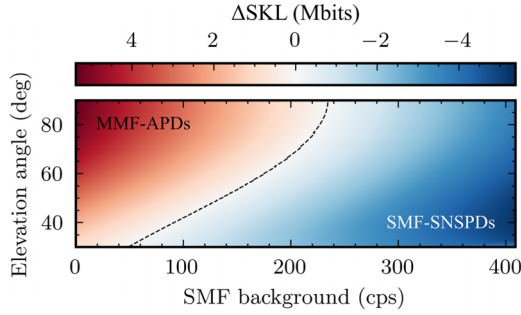


FIG. 3. Background counts sensitivity. Analysis of the crossover between MMF-APDs and SMF-SNSPDs with increasing background counts. Heatmap: The color represents the difference between keys generated with each detector configuration, where the background counts are scaled (1:30) for SMF:MMF. Dashed line indicates where MMF-APDs = SMF-SNSPDs.

However, it is clear that if the clock rate of our system were increased beyond 1 GHz, the effects of jitter become very prominent, motivating the need for low-jitter detectors such as SNSPDs, with adaptive optics, in high clock rate systems.

E. Background counts

Although we use estimated background count rates, for the comparison of SMF- and MMF fiber-based systems, the comparison is worth exploring. We verify the relative background levels seen by SMF and MMF at a ratio approximately 1:30, using a broadband lamp. By varying the background count levels in our finite-key model, we analyze the crossover of SMF-SNSPDs and MMF-APDs, i.e., the maximum elevation angle for which MMF-APDs and SMF-SNSPDs (scaling background counts for MMF) generate the same amount of key. Figure 3 shows the difference in secure key length (SKL) generated per overpass for MMF-APDs and SMF-SNSPDs:

$$\Delta \text{SKL} = \text{SKL}_{\text{MMF-APDs}} - \text{SKL}_{\text{SMF-SNSPDs}}. \quad (4)$$

The inferred crossover, for which SMF-SNSPDs begin to outperform MMF-APDs, is subject to the total receiver loss; this is considered in the next section, where we look at the sensitivity to AO correction.

F. Turbulence model

An important consideration when performing satellite-to-ground QKD is the impact of the atmosphere on the wave front of the quantum signal beam. This affects the coupling into fiber at the receiver. In this section, we provide a simple model to demonstrate the impact of turbulence to the coupling into both single-mode and multimode fibers. This is done to understand the realistic performance of a satellite link with each type of detector coupling method, and these simulations provide useful insights for future experiments.

We use the model used in Refs. [60,61] and the python simulation tool provided in Ref. [62] to model the coupling efficiency to single-mode fiber with varying orders of AO correction (also detailed in Appendix B). The results of the simulated secure key per pass for a 90° elevation overpass are shown against normalized turbulence (D/r_0) in

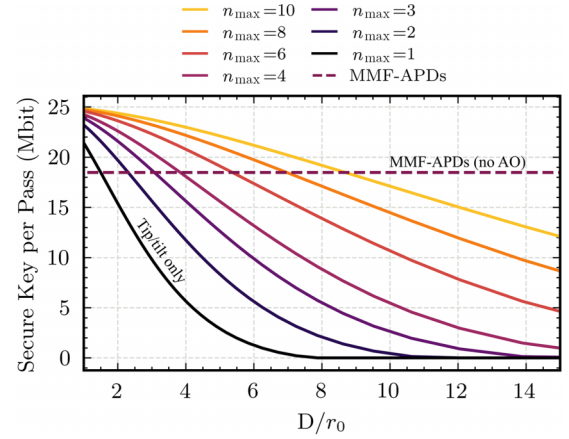


FIG. 4. Secure key per pass under turbulence (SMF-SNSPDs) (90° maximum elevation). Dashed line: The secure key per pass for multimode fiber APDs at receiver with -1.6 dB optics efficiency. Solid lines: Secure key per pass for SNSPDs with AO correction orders of $n_{\text{max}} = \{1, 2, 3, 4, 6, 8, 10\}$.

Fig. 4, where D is the receiver telescope diameter and r_0 is the Fried parameter [63]. For these simulations, we include a fixed receiver optics efficiency of -1.1 dB. The results show the impact of increasing turbulence on the coupling to single-mode fiber with orders of AO correction ($\{1, 2, 3, 4, 6, 8, 10\}$) calculated using the model in Ref. [61]. The simulations suggest that beyond moderate turbulence ($D/r_0 = 8$), key generation with single-mode coupling to SNSPDs, without AO (only tip-tilt correction), is infeasible. Scintillation is assumed to have negligible effects on MMF-APD coupling, compared to SMF-SNSPDs, due to the averaging of speckles across higher order modes. The aperture-averaged scintillation index (flux variance) is used from Ref. [61]. The average residual loss after AO correction is calculated as

$$\langle \eta_{\text{turb}}^{\text{SMF}} \rangle = \langle \eta_{\text{AO}} \rangle \langle \eta_{\text{S}} \rangle, \quad (5)$$

where η_{AO} is the average coupling efficiency after AO correction and η_{S} is the average coupling efficiency due to scintillation (Appendix B).

Assuming a residual loss after AO correction, η_{turb} , of 2 dB [Eq. (5)] for adaptive optics correction ($n = 8$) corresponds to moderate-to-strong turbulence ($D/r_0 \approx 10$). We measure a mean r_0 of 8.4 ± 3 cm, across 2 years, measured at 00:00:00 GMT from May to October 2024 and Jun to November 2025, as presented in the Supplemental Material [52]. For an aperture of $D = 1$ m, this 2 dB residual loss represents a reasonably optimistic scenario, for an AO system which can correct up to $n = 8$. Using geometric optics assumptions [27,64,65], the number of modes required to couple a scintillated beam is approximately $(p \approx (\frac{\pi D}{2r_0})^2)$ [66,67]. Multimode fibers have also been shown experimentally to be very resilient up to the strong turbulence regime [68,69]. We therefore assume that the coupling loss due to turbulence in this range is negligible with MMF-APDs D/r_0 ($\eta_{\text{turb}}^{\text{MMF}} = -0.1$ dB); this is because the scintillated beam is able to redistribute power into higher order modes [28,70,71]. We therefore analyze the dependence of the MMF-APD versus SMF-SNSPD crossover on η_{turb} (0–5 dB). The results are shown in a sensitivity plot

