

Finite-Resource Performance of Small-Satellite-Based Quantum-Key-Distribution Missions

Tanvirul Islam^{1,*}, Jasminder S. Sidhu^{2,†}, Brendon L. Higgins^{3,‡},
Thomas Brougham², Tom Vergoossen⁴, Daniel K.L. Oi², Thomas Jennewein³, and Alexander Ling^{1,5}

¹*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2,
Singapore 117543, Singapore*

²*Scottish Universities Physics Alliance (SUPA) Department of Physics, University of Strathclyde,
Glasgow G4 0NG, United Kingdom*

³*Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo,
Ontario N2L 3G1, Canada*

⁴*SpeQtral Pte. Ltd., 73 Science Park Drive Science Park 1, Singapore 118254, Singapore*

⁵*Department of Physics, National University of Singapore, Blk S12, 2 Science Drive 3, Singapore 117551,
Singapore*



(Received 1 July 2022; published 11 July 2024)

In satellite-based quantum-key-distribution (QKD), the number of secret bits that can be generated in a single satellite pass over the ground station is severely restricted by the pass duration and the free-space optical channel loss. High channel loss may decrease the signal-to-noise ratio due to background noise, reduce the number of generated raw key bits, and increase the quantum bit error rate (QBER), all of which have detrimental effects on the output secret key length. Under finite-size security analysis, a higher QBER increases the minimum raw key length necessary for nonzero secret-key-length extraction due to less efficient reconciliation and postprocessing overheads. We show that recent developments in finite-key analysis allow three different small-satellite-based QKD projects, CQT-Sat, the United Kingdom QUARC-ROKS, and QEYSSat, to produce secret keys even under conditions of very high loss, improving on estimates based on previous finite-key bounds. This suggests that satellites in low Earth orbit can satisfy finite-size security requirements but that this remains challenging for satellites further from Earth. We analyze the performance of each mission to provide an informed route toward improving the performance of small-satellite QKD missions. We highlight the short- and long-term perspectives on the challenges and potential future developments in small-satellite-based QKD and quantum networks. In particular, we discuss some of the experimental and theoretical bottlenecks and the improvements necessary to achieve QKD and wider quantum networking capabilities in daylight and at different altitudes.

DOI: [10.1103/PRXQuantum.5.030101](https://doi.org/10.1103/PRXQuantum.5.030101)

I. INTRODUCTION

The emergence of terrestrial quantum networks in large metropolitan areas demonstrates an increasing maturity of quantum technologies. A networked infrastructure enables increased capabilities for distributed applications in delegated quantum computing [1,2], quantum communications

[3,4], and quantum sensing [5]. However, extending these applications over global scales is currently not possible owing to exponential losses in optical fibers. Space-based segments provide a practical route to overcome this and realize global quantum networking [6–8]. Satellite-based quantum-key-distribution (SatQKD) has become a precursor to long-range applications of general quantum communication [9,10]. Although a general-purpose quantum network [11] will require substantial advancements in quantum memories and routing techniques, a satellite-based QKD system adds to the progress of global-scale quantum networks by driving the maturation of space-based long-distance quantum links.

There has been growing interest in SatQKD. The recent milestone achievements by the Micius satellite [12,13], which has demonstrated space-to-ground QKD and entanglement distribution, have energized this interest.

*Contact author: cqmtti@nus.edu.sg

†Contact author: jsmrdsidhu@gmail.com

‡Contact author: brendon.higgins@uwaterloo.ca

§These authors contributed equally to this work.

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.

Micius, being a relatively large satellite, leaves open the exploration into using smaller satellites to perform satellite-based QKD. Toward this goal, a small payload experiment has been designed for operation on the large Tiangong space station [14], providing an initial stepping stone. There have also been feasibility studies for small-satellite-based QKD and CubeSat-based pathfinder missions [15] for QKD applications. Several small-satellite-based QKD and quantum communication missions are under active development in China [16,17], India [18], Europe [19], Singapore [20], and the United Kingdom [21], which are likely to lead to a succession of imminent launches [9,13,17].

The recent surge in efforts emphasizes the importance of understanding specific limitations to the performance of different SatQKD systems. For low-Earth-orbit (LEO) satellites, a particular challenge is the limited time window in which to establish and maintain a quantum channel with an optical ground station (OGS). This limitation disproportionately constrains the volume of secure keys that can be generated due to a pronounced impact of statistical fluctuations in estimated parameters [22,23].

In this work, we give a scientific perspective on the progress of small-satellite-based QKD under resource constraints. More specifically, we analyze three different mission configurations: the Singapore Centre for Quantum Technologies CQT-Sat, the United Kingdom (UK) Quantum Research CubeSat–Responsive Operations for Key Services (QUARC-ROKS) satellite, and the Canadian Quantum Encryption and Science Satellite (QEYSSat), on which we are actively participating. In addition, these three missions are representative of near-term small-satellite-based QKD missions.

The quantum channel configuration for each mission is illustrated in Fig. 1. With the exception of a down-link entanglement-based channel, these configurations cover up link and down link with entanglement-based and prepare-and-measure-based QKD. These configurations give representative quantum channels to support the capability of a range of distributed applications. Depending on the ground-station location and the specific LEO orbit, a satellite may have a limited number of passes over the OGS for which QKD key generation is possible—e.g., current technology requires that passes are conducted during nighttime. Therefore, it is important to understand the conditions that allow a SatQKD system to produce secret keys successfully from a single pass over the OGS. More specifically, *for any given satellite overpass, how many secret key bits can be generated?* We answer this for the three mission configurations by revisiting the supporting theory and modeling of key generation [24–28]. It is shown that all three missions demonstrate enhanced key generation with the latest advancements in finite-key analysis. We conclude by looking at the prospects for satellites at higher altitudes, where the longer access time for a ground receiver does not overcome the increased diffraction loss.

Based on the performance analysis of each of these missions, we provide an informed and forward-looking perspective for global quantum communications, with a specific outlook on the outstanding challenges for SatQKD and long-term perspectives. In particular, we explore how improved finite-key analyses can improve SatQKD performance and, more widely, how advances in hardware can support greater capabilities for networked quantum technologies. This perspective provides a view of the medium-

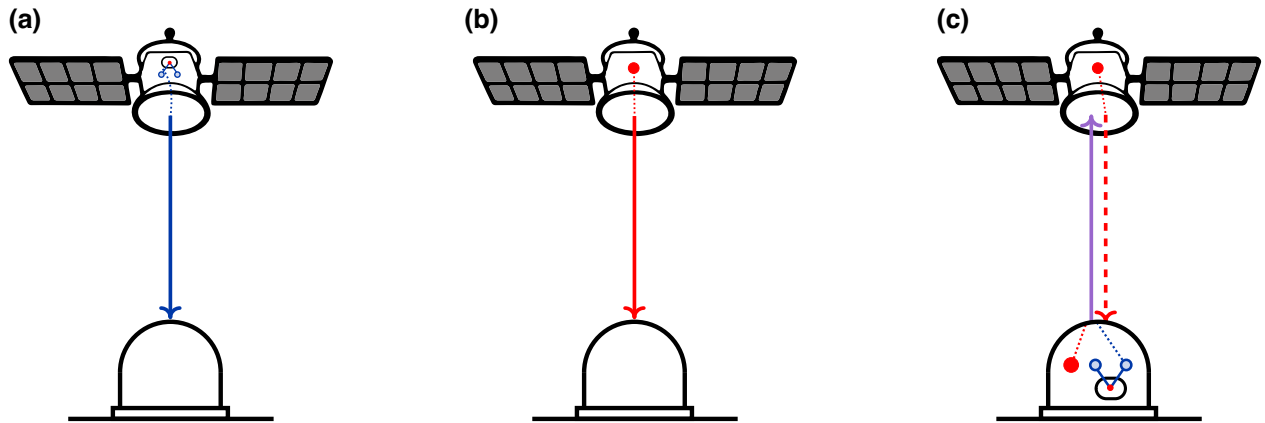


FIG. 1. The quantum channel configuration for three different SatQKD missions. Each mission implements a different combination of QKD protocols and quantum channel configurations between an OGS and an orbiting satellite. (a) The Singaporean CQT-Sat mission implements the entanglement-based BBM92 protocol (blue arrow) in a down-link configuration. For this mission, one of the photon pairs is measured on board and the other is transmitted to the OGS. (b) The UK QUARC-ROKS mission implements the weak-coherent-pulse (WCP) decoy-state BB84 protocol (red arrow) in a down-link configuration. (c) The Canadian QEYSSat mission implements both the decoy BB84 and BBM92 protocols (purple arrow) in an up-link configuration and intends to also incorporate a decoy BB84 down link.

TABLE I. The space-to-ground optical-link parameters for CQT-Sat. The M^2 parameter is the beam quality factor, which quantifies the variation of the beam from an ideal Gaussian beam.

Parameter	Value	Description
Transmitter aperture	0.09 m	Realistic aperture size for nanosatellite
Receiver aperture	0.6 m	Optimum aperture
Beam quality	$1.6 M^2$	Fundamental limit is 1.4 due to diffraction
Pointing jitter	$5 \mu\text{rad}$	$1.2 \mu\text{rad}$ demonstrated on Micius satellite
Efficiency	50%	Estimated based on reflectivity and number of optical surfaces
Background counts	1300 counts/s	Measured with respective setup in Singapore

to long-term challenges and milestones that present building blocks for enabling the quantum Internet.

II. SATELLITE-TO-GROUND ENTANGLEMENT-BASED QKD USING BBM92

CQT-Sat is a concept for a 12U nanosatellite capable of performing space-to-ground entanglement-based QKD, where U denotes a single cubic unit with dimensions $10 \times 10 \times 10$ cm. Its precursor, SpooQy-1, has demonstrated [15] the successful launch and operation of a miniaturized polarization-entangled photon-pair source in LEO. The subsequent instruments will build upon this to perform space-to-ground entanglement distribution and demonstrate entanglement-based BBM92 [29] QKD.

