communications physics

ARTICLE

https://doi.org/10.1038/s42005-023-01299-6 OPEN

Finite key performance of satellite quantum key distribution under practical constraints

Jasminder S. Sidhu [1✉], Thomas Brougham[1], Duncan McArthur[1], Roberto G. Pousa [1] & Daniel K. L. Oi [1]

Global-scale quantum communication networks will require efficient long-distance distribution of quantum signals. While optical fibre communications are range-limited due to exponential losses in the absence of quantum memories and repeaters, satellites enable intercontinental quantum communications. However, the design of satellite quantum key distribution (SatQKD) systems has unique challenges over terrestrial networks. The typical approach to modelling SatQKD has been to estimate performances with a fully optimised protocol parameter space and with few payload and platform resource limitations. Here, we analyse how practical constraints affect the performance of SatQKD for the Bennett-Brassard 1984 (BB84) weak coherent pulse decoy state protocol with finite key size effects. We consider engineering limitations and trade-offs in mission design including limited in-orbit tunability, quantum random number generation rates and storage, and source intensity uncertainty. We quantify practical SatQKD performance limits to determine the long-term key generation capacity and provide performance benchmarks to support the design of upcoming missions.

[1] SUPA Department of Physics, University of Strathclyde, Glasgow G4 0NG, UK. ✉email: jsmdrsidhu@gmail.com

Quantum technologies have the potential to enable or greatly enhance applications including secure communications[1–4], improved computation[5,6], sensing, and imaging[7–13]. In addition, a distributed ecosystem of quantum technologies would provide further performance improvements and additional capabilities. The distribution of quantum resources across such a networked architecture comprises the fundamental building blocks of the quantum internet[4].

Satellites will be integral to a scalable architecture to expand the range of quantum networks to global scales, motivating the surge in recent activities in space quantum communications[14–22]. Satellite-based quantum key distribution (SatQKD) is a precursor to long-range applications of general quantum communication[2,21]. Although a general-purpose quantum network requires substantial advancements in quantum memories, multi-partite entangled state generation, routing techniques, and error correction[23], the development of SatQKD provides crucial knowledge and experience for global-scale quantum networks by developing the infrastructure and maturity of space-based long-distance quantum links.

Pioneering quantum communication demonstrations by the ~650 kg Micius satellite showed that SatQKD and entanglement distribution is possible over record scales[15,24,25]. Building upon these results, small satellite (<100 kg) missions are attractive due to lower development costs and faster development times compared with conventional large satellites. However, the limited size, weight, and power (SWaP) available on small satellites and reduced capabilities put them at a marked disadvantage versus larger satellites such as Micius. Despite this, feasibility studies for small-satellite-based QKD and in-orbit demonstration CubeSat-based pathfinder missions are promising[18,26]. For low-Earth orbit (LEO) satellites, a particular challenge is the limited time window to operate a quantum channel with an optical ground station (OGS)[27,28]. This limitation disproportionately constrains the volume of secure keys that can be generated due to a pronounced impact of statistical uncertainties in estimated parameters. Together with the constrained SWaP available, small-satellite missions operate under the framework of finite-resource quantum information. Understanding the impact of these constraints on SatQKD has received little attention and has both immediate and practical relevance to future satellite-based missions. Here, we fill this gap by establishing practical performance bounds on SatQKD operation under a representative set of physical resources.

The first constraint we consider is the limited practicality of reconfiguring all QKD protocol parameters in-flight and on a pass-by-pass basis. SatQKD modelling often does not consider this, optimising the secret key length (SKL) over the entire parameter space of the protocol for each pass scenario[29,30]. It is more realistic to consider a number of parameters as fixed, that include the operating basis bias at the OGS and the transmitted intensities. Parameter fixing has been explored in the context of terrestrial free-space QKD[31]. In SatQKD the highly variable channel losses in SatQKD with fixed parameters require more sophisticated modelling and analysis. The limited transmission times of SatQKD further make these effects more pronounced, highlighting the importance of considering limited system adaptability. We consider a second constraint from small satellite SWaP envelopes that may limit the quantum random number generation (QRNG) subsystem driving a prepare and measure source. This directly impacts the achievable SKL by limiting signal transmission.

In Results, an overview of our SatQKD system modelling and the protocol optimisation framework is provided, including a discussion of all modifications that account for different constraints from engineering limitations and limited in-orbit tunability. Following the recent progress of SatQKD sources, we explore the effect of the repetition rate on key length. We highlight the impact of finite-key effects and establish minimum source rates based on tolerance to operational losses. Given the difficulty of implementing a SatQKD system where all parameters can be reconfigured for different overpasses, we then determine the impact of fixed parameters on the key length. In particular, we fix the signal intensities and the receiver basis bias. We then explore SKL generation for restricted QRNG resources and illustrate the significant impact of limited random bit generation rates on the SKL in the 'QRNG subsystem limitations' subsection of Results. Here, we also quantify the minimum memory storage required for non-zero finite key extraction for one overpass. Further, we explore the impact of intensity uncertainties due to limited onboard monitoring accuracy. Conclusions and discussions are provided, where we provide key conclusions to help overcome these limitations for future SatQKD systems.

Results

Modelling framework. We consider a satellite in a circular Sun-synchronous orbit (SSO) of altitude $h = 500$ km implementing downlink QKD to an OGS during the night to minimise background light. The elevation and range of the satellite-OGS channel are calculated as a function of time for different satellite overpass geometries and ground track offsets, $d_{\min}$, and maximum satellite overpass elevations, $\theta_{\max}$ (Fig. 1). Different satellite overpasses have different values for $d_{\min}$. This means $d_{\min}$ can be used to characterise each overpass. In fact, for a fixed orbital altitude, the ground track offset $d_{\min}$ and the maximum elevation angle, $\theta_{\max}$, are equivalent. The ideal overpass corresponds to the satellite passing the OGS directly overhead, or zenith ($d_{\min} = 0$ m, $\theta_{\max} = 90°$), since it provides the longest transmission time and has the lowest average channel loss. Generally, a satellite will not pass zenith but will reach a maximum elevation $\theta_{\max}$(<90°). We consider a minimum elevation transmission limit of $\theta_{\min} = 10°$ that reflects practicalities such as local horizon visibility and system pointing limitations.