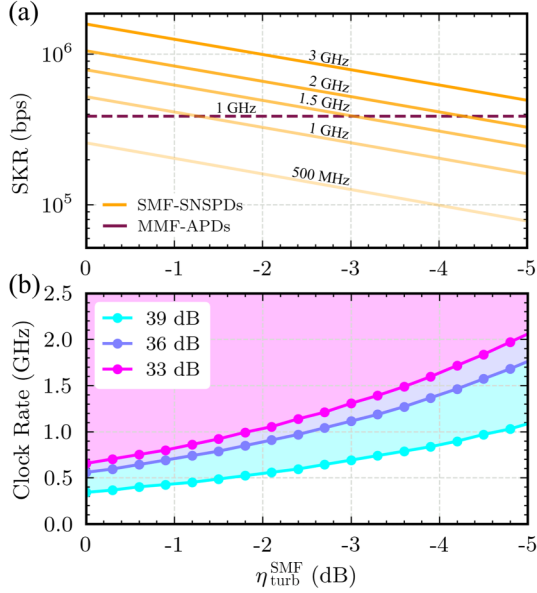


FIG. 5. AO sensitivity analysis. (a) Sensitivity plot for increasing residual loss, η_{turb} (0–5 dB), comparing SMF-SNSPDs at different clock rates, with MMF-APDs at 1 GHz, for 20 dB channel loss. (b) Required clock rate for SNSPD-based system to beat 1 GHz MMF-APDs at a given channel loss (33, 36, 39 dB).

in Fig. 5(a). Figure 5(b) shows the required clock rate that an SMF-SNSPD-based system would need to be clocked in order to outperform MMF-APDs (1 GHz), in key rate, for varying channel loss (33, 36, and 39 dB).

Figure 5, shows explicitly the performance required of an AO system for coupling to single-mode fiber for SNSPDs, the residual loss would need to be $\lesssim 1$ dB, for similar performance to MMF-APDs at 1 GHz.

The experimental emulation of turbulent effects in laboratory is an interesting and active area of research in the field of free-space optical communication and QKD [72,73]. Experiments have looked at the contribution of atmospheric turbulence to the timing jitter [74]; however, this is not taken into account in our model.

III. EXPERIMENTAL RESULTS

In this section, we use an in-laboratory, 3 m free-space QKD system to emulate the high-loss conditions of a satellite-to-ground link, we perform real-time sifting of QKD keys across this link at a clock rate of 1 GHz [14], using the T12 protocol [34]. The parameters used for the protocol are listed in Table III, the protocol is explained in more detail in Appendix D; the parameters chosen here are representative of previous free-space T12 implementations [2,14,34] and were chosen to optimize the secure key generation rate for the expected channel losses in satellite-to-ground channels (>30 dB) [75]. The results comparing MMF-APDs and SNSPDs are shown in this section.

A. Experimental setup

The satellite QKD source utilizes eight VCSELs to generate four polarisation states; $|H\rangle$, $|V\rangle$, $|D\rangle$, and $|A\rangle$ at signal

TABLE III. Decoy-state BB84 parameters: Mean photon number per pulse, μ , X-basis probability, p_x , signal state intensity, μ_u , decoy state intensity, $p = \mu_v$, vacuum state intensity, $p = \mu_w$, error correction efficiency, η_{EC} , security parameter, and ϵ .

Parameter	Value
Clock rate, f_c	1 GHz
X-basis probability, p_x	1/16
Signal state intensity, μ_u	0.4
Decoy state intensity, μ_v	0.05
Vacuum state intensity, μ_w	0.00125
Error correction efficiency, η_{EC}	1.15
Security parameter, ϵ	10^{-10}

and decoy levels. The VCSELs are operated in gain-switched mode, which creates phase-randomized pulses. The width of the applied signal voltage to the lasers is 125 ps. The four polarization states are combined using a polarization-maintaining fiber-based combiner used in Ref. [14] and output from the transmitter as a single-mode beam.

We use eight variable optical attenuators (VOAs) to set the relative levels between each polarization state and one VOA at the output to control the total mean photon number. The single-mode output is split on a beam splitter to allow for monitoring of the output power using an optical power meter. This monitoring power meter is used to accurately characterize the channel and receiver losses of the system, by using a flip mirror to direct the attenuated light toward it. Using a characterization laser, the channel losses can be measured and the receiver loss can be characterized. Two quarter wave plates are used to align the polarization states after propagation through the single-mode fiber.

At the receiver, the majority (Z) and minority (X) bases are split by a 90:10 beam splitter and the polarization states are separated by polarizing beam splitters (PBS). A PBS is placed on the reflected arm of each basis measurement, effectively functioning as a polarizing filter to avoid angle-dependent polarisation extinction ratio (PER) effects of the reflected beam. Each state is coupled into a fiber. When coupled to SNSPDs, the single-mode fibers are sent through polarization controllers and then pass down 20 m of SMF-28, because the SNSPD system is located outside our laboratory. The extra 20 m of fiber was measured to have minimal effect on the mode dispersion and FWHM of the pulses. The output from the detectors is sent both to a time tagger and to a custom FPGA, which allows for real-time sifting of the keys. See the Supplemental Material [52] for more details on the experimental setup.