During the overpass of a satellite over the ground station, the link loss for the down-link quantum channel will depend on the relative distance between the satellite and the OGS. Using a variable attenuator, a tabletop setup can emulate a time-varying satellite-to-ground link loss (a similar experiment has been conducted previously in the context of QEYSSat [30]). This enables us to produce an estimation of the achievable raw key length and the overall QBER for various satellite passes. Using these parameters, we perform finite-key analysis and show that CQT-Sat can successfully generate shared secret keys between the satellite and OGS when the maximum elevation is as low as 33° .

A. System configuration

The satellite quantum source generates polarization-entangled photon pairs by superposing orthogonally polarized photons created from spontaneous parametric down-conversion using two pump-decay paths [31]. The detailed design of a functional model of the source and associated design trade-offs can be found in Ref. [32]. The source generates pairs of polarization-entangled photons, where each pair consists of a 785-nm-wavelength signal photon and an 837-nm-wavelength idler photon. For the purpose of QKD, each of the idler photons is measured aboard the satellite in either the computational or the diagonal basis with probability $1/2$. The signal photon is sent to the optical terminal of the satellite using an optical interface. A subsystem inside the optical source also generates

a synchronization beacon. Both the beacon and the signal photons are transmitted to the OGS through the optical terminal of the satellite.

Optical terminals on both the satellite and in the ground station help establish a space-to-ground free-space optical link. The terminals consist of optical telescopes and fine-pointing mechanisms for transmitting and collecting the signal photons, and synchronization and tracking beacons. Table I presents the parameters of the quantum source and the optical link.

B. Emulating space-to-ground QKD using a tabletop setup

To emulate a space-to-ground QKD link, we have built the entanglement source and the detection apparatus representative of both the satellite and ground systems, respectively. The system parameters for this setup are listed in Table II.

We consider a Sun-synchronous LEO with 500-km altitude above sea level. This orbit choice provides us with daily passes over the CQT ground station at a prespecified time of the day [33]. We compute a time series of the angular elevation of the satellite with respect to the OGS and the loss at that elevation for a pass using a simulation model that we have developed [32,34]. Regarding the simulation details, we compute the satellite range with respect to the OGS using the orbital simulation model and use parameters from Table II to compute the link loss at every point of the satellite pass. A satellite may pass over a ground

TABLE II. The source and detector parameters for CQT-Sat.

System parameter	Value
Entangled pair-production rate	20 Mcounts/s
Source intrinsic QBER	0.91%
Signal wavelength	785 nm
Idler wavelength	837 nm
Bandwidth	5 nm
Detection efficiency	25%
Dark-count rate per detector	500 counts/s
Detector dead time	50 ns
Detection jitter	320 ps
Detector after-pulsing probability	5%

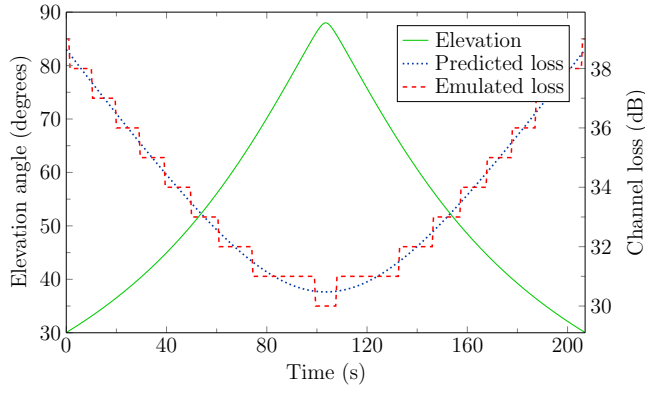


FIG. 2. An example simulated satellite pass reaching 88° elevation angle (green line). The experimental data are assembled such that their loss profile (red line) closely matches the theoretically predicted optical loss (blue line).

station with different maximum elevations. We simulate overpasses with a maximum elevation ranging from 30° to 90° . For example, in Fig. 2, we show a pass with 88° maximal elevation and the associated loss that the optical link experiences.

Using a variable attenuator, we introduce different losses and record detection time stamps for both signal and idler photons. Due to physical limitations, we only use a finite number of attenuator settings and stitch the experimental data together to emulate the predicted loss of the optical down link. To achieve this, we compute the link loss using our link model [34] for every second of a satellite pass over the OGS. In Fig. 2, this is labeled as “Predicted loss.” The staircase-shaped “Emulated loss” curve is then computed to closely approximate the “Predicted loss” curve using a small number of attenuation settings. This determines a finite number of attenuator settings at finite number of time steps. Using the tabletop QKD setup, the experiment is run under each of these loss settings for the time duration determined by the “Emulated loss” curve. Finally, the collected data are concatenated to approximately emulate a satellite-to-ground BBM92 QKD protocol.

This technique enables an investigation of satellite overpasses with different maximum elevations and allows us to generate the associated detection time stamps both on board the satellite and in the OGS. These time-stamp sets are processed through the rest of the QKD protocol stack including finite-key analysis to compute the secure key length achievable from each pass. A recent demonstration of a QKD system with a similar emulated satellite overpass has been capable of establishing a 4.58-Mb secure key between two nodes [35].

C. Key length of CQT-Sat for various LEO satellite passes

Depending on the geographical location and satellite orbit, a ground receiver might observe between two and

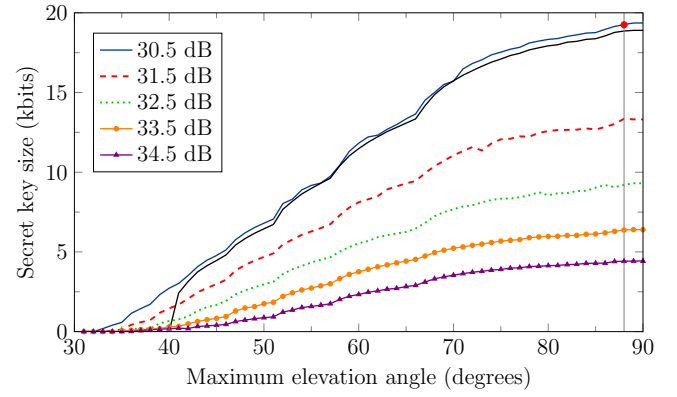


FIG. 3. The secret key lengths achievable by CQT-Sat for passes of given maximal elevations. The blue curve gives results for the default simulation setting, where the minimum loss at zenith is 30.5 dB. The other curves show the behavior for optical links with additional (1–4)-dB losses. All lines without markers are based on laboratory-based experimental data constructed to emulate pass-loss profiles. The results corresponding to the curves with markers contain loss profiles that are simulated numerically. The red marker on the blue curve corresponds to the simulation depicted in Fig. 2, where the satellite pass has maximum elevation 88° . The black curve, corresponding to the default simulation setting (30.5 dB at Zenith), shows the secret key size achieved using an older finite-key analysis [36] technique.

six satellite passes each day. An ideal satellite pass would transit directly over the ground station with a maximal elevation of 90° (zenith). At zenith, the satellite is closest to the OGS and in clear weather this pass would exhibit the lowest transmission loss and the longest link time. However, such a pass is less likely than more “glancing” passes. For a given detector dark-count rate, higher losses would result in a poorer signal-to-noise ratio and increase the QBER. Moreover, the pass duration and the number of photons successfully received from the satellite would also decrease. In Fig. 3, we show how the secret key length changes with different satellite passes. Here, we use the finite-key analysis from Ref. [28], taking the security parameter 10^{-10} , where the error-correction efficiency is 1.18.

The analysis shows that no secret key is generated for passes with a maximum elevation below 33° . This is acceptable for CQT-Sat, which was designed to avoid operation at low elevation. In this case, the ground receiver is sited at sea level in a tropical urban environment and the optical channel below 30° elevation suffers more loss and light pollution due to the thicker atmospheric column. Recent improvements [28] in finite-key analysis for smaller block lengths are especially important to achieve a positive secret key for low-elevation passes. For comparison, in Fig. 3 (black curve), we illustrate the secret key lengths achieved using an older finite-key-analysis technique from Ref. [36]. Note that using this older security

analysis for CQT-Sat, secret keys can only be achieved for overpasses with a maximum elevation above 40° , which is significantly worse compared to the 33° for the latest analysis. This improvement in extracting secret key from small raw key blocks results from a general theoretical improvement in the newer analysis. Therefore, in the remaining mission analyses in this work, we only use the newer finite-key-analysis technique [28].

III. SATELLITE-TO-GROUND QKD USING DECOY-STATE BB84

The UK Quantum Research CubeSat (QUARC) project provides a design and architectural foundation for the Responsive Operations for Key Services (ROKS) mission in the National Space Innovation Programme (NSIP) [37,38]. ROKS uses a continuation of the same 6U CubeSat platform as QUARC and will first implement the decoy-state BB84 protocol in a down-link configuration for QKD service provision using a weak-coherent-pulse (WCP) source (Fig. 1).

The satellite quantum modeling and analysis (SatQuMA) open-source software has been developed to estimate the expected key-generation performance for such satellite QKD missions [39]. SatQuMA models the efficient BB84 WCP two-decoy (three-intensity) protocol and can optimize over the entire protocol parameter space and transmission segment time. It also incorporates recent results in finite-block composable secure-key-length estimation [28,40,41]. SatQuMA can be applied to model the expected key-generation performance for ROKS for a general satellite-pass geometry in a Sun-synchronous orbit (SSO) at altitude h .

A. System configuration

We use published empirical Micius-mission measurements of the total optical loss of the SatQKD channel [42] to construct a representative total-system link efficiency as a function of the elevation angle during a satellite pass. To account for local horizon constraints around the OGS, we restrict quantum transmissions to elevations above 10° .

The link efficiency (loss) is highly dependent on the system parameters, OGS conditions, and orbits. The nominal system parameters are summarized in Table III, where the minimum total system loss at zenith is computed to be 34 dB. One can scale the minimum system loss at zenith to allow the comparison of differently performing SatQKD systems. Changes to the minimum system loss at zenith would then account for differences in the transmit and receive aperture sizes, pointing accuracy, atmospheric absorption, turbulence, receiver internal losses, and detector efficiencies. For the current simulations, we consider a nominal baseline value of 34 dB. SatQKD missions with differing performance can be modeled by linearly scaling

TABLE III. The reference system parameters for the QUARC-ROKS mission. We take published information of the Micius satellite and OGS system as representing an empirically derived set point for our finite-key analysis. The total loss at zenith can be linearly scaled to model other systems with smaller OGSs or differing source rates.