The instantaneous link efficiency depends on the elevation $\theta(t)$, the range $R(t)$ between the satellite and OGS, and source wavelength λ, and is used to generate count statistics. For a fixed orbital altitude, the satellite-OGS range is implicitly defined

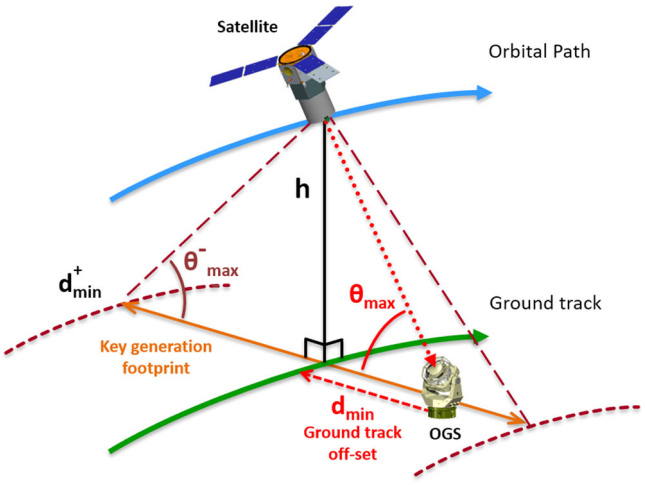

Fig. 1 General satellite overpass geometry. The satellite reaches a maximum elevation of $\theta_{\max}$, corresponding to the minimum optical ground station (OGS) ground track distance, $d_{\min}$. The smallest $\theta_{\max}$ that generates a non-zero finite key is denoted $\theta^{-}_{\max}$ and characterises the operational SatQKD key generation footprint $2d^{+}_{\min}$.

through the satellite's elevation. The link efficiency is then defined as (in dB),

$$\eta_\lambda(\theta) = \eta_{\rm diff}(\lambda,\theta) + \eta_{\rm atm}(\lambda,\theta) + \eta_{\rm int}, \quad (1)$$

where $\eta_{\rm diff}$, $\eta_{\rm atm}$, and $\eta_{\rm int}$ are losses from diffraction, atmospheric scattering and absorption, and a fixed 'intrinsic' system efficiency, respectively. To characterise the overall system electro-optical efficiency independent of satellite overpass trajectory, we define the system loss metric, $\eta_{\rm loss}^{\rm sys}$, as the total instantaneous link efficiency at zenith. Diffraction losses are estimated using the Fraunhofer approximation to the Rayleigh-Sommerfeld diffraction integral to determine the power at the receiver, P_R, which is normalised by the power at the transmitter, P_T such that $\eta_{\rm diff} = -10\log_{10}(P_R/P_T)$. Atmospheric absorption and scattering losses are calculated using $\eta_{\rm atm} = -10\log_{10}T_\lambda$, where the transmissivity, T_λ, is determined using MODTRAN for a given wavelength and elevation[32]. The 'intrinsic' system loss, $\eta_{\rm int}$, accounts for: fixed losses inherently built into the system due to detector efficiency, internal losses of the receiver; pointing losses; and imperfect non-diffraction-limited beam propagation, and is conservatively set to 20 dB to model a SatQKD system with overall $\eta_{\rm loss}^{\rm sys} = 40$ dB. Different SatQKD systems with various fixed losses can be modelled by scaling the $\eta_{\rm loss}^{\rm sys}$ value. See the Methods subsection 'Loss modelling' for more detail on loss modelling.

The link loss characterises the probability that a single photon transmitted by the satellite is detected by the OGS. A lower dB value of $\eta_{\rm link}$ represents smaller loss due to better system electro-optical efficiency. This improvement could stem from the use of larger transmit and receive aperture diameters, better pointing accuracy, lower receiver internal losses, and higher detector efficiencies. Internal transmitter losses are not included since they can be countered by adjusting the weak coherent pulse (WCP) source to maintain the desired exit aperture intensities[33]. We also do not explicitly consider time-varying transmittance, modelling the average change in channel loss due only to the change in elevation with time. For discrete variable QKD (DV-QKD) protocols, e.g. BB84, channel transmissivity fluctuations do not directly impact the secret key rate, in contrast to continuous variable QKD where this appears as excess noise leading to key reduction[34,35].

We model a small satellite QKD system, for example[36], implementing a decoy-state BB84 protocol in a downlink configuration for QKD service provision using a WCP source. We consider a source wavelength of $\lambda = 785$ nm, a transmitter (receiver) aperture diameter of 8 cm (70 cm), and a Gaussian beam waist of 8 cm. Our general analysis is wavelength agnostic, but we specifically analyse $\lambda = 785$ nm as this is representative of several missions currently in development[26,36,37], partly due to favourable atmospheric transmission and the availability of relevant sources and detectors[33]. Figure 2a illustrates the modelled transmission loss and Fig. 2b the link efficiency for different overpass geometries.

In addition to this link loss, we include several error sources. First, after-pulsing in a photon detector can have adverse effects on the estimate of click statistics. While the after-pulsing probability is detector and operating condition-dependent, we take a value of 0.1%, which is consistent with the literature[38–40]. Second, the intrinsic quantum bit error rate, $\mathrm{QBER_I}$, is defined as the lumped error from source quality, receiver measurement fidelity, basis misalignment, and polarisation fluctuations[41]. Finally, we define the extraneous count probability, $p_{\rm ec}$, as the sum of dark and background light count rates and is assumed constant and independent of elevation. Together, these losses and errors provide a complete characterisation of a SatQKD system and are summarised in Table 1.