B. Real-time QKD comparison

The results are shown for secure key rate and QBER against loss in Figs. 6(a) and 6(b) for MMF-APDs and SNSPDs, respectively. These data are generated by performing EC and PA on real-time sifted keys, processed with 16 Mbit block size. The expected key rates and QBER are shown (solid line), based on the parameters in Table III. Due to system imperfections and fluctuation in the QBER during measurement periods, the measured secure key rates for

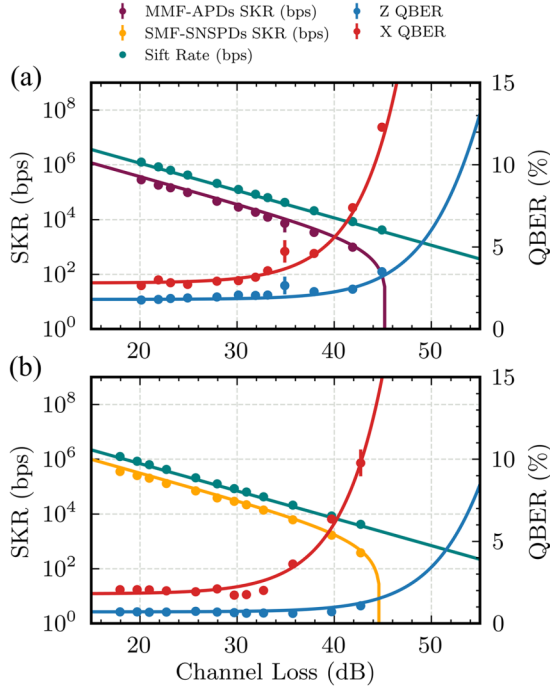


FIG. 6. Experimental results comparison. (a) Results for key rate vs loss using multimode fiber-coupled APDs with an Rx loss of 1.6 dB. The Z and X QBER is plotted with baseline values of 0.018 and 0.028, respectively. (b) Results for key rate vs loss using single-mode fiber-coupled SNSPDs, with an Rx loss of 5.6 dB. The Z and X QBER is plotted with baseline values of 0.008 and 0.018, respectively. All data are at 1 GHz clock rate.

both systems fluctuates. It is worth noting that no additional background light was introduced to the model or experiment. The background light was minimized in the laboratory for both SMF and MMF (approximately 200 cps, on average).

It is important to note that because of the passive basis selection in our receiver, the dark counts impact the minority basis (X) QBER more strongly than the majority basis (Z) QBER. This does not happen in actively selected systems or in systems where the basis selection probability is equal. Erroneous counts due to dark counts and background counts in the Z-basis signal ($EuZZ$) are proportional to $N_u P_Z (P_Z P_{BGC} + P_{DC})$, where N_u is the number of signal states sent by Alice and P_Z is the Z-basis selection probability.

IV. DISCUSSION AND CONCLUSIONS

In this paper, we have assessed the feasibility of performing satellite-to-ground quantum key distribution under realistic channel losses at clock rates beyond 1 GHz. While the experimental validation presented here is limited to end-to-end QKD operation at a 1 GHz clock rate, detector timing measurements and finite-key modeling are used to project performance at clock rates up to 15 GHz, with realistic budgets for timing and synchronization error. These projections estimate an optimal operating clock rate of 0.9 and 7.2 GHz for MMF-APD- and SMF-SNSPD-based systems, respectively. The results of the comparison both theoretically and experimentally indicate that at clock rates lower than 1 GHz, MMF-APDs are generally a better option, due to low cost, ease of

implementation, and higher secure key rates. This is mainly due to the added insertion loss to the receiver when single-mode coupling is used. We also show that for clock rates beyond 1 GHz, SNSPDs become essential for achieving positive key rates due to having a much smaller contribution to the QBER due to jitter ($QBER_{\text{jitter}}$).

We also provide a detailed sensitivity analysis of AO performance, highlighting the level of residual coupling loss that must be achieved for single-mode SNSPD-based receivers to outperform MMF-APD systems, providing quantitative performance targets for future optical ground station designs. In addition to the capability of SNSPDs to achieve higher clock rates, the improved timing resolution may be useful for security enhancement against timing-based attacks [76,77]. The security against these types of attacks is not fully explored within this study; however, it should be noted that with SNSPDs, the bottleneck in the timing indistinguishability of the pulses is transferred to the transmitter. In our experiments, we ensured that timing of individual lasers at the transmitter were aligned.

A. Further challenges for multi-GHz satellite QKD

One of the main challenges restricting satellite-based QKD to slower rates is the size, weight, and power (SWaP) requirement for on-board transmitters. High-quality and fast lasers often require power-hungry driving electronics, limiting the rates that can be realistically achieved in small satellite implementations. There are other issues with simply achieving high repetition rates, such as the need for fast electronics, and patterning effects in lasers.

B. Outlook

The use of satellites for quantum key distribution proposes a solution for the long-distance transfer of quantum information, which is a vital part of the future “quantum internet.” In an envisioned future global quantum network, >1 GHz clock rate links will be necessary to reduce the need for large satellite constellations which fill the night sky [78]. This investigation should aid the design choices made of future satellite QKD missions aiming for ultrafast clock rates.

ACKNOWLEDGMENT

The authors would like to acknowledge financial support from UKRI Projects 10089202 and 2911864.

O.M.C. designed and performed the study, with input from T.R., C.P., and R.S. T.R. designed the FPGA firmware and electronics. O.M.C. performed the simulations and experimental analysis, with help from T.R., C.P., and R.S. O.M.C. wrote the article, with input from all authors. R.I.W. wrote the software for E.C. and P.A. R.J.D., R.M.S., and A.J.S. provided guidance and direction for the work.

DATA AVAILABILITY

The data that support the findings of this article are not publicly available because they contain commercially sensitive information. The data are available from the authors upon reasonable request.

APPENDIX A: LINK MODEL

The total transmission efficiency of a satellite-to-ground QKD link can be estimated as a function of the satellite elevation angle (α), full-angle beam divergence (θ), PAT error (ϵ_{PAT}), and the wavelength (λ). This considers the impact due to diffraction (η_{diff}), atmospheric transmissivity (η_{atm}), pointing, acquisition, and tracking (PAT) efficiency (η_{pat}), coupling efficiency (η_{coupling}), photon detection efficiency (η_{det}), the efficiency of the optics at the receiver (η_{rx}), and decoherence of the beam via turbulence effects (η_{turb}) [14].

$$\eta(\alpha, \theta, \lambda) = \eta_{\text{diff}}(\alpha, \theta) \eta_{\text{atm}}(\alpha) \eta_{\text{turb}} \eta_{\text{det}} \eta_{\text{rx}} \eta_{\text{coupling}} \eta_{\text{pat}}, \quad (\text{A1})$$

with

$$\eta_{\text{diff}}(\alpha, \theta) = \frac{D_r^2 \eta_{\text{obs}}}{[\theta L(\alpha)]^2}, \quad (\text{A2})$$

and where D_r is the diameter of the receiver telescope, η_{obs} is the transmissivity of the receiver telescope due to the central obstruction (0.91, for 30% diameter obstruction), and L is the link distance. The parameter η_{atm} is given by

$$\eta_{\text{atm}} = \eta_{\lambda}^{\text{csc}(\alpha)}, \quad (\text{A3})$$

where η_{λ} is the atmospheric transmissivity at zenith [79] and changes as a function of wavelength. The link distance and time for which the satellite is visible are given in Refs. [14,80].