Parameter	Value	Description
Intrinsic error	0.5%	Source errors
After-pulsing	0.1%	Probability of p_{ap}
Extraneous count rate	5×10^{-7}	Probability of counts from background light
Source rate	100 MHz	Signal frequency
Error correction	10^{-15}	Error-correction efficiency
Security	10^{-10}	Security parameter
Altitude	500 km	Altitude of satellite orbit
System loss	34 dB	Loss at zenith

the link efficiency versus elevation curve to account for different constant-efficiency factors, such as a change in OGS receiver area.

To evaluate the sensitivity of the achievable secret key length to different errors, we categorize different contributions associated with sources and detectors in two key parameters. First, errors from dark counts and background light are combined together into a single extraneous count probability p_{ec} , here assumed to be constant and independent of elevation. In practice, it will depend strongly on the environment of the OGS and the light from celestial bodies. Second, all other error terms, such as misalignment, source quality, and imperfect detection, are combined into an intrinsic quantum bit error rate, $QBER_i$, independent of channel loss and/or elevation. This allows for an efficient method with which to determine the sensitivity of the secret key length to different categories of errors, which helps to identify targeted improvements for future SatQKD missions.

B. Optimized finite-key length

We model the efficient BB84 protocol, adopting the convention of key generation using signals encoded in the X basis and parameter estimation using signals in the Z basis, chosen with biased probabilities. For a two-decoy-state WCP BB84 protocol, one of three intensities μ_j for $j \in \{1, 2, 3\}$ are transmitted with probabilities p_j . An expression for the final finite-key length, ℓ , for this protocol is given in Ref. [24]. The key is extracted from data for the whole pass as a single block without partitioning and the security proof of Ref. [24] makes no assumptions about the underlying statistics. This avoids having to combine small data blocks with similar statistics from different passes—thus, it is both quicker and avoids the need to track

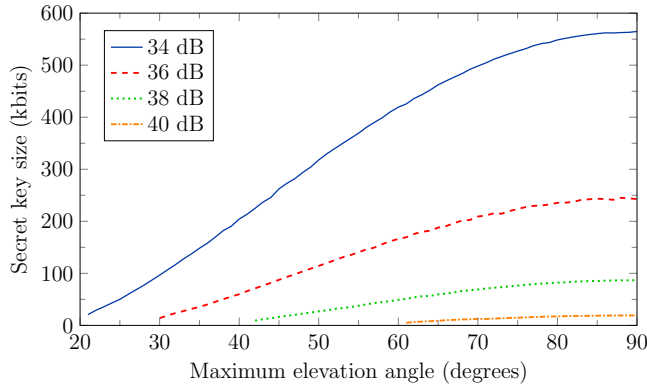


FIG. 4. The estimated secret key length generated by QUARC mission for passes with different maximum elevation angles. In the default simulation, the minimum total system loss is 34 dB. Other curves show behavior for optical links with additional 2-, 4-, and 6-dB losses.

and store a combinatorially large number of link segments until each has attained a sufficiently large block size for asymptotic key extraction.

The limited data sizes from restricted pass times result in key-length corrections to account for the finite statistics of the link. To improve the analysis, we use the tight multiplicative Chernoff bound [27] and improve the estimate of error-correction leakage $\lambda_{EC} \leq \log |\mathcal{M}|$, where $\mathcal{M}$ characterizes the set of error syndromes for reconciliation [25] (for more details, see Ref. [40]).

For a defined SatQKD system, we optimize the finite-key length ℓ by optimizing over the protocol parameter space that includes the source intensities (with $\mu_3 = 0$) and their probabilities and the basis-encoding probability p_X . We also optimize the portion of the pass data used for key generation.

The SatQuMA code is used to generate simulated measurement data. The QBER and phase errors for the key bits are estimated using only the data from the complementary basis. This is a classic sampling-without-replacement problem, which is usually solved in QKD using an approximation for the hypergeometric distribution [43]. Recently, however, an improved sampling bound has been proposed [28]. This can be used to estimate the QBER and phase error. The formalism from Ref. [28] is used together with data generated from SatQuMA to determine the secret key length for different satellite passes, which we characterize through the maximum elevation angle. The secret key is plotted in Fig. 4 as a function of the maximum elevation angle of a pass.

IV. SatQKD USING BBM92 IN UP-LINK OR DOWN-LINK CONFIGURATIONS

The Quantum Encryption and Science Satellite (QEYSSat) mission [44] is a Canadian initiative to develop

and launch a microsatellite-hosted quantum receiver instrument into LEO. The primary objective of the mission is to demonstrate QKD via quantum up link from sources located at two or more ground stations. To support this, the QEYSSat instrument will possess a large front-end telescope for light collection, polarization-discriminating optics, and single-photon avalanche diodes [45]. Support for a WCP down-link protocol is also being developed. QEYSSat is currently in the late design and early construction phase and on schedule to launch in 2025.

A. System configuration

With the nominal configuration of QEYSSat being an up link and the quantum sources being located on the ground, lower secure key rates are expected when compared to a down link with equivalent parameters. This is due to the steering effect of atmospheric turbulence on the beam at the beginning of its propagation, in contrast to atmospheric steering at the end of propagation for a down-link channel. However, a satellite receiver affords considerably greater source flexibility. For this reason, two source types are baselined: WCP with decoy states in an unbiased BB84 protocol and entangled photons (with one photon of each pair kept at the ground) in a BBM92 protocol. It is expected that other quantum source types—e.g., quantum dots (see, e.g., Ref. [46])—will also be employed during the experimental phase of the QEYSSat mission.

Commencement of the QEYSSat mission in 2018 was preceded by several theoretical and experimental investigations into the feasibility of the mission, both as a whole [47] and with a focus on critical subsystems, including pointing [48,49] and photon measurement [50,51]. Of these, one early work [52] numerically modeled the quantum optical link to establish the loss and fidelity of polarized-photon transmission under the assumptions of the expected orbital configuration and (generally conservative) atmospheric conditions. Multiple scenarios were considered, consisting of notional WCP or entangled-photon sources in both up-link and down-link configurations. Although some details of the in-development QEYSSat apparatus and conditions have been refined since, the values remain generally very similar. In this work, we present the secret-key-generation performance of QEYSSat while executing the entanglement-based BBM92 protocol in both satellite-to-ground (down-link) and ground-to-satellite (up-link) quantum communication configuration modes. Although the QEYSSat instrument has ultimately been designed without an entanglement down link, we include its analysis here for two reasons: (1) for comparison with the up-link configuration that is planned and (2) as an extension of the prior feasibility study performed in Ref. [52]. We expect that these updated results may influence future designs.

TABLE IV. The ground-to-space optical-link parameters for the model representing QEYSSat.

Parameter	Value
Orbital altitude	600 km
Transmitter aperture	0.5 m
Receiver aperture	0.3 m
Pointing error	2 μ rad
Optics losses	3 dB
Quantum transmission wavelength	785 nm
Detector loss	2.3 dB
Spectral-filtering bandwidth	1 nm
Dark-count rate per detector	20 counts/s
EPS pair-production rate	100 Mcounts/s
Source intrinsic QBER	1%
Coincidence window	0.5 ns

B. Key-length analysis

In this section, we calculate the secure key rate for the QEYSSat Mission using updated secure-key-length analysis [28], which has improved performance with smaller raw key block size. Performance with smaller block size is important because it has implications on QKD feasibility under high-loss conditions and during low maximum-elevation passes. This improved key-length analysis enables higher key rates than prior analysis [52].

In this analysis, we set the error-correction efficiency to 1.18 and the security parameter to 10^{-10} , which is consistent with the values taken for the CQT-Sat and QUARC-ROKS missions. Table IV summarizes the parameters that describe the quantum source and the optical link. The assumed satellite orbit (Sun-synchronous noon and midnight at 600-km altitude) was simulated for nighttime passes for a duration of a year over a notional ground station located 20 km outside of Ottawa, Canada. The optical-link conditions for each pass were modeled at 10-s intervals. The background light was determined from the Operational Linescan System measurements of the Defense Meteorological Satellite Program [52–54] and combined with an assumed half-moon at 45° (contributing via Earth reflection using its mean albedo) along with Earth’s thermal (black-body) radiation, taking into account the geometry of the optical field of view, which changes over the pass of the satellite, and 1-nm-bandwidth spectral filtering. Detector dark counts of an additional 20 counts/s were also included in the total noise detected.

Here, we consider a transmitter and receiver diameter of 50 cm and 30 cm, respectively, as the baseline configuration. Optical losses have been calculated from the contributions of numerically modeled diffraction given a central obstruction (secondary mirror), an assumed mean pointing error of 2 μ rad, atmospheric attenuation modeled by the MODTRAN 5 software package [55] for a “rural” profile with 5-km visibility, and the Hufnagel-Valley model of atmospheric turbulence at sea level. The photonic states

have been simulated in a seven-dimensional Fock space (between zero and six photons). The choice of this cut-off dimension draws heritage from earlier work [52] and enables efficient simulation of the protocol. Further, since each pulse has a mean photon number of around 0.5, the Fock-space amplitudes quickly become negligible after a few photons, with the total probability for a pulse to have seven or more photons being less than 10^{-6} . Finally, intrinsic reduction in quantum visibility has been included via an operation equivalent to a small rotation.

The detector count-rate statistics have been calculated using an assumed EPS pair-production rate of 100 Mpairs/s via spontaneous parametric down-conversion (SPDC) pumped at $\epsilon = 0.22$ (corresponding to a mean 0.1 pairs per pulse—see Ref. [52]) with 98% intrinsic entanglement visibility and a 0.5-ns coincidence window. Such a source is challenging but possible with current techniques on the ground (for up link) and can be reasonably foreseen as achievable with expected advances for space platforms (for down link). Intervals in which the simulated measurement visibility was below 85% have been filtered out (see Ref. [56]). In this analysis, we have aggregated the remaining statistics at each pass and sorted these by the maximum elevation achieved by the satellite with respect to the ground station for that pass.