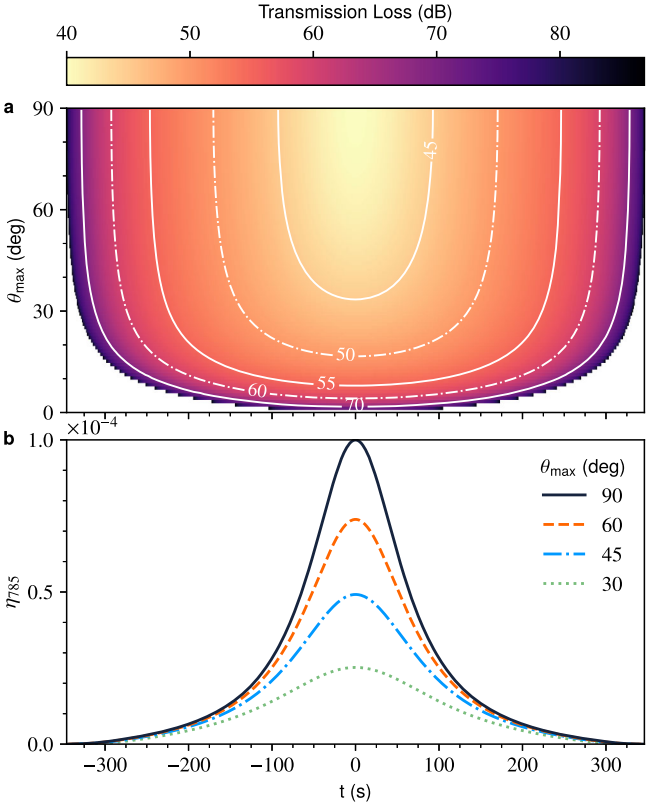

Fig. 2 Link model for satellite-to-ground QKD. a Instantaneous link efficiency, η_{785} (Eq. (1)), for different satellite overpasses with maximum elevation, $\theta_{\rm max}$, and time with $\lambda = 785$ nm. The smallest transmission loss of 40 dB occurs for a zenith overpass ($\theta_{\rm max} = 90°$) at time $t = 0$. **b** η_{785} for specific $\theta_{\rm max}$. System parameters as in Table 1.

Note that our current analysis could be extended to model an uplink channel by using a suitable link-loss model (loss vs elevation). A ground-to-satellite link will increase channel losses due to the shower curtain effect. While turbulence is highly dependent on elevation, it generally leads to an additional 20 dB of loss compared to a downlink channel[33].

With our dynamic link model, we can determine expected click statistics and estimate errors due to losses, which together are used to estimate the SKL. For efficient BB84 with two decoy states, the X-basis is used to construct the secret key, while the Z-basis is used for parameter estimation[19,38,42–45]. The probability for Alice to prepare in the X-basis is $P_{\rm X}^A$, while Bob's probability to measures in the X-basis is $P_{\rm X}^B$. It is standard to take $P_{\rm X}^A = P_{\rm X}^B = P_{\rm X}$, however, it is possible that $P_{\rm X}^A \neq P_{\rm X}^B$, due to practical considerations[31]. To evaluate the secret key length we estimate the number of bits from vacuum events, $s_{\rm X,0}$, the number of bits from single photon events $s_{\rm X,1}$, and the phase error $\phi_{\rm X}$. The exact formulas for these terms are provided in ref. [29], which is based on refs. [19,42]. After privacy amplification, the final SKL, ℓ, is given by[42]

$$\ell = \left\lfloor s_{\rm X,0} + s_{\rm X,1}(1 - h(\phi_{\rm X})) - \lambda_{\rm EC} - 6\log_2\frac{21}{\epsilon_{\rm s}} - \log_2\frac{2}{\epsilon_{\rm c}} \right\rfloor, \quad (2)$$

where $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function, $\lambda_{\rm EC}$ is the amount of bits exchanged during error correction and $\epsilon_{\rm s}$ and $\epsilon_{\rm c}$ are the composable security and correctness parameters, respectively[42,46]. The value for $\lambda_{\rm EC}$ will be known in practice, however, to simulate the performance we use

Table 1 Reference system parameters.

Parameter description	Value
Transmitter aperture diameter, T_X	8 cm
Receiver aperture diameter, R_X	70 cm
Gaussian Beam waist, w_0	4 cm
Source wavelength, λ	785 nm
Source rate, f_s	500 MHz
Satellite orbit altitude, h	500 km
Minimum elevation limit, $\theta_{\min}$	10°
Intrinsic quantum bit error rate, $\mathrm{QBER_I}$	0.5%
Extraneous count probability, p_{ec}	5×10^{-7}
After-pulsing probability, p_{ap}	0.1%
System loss metric, $\eta_{\mathrm{loss}}^{\mathrm{sys}}$	40 dB
↪ Diffraction loss at zenith, $\eta_{\mathrm{diff}}(\lambda, 90)$	19.4 dB
↪ Atmospheric loss at zenith, $\eta_{\mathrm{atm}}(\lambda, 90)$	0.6 dB
↪ Optical inefficiency, ↪ Imperfect beam propagation (η_{int})	12.0 dB, 8.0 dB
Correctness parameter, ϵ_c	10^{-15}
Security parameter, ϵ_s	10^{-10}

Transmitter, receiver, and source properties determine range and elevation-dependent loss. The system loss metric, $\eta_{\mathrm{loss}}^{\mathrm{sys}}$, defined as the link efficiency at zenith, is 40 dB. The 'intrinsic' system loss is broken down into two components (see the section 'Loss modelling'). $\eta_{\mathrm{loss}}^{\mathrm{sys}}$ can be scaled to model other SatQKD systems that differ by a fixed link loss ratio, e.g. different T_X or R_X apertures, or detector efficiencies. The intrinsic quantum bit error rate, $\mathrm{QBER_I}$, incorporates errors from source quality, receiver measurement fidelity, basis misalignment, and polarisation fluctuations, while the extraneous count probability, p_{ec}, incorporates detector dark count and background rate. The correctness and security parameters are used to determine the finite-block composable SKL.

an estimate that varies with the block size, quantum bit error rate, and the required correctness parameter[47]. For more details on the estimated protocol parameters and the SKL see the Methods 'The protocol and secret key length optimsation'.