APPENDIX B: SINGLE-MODE COUPLING UNDER TURBULENCE

The coupling efficiency of the j th mode is the ratio of the average coupled power to the average power incident on the aperture. Single-mode coupling efficiency can be modeled as the overlap integrals of a Gaussian beam with the fundamental mode, using the theoretical framework in Ref. [68]

$$\eta_j = \frac{\langle \mathbf{P}_{c,j} \rangle}{\langle \mathbf{P}_a \rangle} = \frac{|\int_B \mathbf{E}_{i,\text{fiber}}(\vec{r}) E_{j,\text{fiber}}^*(\vec{r}) d\vec{r}|^2}{\langle \int_A |\mathbf{E}_{i,\text{lens}}(\vec{r})|^2 d\vec{r} \rangle}, \quad (\text{B1})$$

where $\mathbf{E}_{i,\text{lens}}(\vec{r})$ and $\mathbf{E}_{i,\text{fiber}}(\vec{r})$, describe the incident optical field on the lens and fiber plane, respectively, and $E_{j,\text{fiber}}^*(\vec{r})$ is the complex conjugate of the j th normalized fiber mode field.

In an ideal situation, the incoming beam is Gaussian, but after propagation through an atmospheric channel, the wave front of the beam will be distorted. The Fried parameter r_0 is commonly used to characterize the transmission of light through the atmosphere [81,82]:

$$r_0 = \left[0.42 k^2 \sec(\zeta) \int_0^{h_{\text{max}}} C_n^2(h) dh \right]^{-3/5}, \quad (\text{B2})$$

where $C_n^2 = (79 \times 10^{-6} P/T^2) C_T^2$, is the structure parameter, $k = 2\pi/\lambda$ is the wave number, ζ is the elevation angle, h_{max} is the turbulent path length, and h is the satellite altitude. The size of the r_0 parameter represents the coherence length of a plane wave in a turbulent medium, or a measure of the distance over which the distortions to the wave front are constant. A larger r_0 means larger turbulent cells and thus coarser distortions to the wave front, which is desirable [83–85].

Turbulence therefore affects the overlap integral with the fundamental mode of a single-mode fiber; this effect is not

nearly as prominent with multimode fiber, which can accept multiple modes.

Using equations derived in Refs. [29,86], the instantaneous single-mode coupling efficiency can be defined in terms of the Zernike coefficients $b_n^m(t)$ [63,87]:

$$\eta_{\text{AO}}(t) = \exp \left[- \sum_{n,m} b_n^m(t)^2 \right]. \quad (\text{B3})$$

The average coupling efficiency is in Refs. [60,61]:

$$\langle \eta_{\text{AO}} \rangle = \prod_{n,m} \frac{1}{\sqrt{1 + 2\langle b_n^m \rangle^2}}, \quad (\text{B4})$$

where $\langle b_n^m \rangle^2$ depends on D/r_0 [88].

Following Ref. [61], for the scintillation-induced irradiance fluctuations, which AO cannot correct for when coupling to SMF, we use the aperture-averaged, on-axis scintillation index σ_I^2 , defined in Ref. [82]:

$$\sigma_I^2(D) = \exp \left[\frac{0.49 \sigma_B^2}{(1 + 0.18d^2 + 0.56\sigma_B^{12/5})^{7/6}} + \frac{0.51 \sigma_B^2 (1 + 0.69\sigma_B^{12/5})^{-5/6}}{(1 + 0.90d^2 + 0.62d^2\sigma_B^{12/5})} \right] - 1. \quad (\text{B5})$$

Here, $k = 2\pi/\lambda$ is the optical wave number and $d = \sqrt{\frac{kD^2}{4z}}$ is the normalized aperture parameter, where z is conservatively set as 100 km. The turbulence strength parameter is defined as $\sigma_B^2 = 0.4065 \sigma_R^2$, where σ_R^2 is the Rytov variance. The average coupling efficiency due to scintillation to SMF, η_S , is approximated as

$$\langle \eta_S \rangle \approx (1 + \sigma_I^2(D))^{-1/4}. \quad (\text{B6})$$

This model for single-mode fiber coupling efficiency with partial adaptive optics corrections and scintillation effects is used for the data presented in Fig. 5.

APPENDIX C: CLASSICAL COMMUNICATION BUDGET

One potential bottleneck that is worth investigating is the classical bandwidth requirements for real-time sifting of QKD at multi-GHz rates. Reference [89] provides an estimation of the postprocessing uplink data rate, given by $R_c = \eta f_c \mu N_b$, where η is the channel efficiency, f_c is the clock rate, μ is the mean photon number, and N_b is the number of bits required to represent a single detection event (64 bits).

In Fig. 7, we show the minimum classical data rate required for real-time sifting at QKD clock rates of 1–15 GHz, during an overpass with a maximum elevation angle of 90°. The lowest data rate required for 15 GHz clock rate is approximately 325 Mbps. Currently, ground-to-satellite (up-link) links remain a challenge in classical laser communications [90–93], which may pose as a bottleneck for the rates that QKD data can be sifted using optical communication.

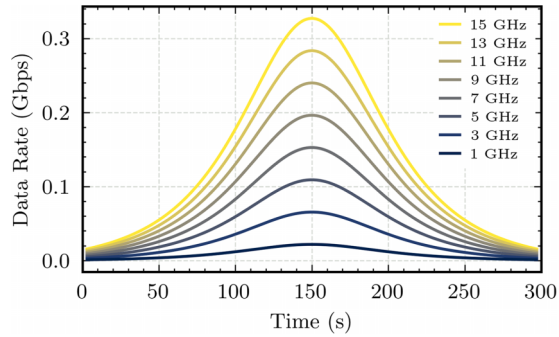


FIG. 7. Classical communication budget. The sifting classical data rate requirements for an overpass with 90° maximum elevation angle, for system clock rates of 1–15 GHz.