In Figs. 5(a) and 5(b), we show the secret key generated for passes with different maximum elevations in the down-link and up-link configurations, respectively, for entanglement-based BBM92. We use the finite-key analysis from Ref. [28], with security parameter 10^{-10} and error-correction efficiency 1.18, to compute the secure key lengths. Note that in comparison with the analysis done in Ref. [52], the secret key size is considerably greater—we expect that this is largely a consequence of the faster source rate and assumed enhancements to intrinsic QBER and pointing accuracy, coupled with the highly nonlinear effect of finite-size statistical analysis.

V. MISSION COMPARISONS

As the three SatQKD missions discussed here have different design specifications for the ground stations, satellites, and protocols implemented, a direct quantitative performance comparison of the missions is difficult. Despite this, we provide a qualitative discussion on the respective strengths and weaknesses of each mission. First, the up-link configuration employed by QEYSSat has the advantage that it relieves the source design from the strict size, weight, and power (SWaP) constraint imposed by a satellite. Moreover, it potentially allows QEYSSat to swap the entanglement source to a prepare-and-measure source at any point of the mission to perform a different SatQKD protocol and could benefit from abstract beam pointing. However, it has a disadvantage in that the optical link suffers larger environmental turbulence during the initial

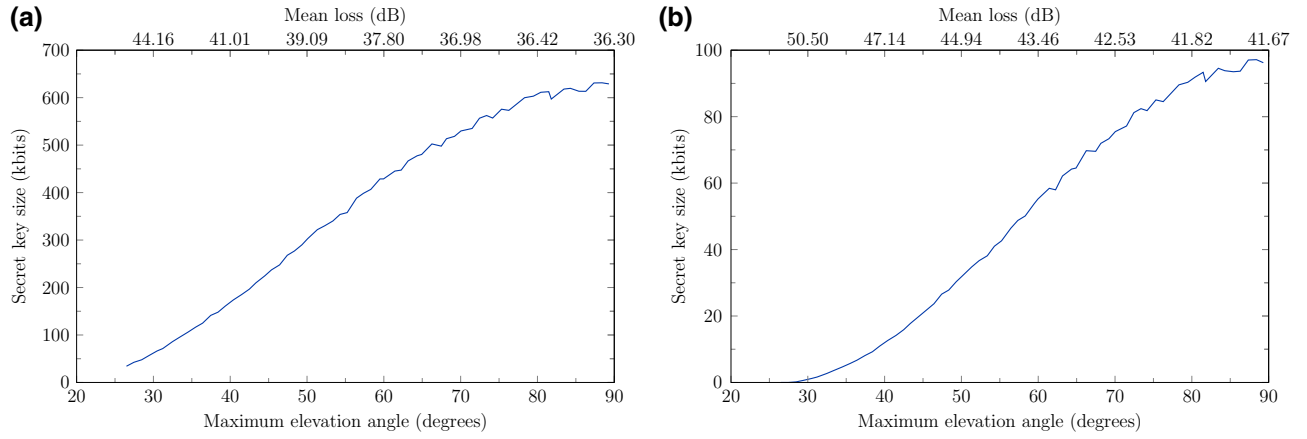


FIG. 5. The expected performance under modeled conditions representative of a QEYSSat-style mission performing entanglement-based (BBM92) QKD in (a) satellite-to-ground down-link configuration and (b) ground-to-satellite up-link configuration. Note that the QEYSSat mission baseline does not include entangled down links.

part of the optical path, generating higher beam wandering compared to a down-link configuration.

The QUARC-ROKS mission uses a prepare-and-measure decoy state BB84 protocol where the source emits a periodic signal. This allows higher repetition rates to achieve larger raw key rates to counter the loss experienced in the satellite-to-ground optical link. In addition to a higher performance requirement for the detection and time-stamping circuits, the repetition rate is also constrained by the speed of quantum random number generation for the choice of quantum signal transmission. A similar attempt to counter the link loss by increasing the brightness of an entanglement source quickly hits a bottleneck because the SPDC-based source does not produce periodic signals; therefore, due to the finite resolution of time-stamping devices and the limits imposed by detector jitters, the source ends up producing too many multiphoton events per time slot, increasing the QBER to an unacceptable value. However, entanglement-based QKD implementations act as precursors to entanglement-sharing links, which are essential for future development toward a general-purpose quantum Internet.

The three SatQKD missions discussed here use silicon-based Geiger-mode avalanche photodiodes as single-photon detectors [32,38,47]. The performance of these photodiodes, together with other optoelectronic components on the QKD system, may degrade due to exposure to high-energy particles and radiation in outer space, causing increased dark counts, detection jitter, and decreased detection efficiency [57–60]. Therefore, space irradiation directly affects the performance of the overall SatQKD system. Fortunately for these LEO-based SatQKD missions, the impact of solar or cosmic radiation is significantly lower than that experienced at medium Earth orbits or geostationary orbits due to protection from Earth’s magnetic field [61]. In addition, space radiation inflicts cumulative

damage on detection systems. Since small-satellite missions operating in LEO can only stay in orbit up to a maximum of 2 years without active orbital boosting, the cumulative damage remains minimal and does not significantly affect the QKD performance. The effects on detection systems have been extensively studied using laboratory-based radiation tests [58,60] and data from the completed SpooQy-1 mission, which is a precursor to the CQT-Sat. Finally, in Figs. 3 and 4, we illustrate that SatQKD is tolerant to additional loss of arbitrary origin, which may stem from reduced detector performance owing to radiation damage.

VI. OUTLOOK FOR GLOBAL QUANTUM COMMUNICATIONS

We have compared three upcoming SatQKD missions in the preceding sections and shown that an individual small satellite can satisfy finite-key requirements for SatQKD. For each of the three missions considered, we have shown that this leads to nonzero finite keys generated for a single overpass. While an individual satellite in an appropriately chosen orbit can cover the Earth’s surface each day, increased performance in the network will probably require constellations of these satellites [34]. Aside from putting more satellites into space, it is important to consider how the performance of each individual satellite could be enhanced. We note from the preceding sections that LEO satellites operate at the edge of performance in terms of SatQKD that satisfy finite-key security. In this section, we report on specific challenges that, if overcome, can provide improved SatQKD performance over a wider range of operations. We also provide a long-term perspective on the demonstration of key milestones toward global quantum communications [62] and applications beyond QKD.

A. Outstanding challenges for SatQKD

Progress in finite-key security analyses presents an immediate and fundamental challenge to improving the achievable key rates. An improved finite-key analysis handles parameter estimation and postprocessing tasks more efficiently. This would enable higher finite keys and successful distillation of nonzero finite keys at higher operating losses (e.g., lower-elevation passes or at ground locations with worse atmospheres) without any hardware changes. Beyond improvements in finite-key analysis, there are specific challenges to hardware that would provide improved performance.

A conventional research program would revolve around improved transmitters and detectors. We propose that building a system that can operate effectively in daylight would be a major step. There has been significant progress [63,64] in terrestrial free-space daylight QKD and optical detection systems [65]. However, due to limited operating margins in a satellite-to-ground quantum link, further development would be necessary before daylight SatQKD could be realized. In practice, every SatQKD mission for the foreseeable future will operate during nighttime to avoid excess background light from the Sun. In order to operate during daylight, the spectral window of the transmitted light has to be sufficiently narrow for effective filtering, while the transmission system has to be built to avoid reflecting sunlight directly into the receiver.

We note that adaptive optics (AO) for an optical ground receiver [66–68], to effectively couple light into a single-mode fiber for direct transmission of the QKD signal to end users located away from the ground receiver will also become increasingly important. This has the added advantage that an AO system will act as a spatial filter, reducing the amount of stray light entering the quantum channel. To be useful, the AO system will need to be able to operate with high coupling efficiency, so that the overall system throughput is not compromised. A ground AO system can also improve up-link configurations [69]. Research into transmission and detection systems that can penetrate cloud and fog would also be highly desirable.

Aside from the transmitter and detector aspects, we note that a major contribution to transmission loss is the diffraction of the beam from the transmitter. This loss could be mitigated using several different approaches. The first is to operate the spacecraft at very low Earth orbit (VLEO). This orbit has a nominal altitude below that of the International Space Station (approximately 400 km) and is often not considered due to satellites experiencing significant drag and reentry into the Earth’s atmosphere within a year. However, with space propulsion systems being developed for station keeping [70,71], this approach may become feasible and would afford significantly lower losses owing to shorter optical links. In designing a VLEO system,

TABLE V. The space-to-ground optical-link parameters used for modeling higher-altitude orbits.

Parameter	Value
Beam-waist-to-aperture ratio	0.89
Satellite-transmitter aperture	0.1 m
Pointing error	2.5 μ rad
Ground-receiver aperture	0.6 m
Wavelength	785 nm

factors such as microbuffeting from the residual atmosphere, degradation from atomic oxygen, and the shorter overhead time of the satellite remain open challenges.

The second is the use of enhanced transmit-receive apertures. The use of larger apertures has been the primary route to minimize link loss, with a doubling in aperture sizes providing 6-dB improvements [40]. However, aperture sizes are restricted for small satellites. Recent efforts rely on deployable and active optics [72,73].

Finally, diffraction losses can also be mitigated by developing larger and more capable satellites at very high altitudes. The advantage is that such satellites can be equipped with large transmit apertures while increasing the ground coverage area as well as improving access time for a ground receiver. The drawback is a dramatic increase in diffraction loss that must be compensated by enlarging the transmit-receive aperture and improving pointing accuracy.