A full optimisation of Eq. (2) over the protocol parameter space yields an optimistic performance that may not be achieved in practice. Specifically, engineering limitations and limited in-orbit tunability would lead to instances where certain protocol parameters are fixed. The optimisation routine can be modified to impose additional constraints that correspond to these limitations. A full description of these modifications is provided in Methods 'The protocol and secret key length optimsation'.

Source rate. Micius performed finite key generation with a 100 MHz source repetition rate, later upgraded in-flight to 200 MHz[39]. Miniaturisation of such high-speed sources enables their use on small satellites. For example, increasing the source repetition rate leads to a larger block size that reduces statistical uncertainties in parameter estimation, hence a higher finite key rate. This expands the pass opportunities that result in non-zero secret keys, enhancing the robustness and effective key transmission footprint of a SatQKD system[29]. In addition, the use of high-speed sources can help higher altitude SatQKD operation by partially compensating for increased channel losses[29]. In this section, we investigate the effect of operating source rate, f_s, on the robustness of SatQKD systems to channel loss in the finite key regime.

To evaluate finite key efficiency, Fig. 3 illustrates the source rate normalised SKL as a function of source rate for a zenith overpass (solid lines) and a satellite overpass with $\theta_{\max} = 30^\circ$ (dashed lines) for three different system configurations of $\{\mathrm{QBER_I}, p_{\mathrm{ec}}\}$. For a given time window Δt, the block size increases with increasing f_s, which improves the normalised finite SKL. This improvement indicates a critical value f_s^{crit} below which finite key effects overwhelm raw key transmission and the distillable finite SKL is zero. For $f_s < f_s^{\mathrm{crit}}$, this *key suppression region* is illustrated in shaded blue for System A with $\mathrm{QBER_I} = 0.1\%$, $p_{\mathrm{ec}} = 1\times10^{-8}$, and $\theta_{\max} = 90^\circ$. Above f_s^{crit}, we note the SKL scales super-linearly with the source rate due to multiple improvements in parameter estimation, error correction efficiency, and reduced overhead of the composable security parameters with increasing block length.

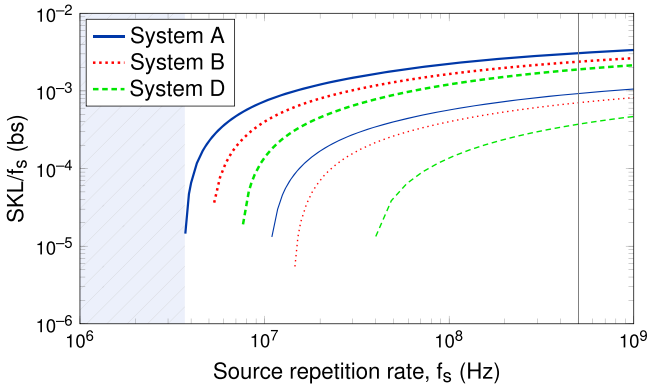

Fig. 3 Finite key efficiency vs source rate. Source rate normalised secret key length (SKL) as a function of f_s for overpasses with $\theta_{\max} = 90^\circ$ (solid lines) and 30° (dashed lines), for three system configurations $\{\mathrm{QBER_I}, p_{\mathrm{ec}}\}$: A = $\{0.1\%, 1\times10^{-8}\}$, B = $\{0.5\%, 1\times10^{-8}\}$, and D = $\{0.5\%, 1\times10^{-7}\}$. The critical f_s value corresponds to the transition of zero and non-zero finite SKL. The shaded blue region illustrates the key suppression region for System A with $\theta_{\max} = 90^\circ$ where statistical fluctuations in estimated parameters overwhelm key generation due to finite available statistics. The vertical line is at $f_s = 500$ MHz, which we consider for the remainder of the paper.

The vertical grey line in Fig. 3 corresponds to 500 MHz, well outside the key suppression region, that we take as a representative value for a near-term small satellite source. This provides robustness against a range of typical extraneous counts and intrinsic QBERs expected in SatQKD and provides feasible finite key generation for a single satellite overpass, but is compatible with modest receiver detectors. Higher source rates, though providing larger key lengths, require lower detector timing jitter. Silicon single-photon avalanche photodiodes (Si-SPADs) typically have timing jitter in the order of ~0.5 ns[48] compatible with coincidence windows of ~1 ns and interpulse separations of 2 ns. Extending clock rates to the GHz range requires lower timing jitters such as provided by superconducting nanowire single-photon detectors (SNSPDs)[49] at the expense of greater SWaP and cost (SWaP-C) owing to the need for cryogenic operation and single mode coupling that raises further system design issues. Therefore, the following analysis will assume a source rate of 500 MHz unless stated otherwise given it balances the tradeoff between detector performance requirements, hence SWaP-C, and count rate.