APPENDIX D: T12 PROTOCOL

The setup utilizes the T12 protocol [34,94] to share keys using polarization encoding. The four polarization states $|H\rangle$, $|V\rangle$, $|D\rangle$, and $|A\rangle$ are selected and encoded relative to two bases $\{Z, X\}$ and two bits $\{0, 1\}$ for each basis. The ba-

sis selection probabilities $\{p(Z), p(X)\}$ can be optimized such that $p(Z) > p(X)$, ensuring the maximum number of events where the bases match while enough events in the minority basis provides reliable estimation of the error, δ . Three intensity levels are selected from at random, referred to as signal (u), decoy (v), and vacuum (w). We send the bases with probabilities of $p_Z = 15/16$ and $p_X = 1 - p_Z$. The relative intensity levels of the three states are set to $\mu_u = 0.4$ photons per symbol, $\mu_v = 0.05$, and $\mu_w < 0.00125$, which we found to be optimum for our system. Both decoy and vacuum intensity are selected with probability, $1/16$.

During an overpass, the time available to collect and sift raw key bits is limited to a few hundreds of seconds in LEO orbits, which the finite-key length effects are large and need to be taken into account during privacy amplification [5]. The finite effects in three decoy-state BB84 have been extensively studied, with multiple methods arising for calculating the security bounds [34,95,96]. For this study, we use a secrecy parameter of 100 dB and calculate finite-key rates based on the security proof of T12 [34,94], which relies on the Clopper-Pearson confidence interval [97].

- [1] V. Mavroudis, K. Vishi, M. D. Zych, and A. Jøssang, The impact of quantum computing on present cryptography, *Int. J. Adv. Comput. Sci. Appl.* **9**, 405 (2018).
- [2] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, *Nature (London)* **557**, 400 (2018).
- [3] Y. Li, W.-Q. Cai, J.-G. Ren, C.-Z. Wang, M. Yang, L. Zhang, H.-Y. Wu, L. Chang, J.-C. Wu, B. Jin *et al.*, Microsatellite-based real-time quantum key distribution, *Nature (London)* **640**, 47 (2025).
- [4] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villorresi, Feasibility of satellite quantum key distribution, *New J. Phys.* **11**, 045017 (2009).
- [5] J. Sidhu, T. Brougham, D. McArthur, R. Pousa, and D. Oi, Finite key effects in satellite quantum key distribution, *npj Quantum Inf* **8**, 18 (2022).
- [6] T. Islam, J. S. Sidhu, B. L. Higgins, T. Brougham, T. Vergoossen, D. K. Oi, T. Jennewein, and A. Ling, Finite-resource performance of small-satellite-based quantum-key-distribution missions, *PRX Quantum* **5**, 030101 (2024).
- [7] R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, and C. G. Peterson, Quantum cryptography for secure free-space communications, in *Free-Space Laser Communication Technologies XI*, edited by G. S. Mecherle (SPIE, San Jose, CA, United States, 1999), Vol. 3615, pp. 98–103.
- [8] A. Tomaello, C. Bonato, V. Da Deppo, G. Naletto, and P. Villorresi, Link budget and background noise for satellite quantum key distribution, *Adv. Space Res.* **47**, 802 (2011).
- [9] J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. K. Khandani, N. Lütkenhaus, and T. Jennewein, Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations, *Phys. Rev. A* **92**, 052339 (2015).
- [10] V. M. Acosta, D. Dequal, M. Schiavon, A. Montmerle-Bonnefois, C. B. Lim, J.-M. Conan, and E. Diamanti, Analysis of satellite-to-ground quantum key distribution with adaptive optics, *New J. Phys.* **26**, 023039 (2024).
- [11] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, Satellite-to-ground quantum key distribution, *Nature (London)* **549**, 43 (2017).
- [12] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li *et al.*, Ground-to-satellite quantum teleportation, *Nature (London)* **549**, 70 (2017).
- [13] C.-Y. Lu, Y. Cao, C.-Z. Peng, and J.-W. Pan, Micius quantum experiments in space, *Rev. Mod. Phys.* **94**, 035001 (2022).
- [14] T. Roger, R. Singh, C. Perumangatt, D. G. Marangon, M. Sanzaro, P. R. Smith, R. I. Woodward, and A. J. Shields, Real-time gigahertz free-space quantum key distribution within an emulated satellite overpass, *Sci. Adv.* **9**, eadj5873 (2023).
- [15] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, Performance and security of 5 GHz repetition rate polarization-based quantum key distribution, *Appl. Phys. Lett.* **117**, 144003 (2020).
- [16] Z.-X. Wang, H.-X. Xu, J. Li, H.-C. Yu, J.-Q. Huang, H. Han, C.-L. Wang, P. Zhang, F.-F. Yin, K. Xu *et al.*, 10 GHz robust polarization modulation towards high-speed satellite-based quantum communication, *EPJ Quantum Technol.* **12**, 47 (2025).
- [17] G. Buller and R. Collins, Single-photon generation and detection, *Meas. Sci. Technol.* **21**, 012002 (2010).
- [18] R. Bedington, J. M. Arrazola, and A. Ling, Progress in satellite quantum key distribution, *npj Quantum Inf.* **3**, 30 (2017).
- [19] S. Ecker, B. Liu, J. Handsteiner, M. Fink, D. Rauch, F. Steinlechner, T. Scheidl, A. Zeilinger, and R. Ursin, Strategies for achieving high key rates in satellite-based QKD, *npj Quantum Inf.* **7**, 5 (2021).
- [20] B. Korzh, Q.-Y. Zhao, J. P. Allmaras, S. Frasca, T. M. Autry, E. A. Bersin, A. D. Beyer, R. M. Briggs, B. Bumble,