We have modeled the performance of SatQKD systems for varying orbital altitudes, by imposing similar capabilities on the satellites for LEO, medium Earth orbit (MEO) [74], and geostationary orbit (GEO) [75]. Under a

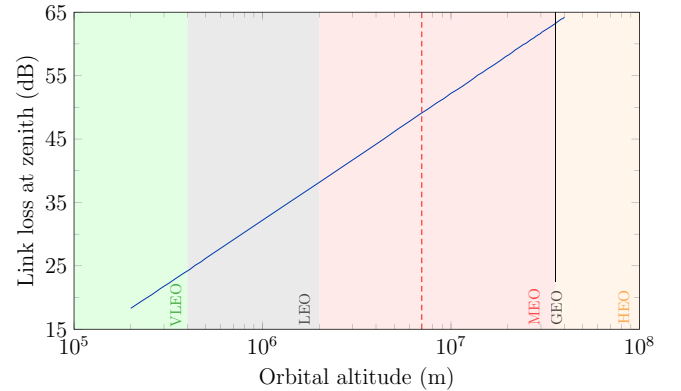


FIG. 6. The link loss as a function of the orbital altitude using parameters from Table V. The green shaded region indicates the altitude range for VLEO orbits, with gray for LEO orbits, red for MEO orbits, orange for HEO, and the solid black line for a GEO orbit. The red dashed line corresponds to a representative MEO altitude of 7×10^3 km that we consider later. The link loss at zenith rapidly increases with increasing orbital altitudes.

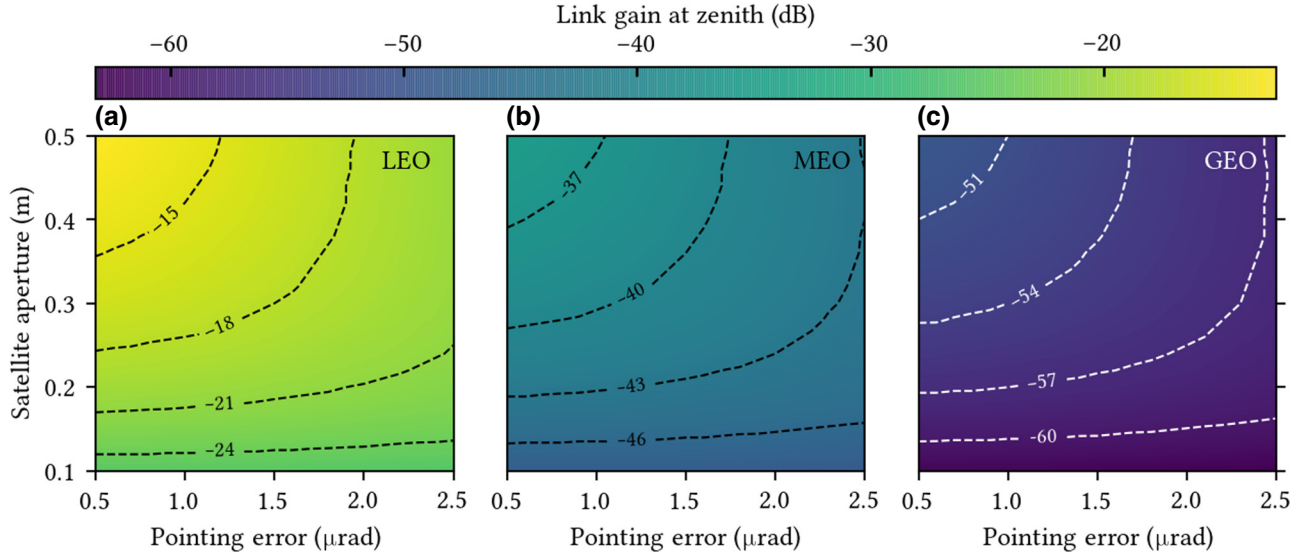


FIG. 7. The trade-off between the telescope aperture on board the satellite and the pointing error with respect to the link gain at zenith. (a) The trade-off for a representative LEO at an altitude of 500 km. (b) The trade-off for a representative MEO at an altitude of 7000 km. (c) The trade-off for GEO.

down-link configuration using the receiver (ground-based) and sender (on-board-satellite) telescope and beam parameters as shown in Table V, we study the space-to-ground optical-link loss (Fig. 6) for higher-altitude orbits. We see that the optical-link loss increases rapidly with the increase in altitude, as expected from the beam expansion. One approach to counter increased losses at higher orbits and ensure successful operation of SatQKD is to use ultra-bright sources capable of operating at gigahertz-bandwidth repetition rates [76]. SatQKD missions typically operate with a source rate in the order of 10^8 Hz. Increasing the source rate to the gigahertz range and beyond requires low timing jitters that are on the subnanosecond scale. This is possible with superconducting-nanowire single-photon detectors (SNSPDs) [77], at the expense of greater SWaP due to the requirement for cryogenic cooling. An alternative approach to compensating the increased loss at higher orbits is to increase parameters such as the sending or receiving telescope apertures and pointing accuracy. In Fig. 7, we show a trade-off heat map on which the aperture and pointing accuracy of the satellite transmitter telescopes are varied to show how they affect the transmission for a satellite in LEO, MEO, and GEO. These trade-off calculations show that for orbits higher than LEO, it is not sufficient to only change the parameter of the satellite to achieve the transmission gain necessary for successful SatQKD. For higher altitudes, one would also need to improve other parameters, such as the aperture, pointing accuracy, and detector performance of the ground telescope.

Due to increased losses at higher-altitude orbits, obtaining a secure key from a single pass over a ground station may not be possible in these cases. It is possible to

accumulate the raw key bits over multiple passes, increasing the block size to reduce finite-block-size effects sufficiently to achieve a secure key. In Fig. 8, we show block sizes and associated QBERs for the raw key bits accumulated over a year for entanglement-based SatQKD operated at various orbital altitudes for a single link. The drawback of key aggregation is that large amounts of data will have to be stored on board the satellite for a long time, which might introduce vulnerabilities due to storage security. In Fig. 8, we discard passes that yield QBER higher than 11%, which generates a key with minimal information known to an eavesdropper after postprocessing [78]. However, given the limited number of bits acquired at each pass, it might not be feasible to determine the QBER reliably by exchanging a subset of these bits between the satellite and the OGS.

Missions that choose to implement larger operating apertures to counter larger losses from higher-altitude orbits should also consider the increased costs associated with the optics and mass of the satellite. Specifically, the estimated cost variation for larger telescopes is $T_x^{1.7}$ [79], largely due to bulk optics and increased mass, making them considerably more expensive than smaller telescopes. Moreover, space-based telescopes are estimated to be 30 times more expensive than ground telescopes.

B. Long-term perspectives

In this section, we provide a perspective on medium- to long-term challenges and milestones that present a blueprint for enabling additional capabilities for the quantum Internet. These milestones relate to the implementation of different QKD protocols to extend the use cases

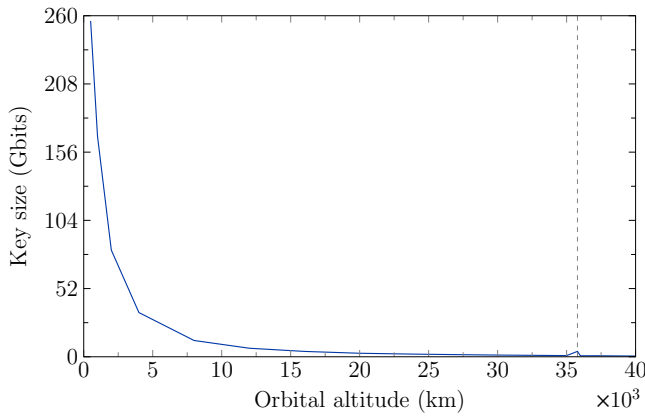


FIG. 8. The raw key length accumulated over a year as a function of the orbital altitude. The gray dashed vertical line indicates a GEO altitude, where the satellite remains stationary at the zenith, leading to a higher raw key and a lower QBER compared to other nearby orbits where the satellite has a varying angular elevation with respect to the OGS during an overpass. To model this, we assume a satellite telescope with aperture 0.5 m, an OGS telescope with aperture 1.8 m, and an entangled pair-production rate of 100 Mcounts/s.

of quantum communications and the development of improved hardware that could enable the demonstration of distributed quantum technologies beyond communications.

To extend the range of quantum communications, the horizon of efforts in developing SatQKD systems is likely to involve the improvement of instrument components such as the sources, detectors, classical communication systems, and optical systems. This would directly generate improved key rates and would enable the implementation of a number of additional QKD protocols.

First, the development of quantum memories will provide synchronization of probabilistic events to enable the implementation of memory-assisted (MA)-QKD protocols. Recent theoretical studies have shown that MA-QKD protocols can yield higher key rates over global distances and provide improved robustness against atmospheric weather and multiple-excitation effects [4,6,80]. The advantage is that MA QKD is less demanding on the performance of quantum memories than those required for probabilistic quantum repeaters. Demonstration of MA-QKD protocols can herald a major progress toward improved rate-versus-distance performance of SatQKD. Beyond communications, satellite-based quantum memories can enable distributed quantum sensing and imaging [81–83]. However, any distributed applications making use of quantum memories will require active tracking and compensation of Doppler shifts that arise from the rapid relative motion of satellites, which provides a further challenge. For example, the typical speed of an LEO satellite is 7800 ms^{-1} , which has a maximum fractional Doppler

shift (generally, elevation dependent) of $\beta = v/c = 2.6 \times 10^{-5}$. Compensating for this shift is important to enable the signal to efficiently couple with a narrow line width of the quantum memory. Compensation for Doppler shifts may also require interconversion between flying and static quantum systems.

Second, continuous-variable (CV) protocols operate with conventional telecommunication devices and homodyne measurements that can be implemented at room temperature. This improves integration with existing ground-based networks and circumvents the need for bulky systems to cryogenically cool single-photon detectors, which may be necessary to support the discrete variable (DV) protocols, including BB84 and BBM92, that have been our focus. Despite these advantages, CV QKD provides limited key rates at high-loss large distances that are typical in SatQKD, which explains their limited use in proposed SatQKD. There are studies that explore the feasibility of CV QKD over large distances [84,85]. In addition, CV QKD does not have the same maturity of proof techniques in the finite-key regime. This in particular leaves an open question about the security of finite keys and how keys can be more efficiently distilled for overpass data. Initial studies on this have provided an optimistic outlook [85] but further studies are required to establish the same maturity and rigor that DV-QKD protocols have. Particular challenges include determining the optimal approach to partition overpass data and finding analytic finite-key methods that do not rely on numerical approximations.