Impact of parameter fixing. SatQKD modelling often involves optimising the operational parameter space associated with the protocol and system configuration to maximise the number of finite keys generated. However, achieving these optimised key lengths assumes all parameters can be easily changed to operate at their optimised values. It may be desirable on cost, complexity, and robustness grounds to deploy SatQKD systems with limited reconfigurability, motivating analyses where some parameters are fixed. First, the OGS basis choice is often implemented passively using a fixed beamsplitter. Thus, changing receiver basis bias by physically swapping out the beamsplitter for different optimised values on a per-pass basis may be impractical in live deployment. A variable beamsplitter could be considered but with cost, complexity, and performance considerations. Note that the transmitter basis bias can be easily adjusted in the random bit

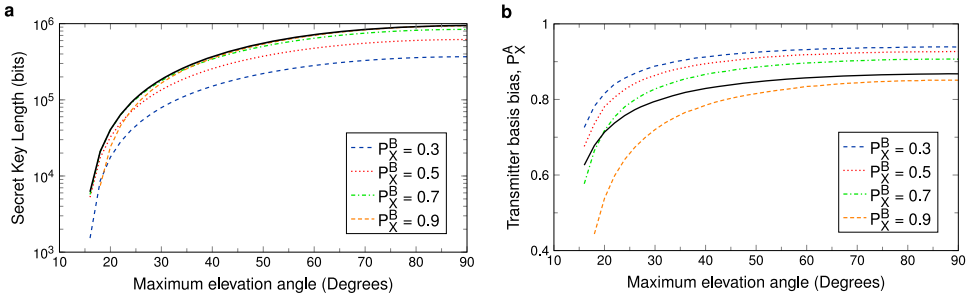

Fig. 4 Impact of fixed receiver basis bias and source intensities. All curves are for source intensities $\mu_1 = 0.71$, $\mu_2 = 0.14$, $\mu_3 = 0$, extraneous count probability $p_{ec} = 10^{-7}$, and intrinsic quantum bit error rate $QBER_I = 0.005$. **a** Secret key length (SKL) as a function of θ_{max} for a fixed P_X^B and fixed pulse intensities. For reference, the black solid line represents the optimal SKL maximised over P_X^A and P_X^B with the same fixed intensity values. **b** Plots of optimised values for P_X^A as a function of θ_{max} for a fixed basis P_X^B and fixed pulse intensities. The black solid line represents the optimal basis bias P_X^A with the same fixed intensity values.

generation and processing of the data used to control the source, hence we consider this parameter to be easily varied. Second, all the operational pulse intensities μ_j may be fixed pre-flight to avoid more complex source driving systems with increased SWaP-C and reliability concerns. Since the optimal decoy-state intensities strongly depend on the channel loss, background counts, and the satellite's orbital trajectory, fixed values may significantly impact the SKL.

In this section, we determine the impact of these engineering constraints on the finite SKL. We constrain the receiver basis bias and decoy-state intensities to certain fixed values, such that $P_X^B = \{0.3, 0.5, 0.7, 0.9\}$ (commonly available beamsplitter splitting ratios) in addition to the ideal value of $P_X^B = 0.84$ that corresponds to a custom beamsplitter and $\{\mu_1, \mu_2, \mu_3\} = \{0.71, 0.14, 0\}$. The derivation of these ideal values can be seen in Methods 4 for fixed parameter optimisation that maximise the long-term average SKL. For these fixed values, Fig. 4a illustrates the finite SKL as a function of different satellite overpasses. Despite this restriction, we note it is possible to generate near-optimal SKLs across a wide range of elevation angles. Further, increasing the OGS bias can generate higher finite SKL. However, we observe that for a choice of $P_X^B = 0.9$, it is not possible to extract a secret key at lower θ_{max}. This suggests that choosing too large an OGS bias can reduce the key generation capacity, owing to fewer overpasses opportunities that generate a non-zero key. To understand this effect, we recall that a larger receiver basis bias corresponds to a smaller portion of received bits dedicated to parameter estimation. Therefore, choosing a large OGS basis bias at larger average channel QBERs leads to less efficient parameter estimation, which generates zero secret keys. SatQKD systems should therefore carefully choose the fixed OGS bias to address the tradeoff between a maximised single pass SKL and the long-term key generation capacity. Notice that the secret key length for $P_X^B = 0.7$ is approximately the same as for $P_X^B = 0.9$, but with non-zero keys at lower elevations.

Figure 4b illustrates the optimal P_X^A values that maximise the SKL as a function of elevation angle for each fixed value of the receiver basis bias. We first note the basis bias for the transmitter and receiver are generally different, which differs from the usual case considered in the literature. The value of P_X^A can vary to compensate for the fixed value of P_X^B. One can show that if both P_X^B and P_X^A can vary freely, then the optimal raw key length is found for $P_X^B = P_X^A$[31]. From Fig. 4b we find that for $P_X^B = 0.3$ and 0.5, we observe that $P_X^A > P_X^B$. This suggests that a small fixed receiver basis bias leads to too large a portion of signals dedicated to parameter estimation, which is compensated for by choosing a large transmitter basis bias. Equally, for $P_X^B = 0.9$ we observe that $P_X^A < P_X^B$. This clearly demonstrates that when we *fix*P_X^B, then choosing an equal basis bias is not optimal. However, when we are free to optimise both P_X^B and P_X^A, then choosing $P_X^A = P_X^B$ is optimal[31].

Despite the impracticality of implementing a fully optimised parameter space, we find a number of ways SatQKD missions can enhance finite key generation. This involves careful selection of P_X^B that maximises both the single-pass SKL and the long-term key generation capacity and careful selection of the decoy-state intensities that can counter the effects of large channel losses.

QRNG subsystem limitations. Prepare and measure protocols require random bits for the preparation of signal states. QRNGs with the required rate to feed a high-speed source in real time may incur significant onboard processing resources and SWaP. Alternatively, the random bits can be generated at a much slower rate with less resource-hungry QRNGs prior to the overpass, assuming that the transmission time duty cycle is small compared to the total orbital time. For this latter situation, we consider limits on the amount of onboard storage for random bits to drive the source, often limited on small satellites. This constrains the amount of reconciled data established between a satellite and OGS, thus directly impacting the achievable SKL per pass. Unlike in previous sections where we assumed the source can run indefinitely, in this section, we extend our analysis to model the impact of varying memory storage limits of cryptographically secure random bits on the final SKL.