- M. Colangelo, *et al.*, Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector, *Nat. Photon.* **14**, 250 (2020).
- [21] D. V. Reddy, R. R. Nerem, S. W. Nam, R. P. Mirin, and V. B. Verma, Superconducting nanowire single-photon detectors with 98% system detection efficiency at 1550 nm, *Optica* **7**, 1649 (2020).
- [22] M. T. Gruneisen, B. A. Sickmiller, M. B. Flanagan, J. P. Black, K. E. Stoltenberg, and A. W. Duchane, Adaptive spatial filtering for daytime satellite quantum key distribution, in *Emerging Technologies in Security and Defence II; and Quantum-Physics-Based Information Security III*, edited by K. L. Lewis, R. C. Hollins, T. J. Merlet, A. Toet, M. T. Gruneisen, M. Dusek, and J. G. Rarity (SPIE, Amsterdam, Netherlands, 2014), Vol. 9254, pp. 7–20.
- [23] M. T. Gruneisen, M. B. Flanagan, and B. A. Sickmiller, Modeling satellite-Earth quantum channel downlinks with adaptive-optics coupling to single-mode fibers, *Opt. Eng.* **56**, 1 (2017).
- [24] C. B. Lim, A. Montmerle-Bonnefois, C. Petit, J.-F. Sauvage, S. Meimon, P. Perrault, F. Mendez, B. Fleury, J. Montri, J.-M. Conan *et al.*, Single-mode fiber coupling with adaptive optics for free-space optical communication under strong scintillation, in *2019 IEEE International Conference on Space Optical Systems and Applications (ICSOS)* (IEEE, Portland, OR, USA, 2019), pp. 1–6.
- [25] M. Chen, C. Liu, and H. Xian, Experimental demonstration of single-mode fiber coupling over relatively strong turbulence with adaptive optics, *Appl. Opt.* **54**, 8722 (2015).
- [26] Y. Bian, Y. Li, E. Chen, W. Li, X. Hong, J. Qiu, and J. Wu, Free-space to single-mode fiber coupling efficiency with optical system aberration and fiber positioning error under atmospheric turbulence, *J. Opt.* **24**, 025703 (2022).
- [27] D. Zheng, Y. Li, E. Chen, B. Li, D. Kong, W. Li, and J. Wu, Free-space to few-mode-fiber coupling under atmospheric turbulence, *Opt. Express* **24**, 18739 (2016).
- [28] Y. Dikmelik and F. M. Davidson, Fiber-coupling efficiency for free-space optical communication through atmospheric turbulence, *Appl. Opt.* **44**, 4946 (2005).
- [29] J. Ma, L. Ma, Q. Yang, and Q. Ran, Statistical model of the efficiency for spatial light coupling into a single-mode fiber in the presence of atmospheric turbulence, *Appl. Opt.* **54**, 9287 (2015).
- [30] L. Zhang, M. Gu, T. Jia, R. Xu, C. Wan, L. Kang, J. Chen, and P. Wu, Multimode fiber coupled superconductor nanowire single-photon detector, *IEEE Photonics J.* **6**, 1 (2014).
- [31] J. Chang, I. E. Zadeh, J. W. N. Los, J. Zichi, A. Fognini, M. Gevers, S. Dorenbos, S. F. Pereira, P. Urbach, and V. Zwiller, Multimode-fiber-coupled superconducting nanowire single-photon detectors with high detection efficiency and time resolution, *Appl. Opt.* **58**, 9803 (2019).
- [32] F. Fleming, W. McCutcheon, E. E. Wollman, A. D. Beyer, V. Anant, B. Korzh, J. P. Allmaras, L. Narváez, S. Leedumrongwathanakun, G. S. Buller, M. Malik, and M. D. Shaw, High-efficiency, high-count-rate 2D superconducting nanowire single-photon detector array, *Opt. Express* **33**, 27602 (2025).
- [33] N. Calandri, Q.-Y. Zhao, D. Zhu, A. Dane, and K. K. Berggren, Superconducting nanowire detector jitter limited by detector geometry, *Appl. Phys. Lett.* **109**, 152601 (2016).
- [34] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, Efficient decoy-state quantum key distribution with quantified security, *Opt. Express* **21**, 24550 (2013).
- [35] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, *Phys. Rev. A* **72**, 012326 (2005).
- [36] A. K. Ekert, Quantum cryptography based on bell's theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [37] F. M. Davidson and X. Sun, Gaussian approximation versus nearly exact performance analysis of optical communication systems with PPM signaling and APD receivers, *IEEE Trans. Commun.* **36**, 1185 (1988).
- [38] P. J. Clarke, R. J. Collins, P. A. Hiskett, M.-J. García-Martínez, N. J. Krichel, A. McCarthy, M. G. Tanner, J. A. O'Connor, C. M. Natarajan, S. Miki *et al.*, Analysis of detector performance in a gigahertz clock rate quantum key distribution system, *New J. Phys.* **13**, 075008 (2011).
- [39] M. Stipčević, D. Wang, and R. Ursin, Characterization of a commercially available large area, high detection efficiency single-photon avalanche diode, *J. Lightwave Technol.* **31**, 3591 (2013).
- [40] A. Ingargiola, M. Assanelli, A. Gallivanoni, I. Rech, M. Ghioni, and S. Cova, Avalanche buildup and propagation effects on photon-timing jitter in Si-SPAD with non-uniform electric field, in *Advanced Photon Counting Techniques III*, edited by M. A. Itzler and J. C. Campbell (SPIE, Orlando, Florida, 2009), Vol. 7320, pp. 103–114.
- [41] M. Sidorova, A. Semenov, A. Kuzmin, I. Charaev, S. Doerner, and M. Siegel, Intrinsic jitter in photon detection by straight superconducting nanowires, *IEEE Trans. Appl. Supercond.* **28**, 1 (2018).
- [42] T. Seki, H. Shibata, H. Takesue, Y. Tokura, and N. Imoto, Comparison of timing jitter between NbN superconducting single-photon detector and avalanche photodiode, *Physica C* **470**, 1534 (2010).
- [43] F. Rosset, A. Pilotto, L. Selmi, M. Antonelli, F. Arfelli, G. Biasiol, G. Cautero, D. De Angelis, F. Driussi, R. Menk *et al.*, A model for the jitter of avalanche photodiodes with separate absorption and multiplication regions, *Nucl. Instrum. Methods Phys. Res. A* **977**, 164346 (2020).
- [44] F. Sun, Y. Xu, Z. Wu, and J. Zhang, A simple analytic modeling method for SPAD timing jitter prediction, *IEEE J. Electron Devices Soc.* **7**, 261 (2019).
- [45] A. Lee, A. T. Castillo, C. Whitehill, and R. Donaldson, Quantum bit error rate timing jitter dependency on multi-mode fibers, *Opt. Express* **31**, 6076 (2023).
- [46] A. R. Pérez, M. F. V. Suárez, A. P. Serrano, J. M. G. Tijero, and I. E. Moscardo, Characterization of optical pulses generated by gain switching a 1310 nm VCSEL, in *X Reunión Española de Optoelectrónica OPTOEL2017*, 12-14 Julio, Santiago de Compostela (2017).
- [47] G. Hasnain, J. Wiesenfeld, T. Damen, J. Shah, J. Wynn, Y. Wang, and A. Cho, Electrically gain-switched vertical-cavity surface-emitting lasers, *IEEE Photonics Technol. Lett.* **4**, 6 (2002).
- [48] K. M. Krishna, M. G. Madhan, and P. Ashok, Study of gain switching in vertical cavity surface emitting laser under different electrical pulse inputs, *Def. Sci. J.* **70**, 538 (2020).
- [49] P. Pepeljugoski, J. Lin, J. Gamelin, M. Hong, and K. Lau, Ultralow timing jitter in electrically gain-switched vertical