Third, if the polarization degree of freedom of a photon is used to encode a qubit in a SatQKD link (as is common), it becomes crucial that both the sender and the receiver have their reference frames well aligned, as misalignment results in quantum bit errors in the output [86]. The relative motion between the satellite and the ground station may introduce additional challenges in acquiring and maintaining a common reference frame during quantum communication. Several reference-frame-independent quantum communication protocols [87–92] have also been proposed to account for this.

Finally, time-bin encoding offers another way of encoding key bits in DV QKD [93]. In principle, time-bin encoding can allow more than one bit to be encoded on each photon [94,95]. The motivation for this approach is that increasing data rates would normally require an increase in the source repetition rate but this eventually reaches a practical limit due to detector dead time. Higher-dimensional encodings could circumvent this issue by allowing multiple bits to be encoded on each photon. Currently, such systems have only been demonstrated in laboratory settings [94]. Considerable work remains to develop setups that could be deployed in the challenging conditions of a satellite. Further, many of the QKD systems investigated to date use fiber, not free space. Only recently have there been

investigations into the effects of errors due to free-space transmission in such setups [96].

Phase-randomized weak coherent pulses have become the most well studied and implemented information carriers in satellite-based missions due to their maturity and ease of implementation [9]. However, recent progress in quantum source development provides access to alternative QKD sources. For example, true single-photon sources (SPSs) based on nitrogen-vacancy centers [97] and quantum dots [98] are being developed and may become suitable for small SatQKD applications in the near future. The use of SPSs would provide enhanced security given their inherent immunity to photon-number-splitting attacks and would also provide advantages in general-purpose quantum communications such as quantum repeaters [99], optical quantum memory [100], and on-demand entanglement generation [101].

Twin-field (TF) QKD has gained popularity in fiber-based application for its ability to mitigate the effect of transmission loss [102,103]. However, TF and measurement-device-independent (MDI)-QKD [104–106] are currently beyond the scope of small satellites, owing to the requirements for phase stabilization (as required in TF) and received quantum pulse synchronization (required in TF and MDI) being extremely challenging to implement, especially on a SWaP-constrained platform. A more general overview of different protocols and their challenges for satellite deployment can be seen in Ref. [9].

For applications beyond QKD, small satellites could benefit by using multiple independently steerable telescopes to distribute entanglement to multiple OGSs. This will help to minimize latency in distributed quantum technologies when multiple ground stations are in view. Although steering multiple telescopes on small satellites increases the mechanical complexity and mass of the instrument, possible disturbance to the alignment of optical systems could be mitigated with twin tethered nanosatellites. This naturally raises the possibility of formation flying of small-satellite clusters that can extend the range of applications. This would be particularly important for distributed quantum technologies.

A LEO satellite is inherently limited in the geographical area that it can cover at any one time. A satellite-based global quantum network will therefore need a constellation of satellites [34] that may involve small-satellite-based quantum communication between satellites [107] and other high-altitude flying platforms [108]. Along with the DV SatQKD systems described in this work, there are studies [109] investigating the feasibility of CV satellite-based QKD systems.

VII. CONCLUSIONS

There is growing interest in deploying satellites to enable a global QKD network. To ensure that this goal

remains feasible and to guide experimental and engineering efforts, it is crucial to understand how SatQKD can yield efficient secret key generation under finite transmission times and high-loss regimes. Previous works have shown that secret key generation with SatQKD is possible using finite-key analyses. Recent advancements in the treatment of finite-key effects have improved the efficiency of key extraction, which greatly decreases the requirements on the minimum raw key length necessary for key extraction.

We use these latest finite-key bounds in the performance analyses of three different LEO-based satellite-mission concepts; the 12U CQT-Sat mission implementing an entanglement-based BBM92 down link, the 6U QUARC project implementing a WCP decoy-state BB84 in down-link configuration, and the QEYSSat mission implementing both the decoy BB84 and BBM92 protocols in an up-link configuration, in addition to a decoy BB84 state down link. All three SatQKD missions achieve good secure key yields on the order of kilobits from a single pass over a ground receiver, even for the missions based on resource-constrained and aperture-limited CubeSats. This provides reassurance that planned SatQKD missions are on course to achieve important milestones that can lead to an effective global QKD network.

The long-term vision of a satellite-based global quantum network remains a principal motivation behind SatQKD. Therefore, developing the infrastructure for a global QKD network sets the stage for future theoretical, experimental, and engineering milestones. We list these milestones together with outstanding challenges in the field and discuss potential routes to overcome them. Prominent challenges discussed include the daylight operation of SatQKD, the cooperation of multiple OGSs with a constellation of satellites to improve the reliability of general applications beyond QKD services, and implementing SatQKD from different altitudes to enable longer-range communications and intersatellite links. We extend our discussion by modeling the performance of SatQKD systems with varying orbital altitudes and quantify system design trade-offs to offset the increased link losses at higher altitudes. While our calculations demonstrate that all three LEO SatQKD missions considered here have the ability to yield secure finite keys, it is clear that implementing SatQKD from higher altitudes require overcoming numerous hardware challenges and further improving security analyses simultaneously.

For applications beyond QKD, the most demanding technological challenge is to implement general-purpose quantum communications that have applications in distributed quantum technologies, such as quantum computing, error correction, and quantum sensing. This will require a constellation of satellites, each synchronized and equipped with entanglement sources and quantum memories to dynamically create multilink connections between

any two points on Earth. Our discussion on the short- and long-term perspectives of satellite-based quantum communications should help to build a blueprint for enabling the global quantum Internet.

ACKNOWLEDGMENTS

J.S.S., T.B., and D.K.L.O. acknowledge the support of the UK National Quantum Technologies Programme (NQTP) and the Quantum Technology Hub in Quantum Communications (Engineering and Physical Sciences Research Council (EPSRC) Grant No. EP/T001011/1). B.L.H. and T.J. acknowledge support from the Canadian Space Agency and thank J.-P. Bourgoin for discussions. T.I. and A.L. acknowledge support from the Research Centres of Excellence program supported by the National Research Foundation (NRF) Singapore and the Ministry of Education, Singapore. This work was supported by the EPSRC International Network in Space Quantum Technologies (Grant No. EP/W027011/1).

- [1] A. Yimsiriwattana and S. J. Lomonaco Jr., in *Quantum Information and Computation II*, edited by E. Donkor, A. R. Pirich, and H. E. Brandt (SPIE, Orlando, Florida, United States, 2004), Vol. 5436, p. 360.
- [2] R. Van Meter and S. J. Devitt, The path to scalable distributed quantum computing, *Computer* **49**, 31 (2016).
- [3] C. Liorni, H. Kampermann, and D. Bruß, Quantum repeaters in space, *New J. Phys.* **23**, 053021 (2021).
- [4] J. Wallnöfer, F. Hahn, M. Gündoğan, J. S. Sidhu, F. Krüger, N. Walk, J. Eisert, and J. Wolters, Simulating quantum repeater strategies for multiple satellites, *Commun. Phys.* **5**, 169 (2022).
- [5] J. S. Sidhu and P. Kok, Geometric perspective on quantum parameter estimation, *AVS Quantum Sci.* **2**, 014701 (2020).
- [6] M. Gündoğan, J. S. Sidhu, V. Henderson, L. Mazzarella, J. Wolters, D. K. Oi, and M. Krutzik, Proposal for spaceborne quantum memories for global quantum networking, *npj Quantum Inf.* **7**, 128 (2021).
- [7] M. Gündoğan, *et al.*, Topical white paper: A case for quantum memories in space, *ArXiv:2111.09595*.
- [8] M. Gündoğan, J. S. Sidhu, M. Krutzik, and D. K. L. Oi, Time-delayed single satellite quantum repeater node for global quantum communications, *Optica Quantum* **2** (3), 140 (2024).
- [9] J. S. Sidhu, S. K. Joshi, M. Gündoğan, T. Brougham, D. Lowndes, L. Mazzarella, M. Krutzik, S. Mohapatra, D. Dequal, G. Vallone, P. Villoresi, A. Ling, T. Jennewein, M. Mohageg, J. G. Rarity, I. Fuentes, S. Pirandola, and D. K. L. Oi, Advances in space quantum communications, *IET Quantum Commun.* **2**, 182 (2021).
- [10] A. Belenchia, M. Carlesso, Ö. Bayraktar, D. Dequal, I. Derkach, G. Gasbarri, W. Herr, Y. L. Li, M. Rademacher, J. Sidhu, D. K. Oi, S. T. Seidel, R. Kaltenbaek, C. Marquardt, H. Ulbricht, V. C. Usenko, L. Wörner, A. Xuereb, M. Paternostro, and A. Bassi, Quantum physics in space, *Phys. Rep.* **951**, 1 (2022).
- [11] S. Wehner, D. Elkouss, and R. Hanson, Quantum Internet: A vision for the road ahead, *Science* **362**, eaam9288 (2018).
- [12] P. Jianwei, Progress of the quantum experiment science satellite (QUESS) Micius project, *Chin. J. Space Sci.* **38**, 604 (2018).
- [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] S.-K. Liao, *et al.*, Space-to-ground quantum key distribution using a small-sized payload on Tiangong-2 space lab, *Chin. Phys. Lett.* **34**, 090302 (2017).
- [15] A. Villar, A. Lohrmann, X. Bai, T. Vergoossen, R. Bedington, C. Perumangatt, H. Y. Lim, T. Islam, A. Reezwana, Z. Tang, *et al.*, Entanglement demonstration on board a nano-satellite, *Optica* **7**, 734 (2020).
- [16] A. Jones, China plans to take ‘hack-proof’ quantum satellite technology to new heights, *Space* (2023), <https://www.space.com/china-quantum-communications-satellite-higher-orbit-plans>.
- [17] A. Jones, China is developing a quantum communications satellite network, *Spacenews* (2023), <https://spacenews.com/china-is-developing-a-quantum-communications-satellite-network/>.
- [18] IANS, ISRO aims to launch QKD satellite, Ahmedabad to play key role, *Indiatimes* (2023), <https://telecom.economictimes.indiatimes.com/news/portal-in-portal/satcom/isro-aims-to-launch-qkd-satellite-ahmedabad-to-play-key-role/101230570>.
- [19] A. Jones, Europe plans to launch a quantum encryption satellite for ultrasecure communications in 2024, *Space* (2022), <https://www.space.com/europe-quantum-encryption-satellite-planned>.
- [20] K. Cowing, SpeQtral-1 will serve as a pathfinder commercial demonstrator for future quantum key distribution services, *Spaceref* (2023), <https://spaceref.com/space-commerce/speqtral-1-will-serve-as-a-pathfinder-commercial-demonstrator-for-future-quantum-key-distribution-services/>.
- [21] C. Dalibot and S. Tustain, in *2020 International Conference on Environmental Systems* (Texas Digital Library, 2020), <https://www.tdl.org>.
- [22] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. L. Oi, Finite key performance of satellite quantum key distribution under practical constraints, *Commun. Phys.* **6**, 210 (2023).
- [23] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. L. Oi, in *Quantum Computing, Communication, and Simulation III*, edited by P. R. Hemmer and A. L. Migdall, International Society for Optics and Photonics (SPIE, San Francisco, California, United States, 2023), Vol. 12446, p. 124460M.
- [24] 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).
- [25] M. Tomamichel, J. Martinez-Mateo, C. Pacher, and D. Elkouss, Fundamental finite key limits for one-way information reconciliation in quantum key distribution, *Quantum Inf. Proc.* **16**, 280 (2017).