For a two decoy-state weak coherent state protocol, each pulse consumes four random bits; one for the basis choice, one for the key value, and two for the intensity choice. For the efficient BB84 decoy-state protocol, the basis choice bit and the intensity bits are biased. In general, it takes at most two unbiased bits on average to generate one biased bit[50], hence each pulse requires up to seven unbiased bits from the quantum random number generator (QRNG), though only four bits need to be stored after biasing. At 500 MHz source rate, this requires 2 Gb/s of stored random bits to drive the source. Therefore, a zenith pass with a maximum overpass duration of 444 s (accounting for a minimum elevation limit of 10°) requires a minimum availability of 111 GB of random bits. Current state of the art in space-validated QRNGs can achieve rates of 1–20 Mb/s[51,52], which falls short to support complete transmission, and thus necessitates a buffer.

First, we examine the effects of a limited random bit memory buffer on the finite key. An 8 GB buffer can support up to 32 s transmission time for a 500 MHz source, which is much shorter than the maximum overpass duration of 444 s. Figure 5a (left-hand axis) shows the per-pass SKL for different memory buffers as a function of overpass geometry (d_{min}, θ_{max}). A larger memory buffer

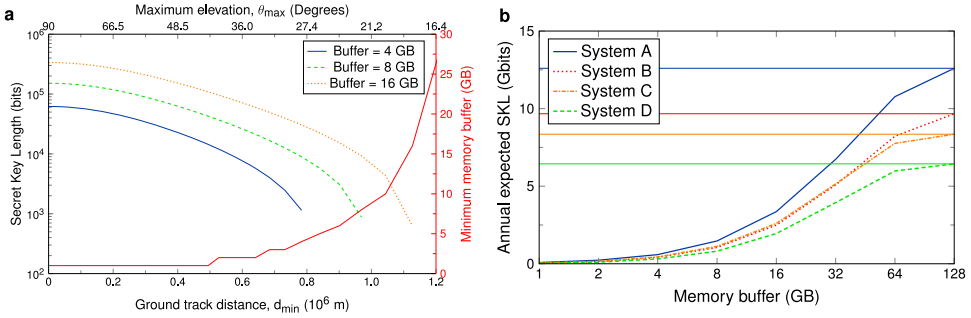

Fig. 5 Overpass and memory buffer effects with $\eta_{loss}^{sys} = 40$ dB and $f_s = 500$ MHz. a Secret key length (SKL) (left axis) and minimum memory buffer (right axis) as a function of ground track distance. We consider $QBER_I = 0.5\%$, and $p_{ec} = 1 \times 10^{-7}$ (System D). A larger memory buffer permits a longer transmission time, which extends the operational footprint of the SatQKD system. Further, a larger minimum memory buffer requirement is observed at larger ground track distances to generate non-zero finite keys. This provides an indication of SatQKD system specifications. **b** Annual expected SKL for an OGS at a latitude of 55.9° N as a function of Memory Buffer. We illustrate four distinct system configurations $\{QBER_I, p_{ec}\}$: A = $\{0.1\%, 1 \times 10^{-8}\}$, B = $\{0.5\%, 1 \times 10^{-8}\}$, C = $\{0.1\%, 1 \times 10^{-7}\}$, and D = $\{0.5\%, 1 \times 10^{-7}\}$. Dashed lines indicate the annual SKL expected without memory constraints.

permits longer transmission times, which enhances the finite SKL and extends the operational footprint of the SatQKD system. Second, we determine the minimum memory buffer required to yield non-zero finite keys for different overpasses. For a given overpass, the smallest block size that yields a non-zero finite key defines the smallest operational time window, t_{min}, that should be supported by the onboard storage. This provides a measure of the memory buffer requirement for a SatQKD mission, given by $f_s t_{min}/2$ Bytes. The right-hand axis of Fig. 5a illustrates the minimum memory buffer required for different satellite overpass trajectories. The demand for larger onboard storage requirements increases with increasing ground track distances. This is because satellite overpasses with larger ground track distances require larger minimum transmitted signals to overcome the larger average channel losses and generate a non-zero finite key.

Third, to quantify the overall impact of limited memory buffers on the SKL, we estimate the annual amount of secret keys that can be generated using methods from ref. [29]. For a Sun-synchronous orbit and neglecting weather effects, the expected annual key for single overpass blocks with an OGS site situated at a particular latitude is approximated by[29]

$$\overline{\mathrm{SKL}}_{\mathrm{year}} = N_{\mathrm{orbits}}^{\mathrm{year}} \frac{\mathrm{SKL}_{\mathrm{int}}}{L_{\mathrm{lat}}}, \tag{3}$$

where $\mathrm{SKL}_{\mathrm{int}}$ is twice the integrated area under the SKL vs d_{min} curve in Fig. 5a (units of bit metres), $N_{\mathrm{orbits}}^{\mathrm{year}}$ is the number of orbits per year, and L_{lat} is the longitudinal circumference along the line of latitude at the OGS location. Figure 5b illustrates how $\overline{\mathrm{SKL}}_{\mathrm{year}}$ varies as a function of the memory buffer for an OGS at a latitude of 55.9° N (latitude of Glasgow). For our reference configuration (System D) with $\eta_{\mathrm{loss}}^{\mathrm{sys}} = 40$ dB, $\overline{\mathrm{SKL}}_{\mathrm{year}}$ is 0.81 Gb (3.94 Gb) for a memory buffer of 8 GB (32 GB), respectively. For comparison, without QRNG limitations, $\overline{\mathrm{SKL}}_{\mathrm{year}}$ is 6.44 Gb. Figure 5b also shows the gains to $\overline{\mathrm{SKL}}_{\mathrm{year}}$ from better performing sources and detectors. Comparing Systems B and C shows a crossover in their $\overline{\mathrm{SKL}}_{\mathrm{year}}$ at around 32 GB, highlighting a tradeoff between the operational performance of sources and receiver for fixed memory buffers. Namely, SatQKD systems operating with constrained memory buffers should focus on improving sources (minimising $QBER_I$, System C). This is because small memory buffers can only support a short signal transmission time around the maximum elevation of a satellite's trajectory, where losses are minimised. Improving the performance of the source leads to a direct improvement of $\overline{\mathrm{SKL}}_{\mathrm{year}}$. Conversely, SatQKD systems not constrained with memory buffers have a larger operational footprint that maximises the number of overpasses that generate non-zero finite keys. Improving the key generation of these systems can be supported through improved receivers with reduce p_{ec} (System B).