- cavity surface emitting lasers, *Appl. Phys. Lett.* **62**, 1588 (1993).
- [50] P. Pepeljugoski, D. Cutrer, and K. Lau, 3.4 ps wide compressed optical pulses from electrically gain-switched vertical cavity surface emitting laser, *Electron. Lett.* **30**, 491 (1994).
- [51] A. Asahara, S. Chen, T. Ito, M. Yoshita, W. Liu, B. Zhang, T. Suemoto, and H. Akiyama, Direct generation of 2-ps blue pulses from gain-switched InGaN VCSEL assessed by up-conversion technique, *Sci. Rep.* **4**, 6401 (2014).
- [52] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/y12y-yk88> for additional data, supporting figures, and experimental methods.
- [53] I. Khader, H. Bergeron, L. C. Sinclair, W. C. Swann, N. R. Newbury, and J.-D. Deschênes, Time synchronization over a free-space optical communication channel, *Optica* **5**, 1542 (2018).
- [54] K. U. Schreiber, I. Prochazka, P. Lauber, U. Hugentobler, W. Schafer, L. Cacciapuoti, and R. Nasca, Ground-based demonstration of the European Laser Timing (ELT) experiment, *IEEE Trans. Ultrason. Ferroelectr. Freq. Control* **57**, 728 (2010).
- [55] T. Ritz, D. Coogan, J. W. Conklin, J. T. Coffaro, P. Serra, S. Nydam, J. Hanson, A. N. Nguyen, C. Priscal, J. Stupl *et al.*, Laser time-transfer facility and preliminary results from the CHOMPTT CubeSat mission, *Adv. Space Res.* **71**, 4498 (2023).
- [56] I. Prochazka and F. Yang, Photon counting module for laser time transfer via Earth orbiting satellite, *J. Mod. Opt.* **56**, 253 (2009).
- [57] H. Dai, Q. Shen, C.-Z. Wang, S.-L. Li, W.-Y. Liu, W.-Q. Cai, S.-K. Liao, J.-G. Ren, J. Yin, Y.-A. Chen *et al.*, Towards satellite-based quantum-secure time transfer, *Nat. Phys.* **16**, 848 (2020).
- [58] H. Yang, H. Wang, X. Wang, H. Yi, W. Yang, H. Wang, and S. Zhang, Picosecond-precision optical two-way time transfer in free space using flexible binary offset carrier modulation, *OSA Continuum* **3**, 1264 (2020).
- [59] F. R. Giorgetta, W. C. Swann, L. C. Sinclair, E. Baumann, I. Coddington, and N. R. Newbury, Optical two-way time and frequency transfer over free space, *Nat. Photon.* **7**, 434 (2013).
- [60] I. Karakosta-Amarantidou, R. Yehia, and M. Schiavon, Free-space model for a balloon-based quantum network, *Phys. Rev. Res.* **7**, 023199 (2025).
- [61] A. Scriminich, G. Foletto, F. Picciariello, A. Stanco, G. Vallone, P. Villoresi, and F. Vedovato, Optimal design and performance evaluation of free-space quantum key distribution systems, *Quantum Sci. Technol.* **7**, 045029 (2022).
- [62] I. Karakosta-Amarantidou, R. Yehia, and M. Schiavon, Balloon_qnet code, Zenodo, 2025, <https://zenodo.org/records/15388482>.
- [63] D. L. Fried, Statistics of a geometric representation of wavefront distortion, *J. Opt. Soc. Am.* **55**, 1427 (1965).
- [64] S. Arisa, Y. Takayama, H. Endo, R. Shimizu, M. Fujiwara, and M. Sasaki, Coupling efficiency of laser beam to multimode fiber for free space optical communication, in *International Conference on Space Optics—ICSO 2014* (SPIE, 2017), Vol. 10563, pp. 264–271.
- [65] J. Niu and J. Xu, Coupling efficiency of laser beam to multimode fiber, *Opt. Commun.* **274**, 315 (2007).
- [66] M. Diab, A. N. Dinkelaker, J. Davenport, K. Madhav, and M. M. Roth, Starlight coupling through atmospheric turbulence into few-mode fibres and photonic lanterns in the presence of partial adaptive optics correction, *Mon. Not. R. Astron. Soc.* **501**, 1557 (2020).
- [67] S. Minardi, R. Harris, and L. Labadie, Astrophotonics: Astronomy and modern optics, *Astron. Astrophys. Rev.* **29**, 6 (2021).
- [68] X. Fan, D. Wang, J. Cheng, J. Yang, and J. Ma, Few-mode fiber coupling efficiency for free-space optical communication, *J. Lightwave Technol.* **39**, 1823 (2021).
- [69] V. D. Correia, M. A. Fernandes, P. P. Monteiro, F. P. Guiomar, and G. M. Fernandes, On the impact and mitigation of turbulence in fiber-coupled FSO systems, *IEEE Access* **12**, 69505 (2024).
- [70] Y. Dikmelik and F. M. Davidson, Fiber coupling efficiency for free-space optical communication through atmospheric turbulence, in *Free-Space Laser Communication Technologies XVI*, edited by S. Mecherle, C. Y. Young, and J. S. Strykowski (SPIE, San Jose, CA, 2004), Vol. 5338, pp. 76–80.
- [71] S. Selvanandan and P. Anbarasan, Power coupling efficiency enhancement in multimode step-index fiber using refractive and diffractive microlenses, *Int. J. Opt.* **2010**, 1 (2010).
- [72] A. H. Fahim Raouf, M. Safari, and M. Uysal, Performance analysis of quantum key distribution in underwater turbulence channels, *J. Opt. Soc. Am. B* **37**, 564 (2020).
- [73] L. Scarfe, F. Hufnagel, M. F. Ferrer-Garcia, A. D’Errico, K. Heshami, and E. Karimi, Fast adaptive optics for high-dimensional quantum communications in turbulent channels, *Commun. Phys.* **8**, 79 (2025).
- [74] E. D. Caldwell, W. C. Swann, J. L. Ellis, M. I. Bodine, C. Mak, N. Kuczun, N. R. Newbury, L. C. Sinclair, A. Muschinski, and G. B. Rieker, Optical timing jitter due to atmospheric turbulence: Comparison of frequency comb measurements to predictions from micrometeorological sensors, *Opt. Express* **28**, 26661 (2020).
- [75] R. Singh, T. Roger, C. Perumangatt, M. Sanzaro, R. Woodward, and A. Shields, QKD secret key scaling with ground station aperture size and satellite overpass, in *Quantum 2.0* (Optica Publishing Group, 2024), pp. QTh3A–38.
- [76] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Time-shift attack in practical quantum cryptosystems, [arXiv:quant-ph/0512080](https://arxiv.org/abs/quant-ph/0512080).
- [77] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, *Phys. Rev. A* **78**, 042333 (2008).
- [78] S. Dunne, Rage against the dying of the light: Regulation of light pollution from satellites, *U. Ill. L. Rev.* 1021 (2023).
- [79] D. Vasylyev, W. Vogel, and F. Moll, Satellite-mediated quantum atmospheric links, *Phys. Rev. A* **99**, 053830 (2019).
- [80] I. Ali, N. Al-Dhahir, and J. E. Hershey, Predicting the visibility of LEO satellites, *IEEE Trans. Aerosp. Electron. Syst.* **35**, 1183 (2002).
- [81] H. Weichel, *Laser Beam Propagation in the Atmosphere* (SPIE Press, Bellingham, Washington, 1990), Vol. 3.
- [82] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Media*, 2nd ed. (SPIE Press, Bellingham, Washington, 2005).
- [83] H. Zhan, E. Wijerathna, and D. Voelz, Is the formulation of the Fried parameter accurate in the strong turbulent scattering regime? *OSA Continuum* **3**, 2653 (2020).
- [84] S. Shaklan and F. Roddier, Coupling starlight into single-mode fiber optics, *Appl. Opt.* **27**, 2334 (1988).