- [26] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, Improved key-rate bounds for practical decoy-state quantum-key-distribution systems, *Phys. Rev. A* **95**, 012333 (2017).
- [27] 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).
- [28] C. C.-W. Lim, F. Xu, J.-W. Pan, and A. Ekert, Security analysis of quantum key distribution with small block length and its application to quantum space communications, *Phys. Rev. Lett.* **126**, 100501 (2021).
- [29] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum cryptography without Bell's theorem, *Phys. Rev. Lett.* **68**, 557 (1992).
- [30] 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).
- [31] A. Anwar, C. Perumangatt, F. Steinlechner, T. Jennewein, and A. Ling, Entangled photon-pair sources based on three-wave mixing in bulk crystals, *Rev. Sci. Instrum.* **92**, 041101 (2021).
- [32] C. Perumangatt, T. Vergoossen, A. Lohrmann, S. Sivasankaran, A. Reezwana, A. Anwar, S. Sachidananda, T. Islam, and A. Ling, in *Quantum Computing, Communication, and Simulation* (SPIE, Online Only, California, United States, 2021), Vol. 11699, p. 1169904.
- [33] 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* **549**, 43 (2017).
- [34] T. Vergoossen, S. Loarte, R. Bedington, H. Kuiper, and A. Ling, Modelling of satellite constellations for trusted node QKD networks, *Acta. Astronaut.* **173**, 164 (2020).
- [35] 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**, 5873 (2023).
- [36] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, *Nat. Commun.* **3**, 634 (2012).
- [37] M. Polnik, L. Mazzarella, M. Di Carlo, D. K. Oi, A. Riccardi, and A. Arulselman, Scheduling of space to ground quantum key distribution, *EPJ Quantum Technol.* **7**, 3 (2020).
- [38] L. Mazzarella, C. Lowe, D. Lowndes, S. K. Joshi, S. Greenland, D. McNeil, C. Mercury, M. Macdonald, J. Rarity, and D. K. L. Oi, Quarc: Quantum research CubeSat—A constellation for quantum communication, *Cryptography* **4**, 7 (2020).
- [39] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. L. Oi, Satellite quantum modelling & analysis software version 1.1: Documentation, *ArXiv:2109.01686*.
- [40] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. L. Oi, Finite key effects in satellite quantum key distribution, *npj Quantum Inf.* **8**, 18 (2022).
- [41] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. L. Oi, in *Quantum Technology: Driving Commercialisation of an Enabling Science II*, edited by M. J. Padgett, K. Bongs, A. Fedrizzi, and A. Politi, International Society for Optics and Photonics (SPIE, Glasgow, United Kingdom, 2021), Vol. 11881, p. 1.
- [42] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, *et al.*, Entanglement-based secure quantum cryptography over 1,120 kilometres, *Nature* **582**, 501 (2020).
- [43] C.-H. F. Fung, X. Ma, and H. F. Chau, Practical issues in quantum-key-distribution postprocessing, *Phys. Rev. A* **81**, 012318 (2010).
- [44] Quantum EncryPtion and Science Satellite (QEYSSat), <http://qeyssat.ca/>, 2022.
- [45] A. Scott, T. Jennewein, J. Cain, I. D'Souza, B. Higgins, D. Hudson, H. Podmore, and W. Soh, The QEYSSat mission: On-orbit demonstration of secure optical communications network technologies, *Proc. SPIE* **11532**, 115320H (2020).
- [46] P. Chaiwongkhot, S. Hosseini, A. Ahmadi, B. L. Higgins, D. Dalacu, P. Poole, R. L. Williams, M. E. Reimer, and T. Jennewein, Enhancing secure key rates of satellite QKD using a quantum dot single-photon source, *ArXiv:2009.11818*.
- [47] T. Jennewein, J.-P. Bourgoin, B. Higgins, C. Holloway, E. Meyer-Scott, C. Erven, B. Heim, Z. Yan, H. Hübel, G. Weihs, E. Choi, I. D'Souza, D. Hudson, and R. Laflamme, QEYSSAT: A mission proposal for a quantum receiver in space, *Proc. SPIE* **8997**, 89970A (2014).
- [48] J.-P. Bourgoin, B. L. Higgins, N. Gigov, C. Holloway, C. J. Pugh, S. Kaiser, M. Cranmer, and T. Jennewein, Free-space quantum key distribution to a moving receiver, *Opt. Express* **23**, 33437 (2015).
- [49] C. J. Pugh, S. Kaiser, J.-P. Bourgoin, J. Jin, N. Sultana, S. Agne, E. Anisimova, V. Makarov, E. Choi, B. L. Higgins, and T. Jennewein, Airborne demonstration of a quantum key distribution receiver payload, *Quantum Sci. Technol.* **2**, 024009 (2017).
- [50] E. Anisimova, B. L. Higgins, J.-P. Bourgoin, M. Cranmer, E. Choi, D. Hudson, L. P. Piche, A. Scott, V. Makarov, and T. Jennewein, Mitigating radiation damage of single photon detectors for space applications, *EPJ Quantum Technol.* **4**, 10 (2017).
- [51] I. DSouza, J.-P. Bourgoin, B. L. Higgins, J. G. Lim, R. Tannous, S. Agne, B. Moffat, V. Makarov, and T. Jennewein, Repeated radiation damage and thermal annealing of avalanche photodiodes, *EPJ Quantum Technol.* **8**, 13 (2021).
- [52] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein, A comprehensive design and performance analysis of low Earth orbit satellite quantum communication, *New J. Phys.* **15**, 023006 (2013).
- [53] C. D. Elvidge, K. E. Baught, J. B. Dietz, T. Bland, P. C. Sutton, and H. W. Kroehl, Radiance calibration of DMSP-OLS low-light imaging data of human settlements, *Remote Sens. Environ.* **68**, 77 (1999).
- [54] P. Cinzano, F. Falchi, and C. D. Elvidge, The night sky in the world, <http://www.lightpollution.it/dmsp/>, 2001.