We note that a higher source rate, f_s, can improve the satellite overpass opportunities that generate a non-zero finite key and reduce the required memory storage. For the number of transmitted signals enabled by a limited memory buffer, a higher rate allows signal transmission over a shorter time window around θ_{max}, where the satellite-OGS range is at its smallest, corresponding to a lower average loss. This improves both the received block length and the overall error rate. Also, the minimum amount of buffer required to generate the secret key is reduced due to more efficient transmission during the lower loss segment of an overpass. To illustrate this, consider a zenith pass with time window of 444 s and a source with repetition rate of 100 MHz, which requires 22.2 GB of random bits. If the repetition rate is increased to 500 MHz, then the same data can be transmitted in 88.8 s, five times less. One can thus focus the transmission at higher elevation angles, which have less loss and lower errors. The raw data for the 500 MHz source leads to a greater amount of secret key. It follows that a 500 MHz source could generate the same key length as a 100 MHz source, using fewer pulses and therefore fewer random bits.

Source intensity uncertainties. Standard analyses of WCP decoy-state BB84 protocols usually assume perfect device operation leading to idealised key rates with optimised intensities. We can consider various deviations from ideality, such as a source with fixed and known intensities operational during the entire integration time of a satellite overpass. Active stabilisation of pulse intensities by continuous monitoring and feedback is possible[53] but may be limited by inherent power monitor measurement uncertainties. Instead, instantaneous offsets and long-term drifts in the intensity values lead to parameter uncertainties that depart from the fixed operating intensity assumption, which directly impacts the security of distilled finite keys for two reasons. First, source intensity uncertainties can be exploited in general attacks[54] which may be exacerbated in SatQKD with small block sizes. Second, the estimated vacuum and single-photon yields will differ significantly from true expectation values, potentially leading to an underestimation of the required privacy amplification to ensure security.

Several recent works have looked at this general problem by accounting for the uncertainties in source intensities directly within the parameter estimation[14,55–58]. This changes the estimates of the quantities that appear in Eq. (2) and could also

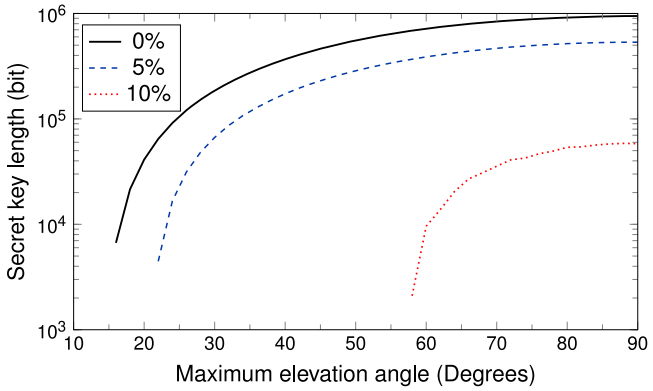

Fig. 6 Impact of source intensity uncertainty. The signal and decoy state intensity values may independently deviate from their assumed values μ_j by fraction f. The per-pass secret key length (SKL) taking into account these intensity uncertainties for $f = 0\%, 5\%, 10\%$ are shown for different overpass geometries.

change the secret key formula itself. A different scenario has also been considered[31] where the existing formalism described in refs. [29,42] is used, but where one assumes that the true intensities are uncertain, though not necessarily fluctuating during a transmission block. This uncertainty results either from measurement uncertainties in the power monitors or from drifts in the calibration settings. We note that in ref. [31] the channels did not vary in time during a transmission block, in contrast to the SatQKD case that we consider here.

In this work, as in ref. [31], we model the impact on the SKL of uncertainties in the source intensities, where we have an upper bound to on the possible deviations of μ_j from the assumed/measured values. Our approach models the case where the fixed intensity values have a constant and unknown offset from their intended values. The intensities can vary from the intended values by a maximum fraction f of the intended values during an overpass. The probability of the intensity values exceeding the range defined by f must be less than the advertised probability of the protocol being insecure, which is determined by ϵ_s. These uncertainties are considered separately for the signal and decoy states μ_1 and μ_2, respectively, but not for the vacuum state, since any deviations in the vacuum state due to extraneous counts have already been considered. Crucially, we consider independent uncertainties for μ_1 and μ_2 for all four encoded bit values. This is a more pessimistic approach than in related works, such as ref. [58], where it is assumed that the uncertainties for μ_j are the same for each bit value and basis. Each intensity value is then sampled independently in the range $\mu_j \pm f\mu_j$ to determine each signal state. Since the true intensity values are unknown to Bob, we take the worst-case combination of deviations that reduces the SKL as a conservative estimate while ensuring security. The range $\mu_j \pm f\mu_j$ is sampled using different numbers of points, though it was found that only 3 points were sufficient to find the worst-case SKL. Figure 6 illustrates the SKL as a function of $\theta_{\max}$ for at most a 5% and 10% uncertainty in the source intensities. To quantify this reduction, a 5% and 10% uncertainty in the source intensities reduces the annual SKL by a significant factor of 2 and 43, respectively. From this reduction, it is clear that source intensity uncertainties have a profound impact on the attainable SKL that significantly reduces the SatQKD operational footprint. For large uncertainties, it is therefore likely that the SKL will be zero for many of the satellite overpass opportunities. This highlights the importance of including the effects of uncertainties in the description of the power monitors. Active stabilisation of intensities in conjunction with high-accuracy power monitoring is crucial to allow operation close to the desired performance.