- [85] R. K. Tyson and B. W. Frazier, *Principles of Adaptive Optics* (CRC Press, Boca Raton, Florida, 2022).
- [86] L. Canuet, N. Védrenne, J.-M. Conan, C. Petit, G. Artaud, A. Rissons, and J. Lacan, Statistical properties of single-mode fiber coupling of satellite-to-ground laser links partially corrected by adaptive optics, *J. Opt. Soc. Am. A* **35**, 148 (2018).
- [87] R. J. Noll, Zernike polynomials and atmospheric turbulence, *J. Opt. Soc. Am.* **66**, 207 (1976).
- [88] G. D. Boreman and C. Dainty, Zernike expansions for non-Kolmogorov turbulence, *J. Opt. Soc. Am. A* **13**, 517 (1996).
- [89] R. Singh, C. Perumangatt, T. Roger, and A. Shields, Feasibility of real-time satellite to ground QKD, in *CLEO: Fundamental Science* (Optica Publishing Group, 2023), pp. JW2A–101.
- [90] K. Saucke, C. Seiter, F. Heine, M. Gregory, D. Tröndle, E. Fischer, T. Berkefeld, M. Feriencik, M. Feriencik, I. Richter *et al.*, The Tesat transportable adaptive optical ground station, in *Free-Space Laser Communication and Atmospheric Propagation XXVIII*, edited by H. Hemmati and D. M. Boroson (SPIE, San Francisco, California, 2016), Vol. 9739, pp. 37–47.
- [91] K. Saucke, F. Heine, D. Tröndle, P. M. Pimentel, E. Fischer, T. Berkefeld, M. Feriencik, I. Richter, M. Lutzer, and R. Meyer, The Tesat transportable adaptive optical ground station and the operational experiences, in *International Conference on Space Optics—ICSO 2016* (SPIE, 2017), Vol. 10562, pp. 1033–1056.
- [92] M. Toyoshima, Y. Takayama, T. Takahashi, K. Suzuki, S. Kimura, K. Takizawa, T. Kuri, W. Klaus, M. Toyoda, H. Kunitomori *et al.*, Ground-to-satellite laser communication experiments, *IEEE Aerosp. Electron. Syst. Mag.* **23**, 10 (2008).
- [93] J.-C. Richard, S. Poulenard, X. Gnata, L. Coret, T. Anfray, M. Crosnier, T. Marduel, L. Zurawski, S. Montigaud, F. Lacoste *et al.*, In-orbit testing of GEO feeder links with TELEO, in *International Conference on Space Optics—ICSO 2024* (SPIE, 2025), Vol. 13699, pp. 58–78.
- [94] M. Lucamarini, J. F. Dynes, B. Fröhlich, Z. Yuan, and A. J. Shields, Security bounds for efficient decoy-state quantum key distribution, *IEEE J. Sel. Top. Quantum Electron.* **21**, 197 (2015).
- [95] H.-L. Yin, M.-G. Zhou, J. Gu, Y.-M. Xie, Y.-S. Lu, and Z.-B. Chen, Tight security bounds for decoy-state quantum key distribution, *Sci. Rep.* **10**, 14312 (2020).
- [96] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, *Phys. Rev. A* **89**, 022307 (2014).
- [97] C. J. Clopper and E. S. Pearson, The use of confidence or fiducial limits illustrated in the case of the binomial, *Biometrika* **26**, 404 (1934).