- [55] A. Berk, G. P. Anderson, P. K. Acharya, L. S. Bernstein, L. Muratov, J. Lee, M. Fox, S. M. Adler-Golden, J. H. Chetwynd, M. L. Hoke, *et al.*, in *Algorithms and Technologies for Multispectral, Hyperspectral, and Ultra-spectral Imagery XI* (SPIE, Orlando, Florida, United States, 2005), Vol. 5806, p. 662.
- [56] C. Erven, B. Heim, E. Meyer-Scott, J.-P. Bourgoin, R. Laflamme, G. Weihs, and T. Jennewein, Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere, *New J. Phys.* **14**, 123018 (2012).
- [57] M. Yang, F. Xu, J.-G. Ren, J. Yin, Y. Li, Y. Cao, Q. Shen, H.-L. Yong, L. Zhang, S.-K. Liao, *et al.*, Spaceborne, low-noise, single-photon detection for satellite-based quantum communications, *Opt. Express* **27**, 36114 (2019).
- [58] Y. C. Tan, R. Chandrasekara, C. Cheng, and A. Ling, Silicon avalanche photodiode operation and lifetime analysis for small satellites, *Opt. Express* **21**, 16946 (2013).
- [59] E. Anisimova, B. L. Higgins, J.-P. Bourgoin, M. Cranmer, E. Choi, D. Hudson, L. P. Piche, A. Scott, V. Makarov, and T. Jennewein, Mitigating radiation damage of single photon detectors for space applications, *EPJ Quantum Technol.* **4**, 1 (2017).
- [60] A. Lenart, S. Sivasankaran, D. K. Oi, A. Ling, P. Neilson, and B. Hidding, CubeSat in-orbit validation of in-situ performance by high fidelity radiation modelling, *ArXiv:2209.00408*.
- [61] Y. Lu, Q. Shao, H. Yue, and F. Yang, A review of the space environment effects on spacecraft in different orbits, *IEEE Access* **7**, 93473 (2019).
- [62] L. de Forges de Parny, O. Alibart, J. Debaud, S. Gresani, A. Lagarrigue, A. Martin, A. Metrat, M. Schiavon, T. Troisi, E. Diamanti, *et al.*, Satellite-based quantum information networks: Use cases, architecture, and roadmap, *Commun. Phys.* **6**, 12 (2023).
- [63] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, J. Lin, H. Dai, S.-Q. Zhao, B. Li, J.-Y. Guan, *et al.*, Long-distance free-space quantum key distribution in daylight towards inter-satellite communication, *Nat. Photonics* **11**, 509 (2017).
- [64] Y.-H. Li, S.-L. Li, X.-L. Hu, C. Jiang, Z.-W. Yu, W. Li, W.-Y. Liu, S.-K. Liao, J.-G. Ren, H. Li, *et al.*, Free-space and fiber-integrated measurement-device-independent quantum key distribution under high background noise, *Phys. Rev. Lett.* **131**, 100802 (2023).
- [65] P. Titum, K. Schultz, A. Seif, G. Quiroz, and B. Clader, Optimal control for quantum detectors, *npj Quantum Inf.* **7**, 53 (2021).
- [66] 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).
- [67] L. Roberts, G. Block, S. Fregoso, H. Herzog, S. Meeker, J. Roberts, J. Tesch, T. Truong, J. Rodriguez, and A. Bechter, in *The Advanced Maui Optical and Space Surveillance Technologies Conference* (Maui Economic Development Board, Maui, Hawaii, USA, 2018), p. 3.
- [68] M. W. Wright, J. F. Morris, J. M. Kovalik, K. S. Andrews, M. J. Abrahamson, and A. Biswas, Adaptive optics correction into single mode fiber for a low Earth orbiting space to ground optical communication link using the OPALS downlink, *Opt. Express* **23**, 33705 (2015).
- [69] C. J. Pugh, J.-F. Lavigne, J.-P. Bourgoin, B. L. Higgins, and T. Jennewein, Adaptive optics benefit for quantum key distribution uplink from ground to a satellite, *Adv. Opt. Technol.* **9**, 263 (2020).
- [70] C. Scharlemann, M. Tajmar, I. Vasiljevich, N. Buldrini, D. Krejci, and B. Seifert, in *32nd International Electric Propulsion Conference, Wiesbaden, Germany, September 2011, IEPC-2011*, Vol. 171 (Electric Rocket Propulsion Society, Wiesbaden, Germany, 2011).
- [71] S. Shafeeq, Nanosatellite with Singapore start-up's thruster deployed into space on SpaceX mission, *The Straits Times* (2022), <https://www.straitstimes.com/singapore/nanosatellite-from-spacex-launches-into-space-with-singapore-tech-start-ups-thruster>.
- [72] N. Schwartz, D. Pearson, S. Todd, A. Vick, D. Lunney, and D. MacLeod, in *30th annual AIAA/USU Conference on Small Satellites (SSC16-WK-3)* (Utah State University, Utah, USA, 2016).
- [73] V. V. Corbacho, H. Kuiper, and E. Gill, Review on thermal and mechanical challenges in the development of deployable space optics, *J. Astron. Telesc. Instrum. Syst.* **6**, 1 (2020).
- [74] D. Dequal, G. Vallone, D. Bacco, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, Experimental single-photon exchange along a space link of 7000 km, *Phys. Rev. A* **93**, 010301 (2016).
- [75] B. Dirks, I. Ferrario, A. Le Pera, D. V. Finocchiaro, M. Desmons, D. de Lange, H. de Man, A. J. Meskers, J. Morits, N. M. Neumann, *et al.*, in *International Conference on Space Optics—ICSO 2020*, International Society for Optics and Photonics (SPIE, Dubrovnik, Croatia, 2021), Vol. 11852, p. 118520J.
- [76] 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**, 1 (2021).
- [77] I. Holzman and Y. Ivry, Superconducting nanowires for single-photon detection: Progress, challenges, and opportunities, *Adv. Quantum Technol.* **2**, 1800058 (2019).
- [78] N. Lütkenhaus, Estimates for practical quantum cryptography, *Phys. Rev. A* **59**, 3301 (1999).
- [79] H. P. Stahl, Multivariable parametric cost model for ground and space telescope assemblies, *Bull. AAS* **51**, 51 (2019).
- [80] N. L. Piparo, N. Sinclair, and M. Razavi, Memory-assisted quantum key distribution resilient against multiple-excitation effects, *Quantum Sci. Technol.* **3**, 014009 (2017).
- [81] J. S. Sidhu and P. Kok, Quantum metrology of spatial deformation using arrays of classical and quantum light emitters, *Phys. Rev. A* **95**, 063829 (2017).
- [82] J. S. Sidhu and P. Kok, Quantum Fisher information for general spatial deformations of quantum emitters, *ArXiv:1802.01601*.
- [83] J. S. Sidhu, Y. Ouyang, E. T. Campbell, and P. Kok, Tight bounds on the simultaneous estimation of incompatible parameters, *Phys. Rev. X* **11**, 011028 (2021).

- [84] M. He, R. Malaney, and J. Green, in *ICC 2019—2019 IEEE International Conference on Communications (ICC)* (Shanghai, China, 2019), p. 1.
- [85] D. Dequal, L. Trigo Vidarte, V. Roman Rodriguez, G. Vallone, P. Villoresi, A. Leverrier, and E. Diamanti, Feasibility of satellite-to-ground continuous-variable quantum key distribution, *npj Quantum Inf.* **7**, 3 (2021).
- [86] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Reference frames, superselection rules, and quantum information, *Rev. Mod. Phys.* **79**, 555 (2007).
- [87] A. Laing, V. Scarani, J. G. Rarity, and J. L. O’Brien, Reference-frame-independent quantum key distribution, *Phys. Rev. A* **82**, 012304 (2010).
- [88] C. Wang, S.-H. Sun, X.-C. Ma, G.-Z. Tang, and L.-M. Liang, Reference-frame-independent quantum key distribution with source flaws, *Phys. Rev. A* **92**, 042319 (2015).
- [89] R. Tannous, Z. Ye, J. Jin, K. B. Kuntz, N. Lütkenhaus, and T. Jennewein, Demonstration of a 6 state-4 state reference frame independent channel for quantum key distribution, *Appl. Phys. Lett.* **115**, 211103 (2019).
- [90] J. Jin, S. Agne, J.-P. Bourgoin, Y. Zhang, N. Lütkenhaus, and T. Jennewein, Demonstration of analyzers for multi-mode photonic time-bin qubits, *Phys. Rev. A* **97**, 043847 (2018).
- [91] J. Jin, J.-P. Bourgoin, R. Tannous, S. Agne, C. J. Pugh, K. B. Kuntz, B. L. Higgins, and T. Jennewein, Genuine time-bin-encoded quantum key distribution over a turbulent depolarizing free-space channel, *Opt. Express* **27**, 37214 (2019).
- [92] R. Tannous, W. Wu, S. Vinet, C. Perumangatt, D. Sinar, A. Ling, and T. Jennewein, Towards fully passive time-bin quantum key distribution over multi-mode channels, *ArXiv:2302.05038*.
- [93] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Quantum cryptography using entangled photons in energy-time Bell states, *Phys. Rev. Lett.* **84**, 4737 (2000).
- [94] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Provably secure and high-rate quantum key distribution with time-bin qudits, *Sci. Adv.* **3**, e1701491 (2017).
- [95] T. Brougham, C. F. Wildfeuer, S. M. Barnett, and D. J. Gauthier, The information of high-dimensional time-bin encoded photons, *Eur. Phys. J. D.* **70**, 214 (2016).
- [96] A. Tello Castillo, C. Novo, and R. Donaldson, in *Emerging Imaging and Sensing Technologies for Security and Defence V; and Advanced Manufacturing Technologies for Micro- and Nanosystems in Security and Defence III* (SPIE, Online Only, United Kingdom, 2020), Vol. 11540, p. 1154006.
- [97] R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J.-F. Roch, A. Beveratos, R. Brouri-Tualle, J.-P. Poizat, and P. Grangier, Experimental open-air quantum key distribution with a single-photon source, *New J. Phys.* **6**, 92 (2004).
- [98] K. Takemoto, Y. Nambu, T. Miyazawa, Y. Sakuma, T. Yamamoto, S. Yorozu, and Y. Arakawa, Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors, *Sci. Rep.* **5**, 14383 (2015).
- [99] N. Sangouard and H. Zbinden, What are single photons good for?, *J. Mod. Opt.* **59**, 1458 (2012).
- [100] A. I. Lvovsky, B. C. Sanders, and W. Tittel, Optical quantum memory, *Nat. Photonics* **3**, 706 (2009).
- [101] M. Müller, S. Bounouar, K. D. Jöns, M. Glässl, and P. Michler, On-demand generation of indistinguishable polarization-entangled photon pairs, *Nat. Photonics* **8**, 224 (2014).
- [102] 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* **557**, 400 (2018).
- [103] Y.-M. Xie, C.-X. Weng, Y.-S. Lu, Y. Fu, Y. Wang, H.-L. Yin, and Z.-B. Chen, Scalable high-rate twin-field quantum key distribution networks without constraint of probability and intensity, *Phys. Rev. A* **107**, 042603 (2023).
- [104] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference, *PRX Quantum* **3**, 020315 (2022).
- [105] P. Zeng, H. Zhou, W. Wu, and X. Ma, Mode-pairing quantum key distribution, *Nat. Commun.* **13**, 3903 (2022).
- [106] L. Zhou, J. Lin, Y.-M. Xie, Y.-S. Lu, Y. Jing, H.-L. Yin, and Z. Yuan, Experimental quantum communication overcomes the rate-loss limit without global phase tracking, *Phys. Rev. Lett.* **130**, 250801 (2023).
- [107] D. P. Naughton, R. Bedington, S. Barraclough, T. Islam, D. Griffin, B. Smith, J. Kurtz, A. S. Alenin, I. J. Vaughn, A. Ramana, *et al.*, Design considerations for an optical link supporting intersatellite quantum key distribution, *Opt. Eng.* **58**, 016106 (2019).
- [108] T. Islam, R. Bedington, and A. Ling, in *Quantum Information Science and Technology III* (SPIE, Warsaw, Poland, 2017), Vol. 10442, p. 28.
- [109] D. Dequal, L. Trigo Vidarte, V. Roman Rodriguez, G. Vallone, P. Villoresi, A. Leverrier, and E. Diamanti, Feasibility of satellite-to-ground continuous-variable quantum key distribution, *npj Quantum Inf.* **7**, 1 (2021).