Discussion

Existing analyses of satellite-based QKD (SatQKD) assume an ideal, fully optimised parameter space to determine the maximum finite key rate. In practice, it is difficult to engineer the control of each parameter for different satellite overpasses. Therefore, these analyses effectively serve as an upper bound to the expected performance of SatQKD. We show that SatQKD operates with limited operating margins. It is therefore of immediate practical relevance to investigate the performance of SatQKD with a reduced parameter space optimisation to reflect restrictions on system operations and deployment, and to understand its robustness to additional losses and system imperfections. Further, the limited volumetric space, weight, and power (SWaP) available on small satellites provide limited physical resources that further depart from the ideal scenario of a fully optimised parameter space. We fill this gap by establishing practical SatQKD performance limits that reflect the nature of current engineering efforts and evaluate the impacts of limited resources on the long-term finite secret key length (SKL) generation capacity.

First, we model the impact of a fixed receiver basis bias P_X^B and pulse intensities μ_j on the SKL given the impracticality of their dynamic control during transmission. The SKL can be enhanced through carefully selecting the operating values of the fixed parameters. We develop a natural approach to determining the ideal fixed parameter values, based on maximising the expected annual SKL, which can be readily generalised to any parameter set. For the nominal system specifications denoted in Table 1, this leads to the fixed parameter set $\{P_X^B, \mu_1, \mu_2\} = \{0.84, 0.71, 0.14\}$, corresponding to the receiver beamsplitter basis bias, and signal and decoy state intensities. Despite these fixed values, we find it is possible to generate near-optimal SKLs across a wide range of overpass maximum elevation angles. While larger P_X^B can generate larger SKL at high elevations, it does so at the expense of zero secret key at lower elevations due to worse parameter estimation. SatQKD missions should therefore carefully choose the fixed OGS bias to address the tradeoff between a maximised single-pass SKL and the long-term key generation capacity. Our optimal fixed value of $P_X^B = 0.84$ balances this tradeoff to achieve close to optimal performance with fixed intensities. The optimum set of $\{P_X^B, \mu_1, \mu_2\}$ will require re-evaluation for different SatQKD systems, especially in a large-scale network with several OGSs and a heterogenous space segment. Further trade-offs will have to be considered to establish a set of standard system parameters based on operational and application-specific factors.

Next, we illustrate the significant impact of limited QRNG resources that drive the source on the expected annual SKL. For the nominal system, increasing the memory buffer from 8 GB to 32 GB substantially increases the expected total annual SKL from 0.81 Gb to 3.94 Gb, corresponding to 3.16×10^6 and 1.54×10^7 AES-256 encryption keys, respectively, though there are diminishing returns for larger buffers. This insight has significant implications for design trade-offs. We provide the minimum memory buffer required to yield non-zero finite keys for different overpass geometries, providing a benchmark to support the design of upcoming SatQKD missions. For missions with higher altitudes and source rates, the QRNG subsystem for prepare-and-measure protocols will be increasingly crucial for sustained operations. High-speed QRNGs with sufficient rate for real-time driving of the source, together with ring-buffers and real-time reconciliation would obviate the need for extremely large random number stores, but will have further system design implications for SWaP-C and required communications capabilities.

Finally, we investigate the impact of uncertainties in the signal and decoy state intensities on the SKL. Maintaining fixed

intensity values require perfect sources during the entire integration time of a satellite overpass. In practice, imperfect knowledge of the transmitted state intensities directly impact the security and amount of distilled finite keys whilst maintaining security. We find that these uncertainties have a profound impact on the SKL and highlight the importance of the accuracy of power monitors. Actively stabilising the intensities close to their intended values is also crucial to approach the optimal performances as modelled.

This study opens up a number of interesting open problems that would extend the scope and applicability of this work. First, a more comprehensive quantum channel model that includes elevation and azimuthal-dependent background light distributions, cloud cover, seasonal weather effects, and other location-dependent effects would provide a more representative performance analysis for detailed OGS siting studies. Second, different orbits and altitudes could also be modelled, the optimum altitude to maximise the integrated key generation footprint, hence its expected annual SKL, could be derived in particular. Third, implementing error correction and privacy amplification can be demanding for SatQKD. While these steps do not have to occur during the quantum transmission phase (the limited overpass time and quantum optical channel is the main bottleneck we consider in this work), modelling any inefficiencies would warrant an analysis in its own right. In particular, exploring the impact of limited resources to efficiently implement and measure error syndromes could impact the security and correctness of finite keys. Finally, an interesting extension toward the aim of establishing a global quantum network would be in exploring additional cost and performance trade-offs to reveal deeper insights into performance bottlenecks in SatQKD.

Methods

Loss modelling. In this section, we introduce the notation and the underlying loss model. In particular, we provide details on our model for the elevation and wavelength-dependent losses for any satellite overpass geometry. Recall that to determine the finite key, we need to determine the expected detector count statistics as a function of time and the operational source wavelength λ. Therefore, we first determine the instantaneous link efficiency as a function of elevation $\theta(t)$, range $R(t)$, and source wavelength λ, which captures all systematic and channel losses. Our method to determine the link efficiency differs from our approach in ref. [29] where we used empirical results published by Micius. In this work, we use a more physically motivated approach that will allow greater flexibility in the analysis and applications that can be considered, such as the effects of OGS positioning. Despite this change, the results of the two methods closely match for elevations above 10° which provides confidence in the new approach.

We write the link efficiency as

$$\eta_\lambda(\theta) = \eta_{\text{diff}}(\lambda,\theta) + \eta_{\text{atm}}(\lambda,\theta) + \eta_{\text{int}}, \tag{4}$$

in units of decibels (dB) and where we have three distinct loss contributors. The first term η_{diff} defines losses from diffraction effects, η_{atm} from atmosphere effects that include scattering and absorption, and η_{int} defines a fixed elevation-independent intrinsic system efficiency corresponding to internal losses, and beam misalignment. Eq. (4) provides a general approach to modelling losses for any SatQKD system. Once a satellite overpass trajectory is defined, we use Eq. (4) to determine the loss for every second of the overpass to estimate the total count statistics. A single block is then constructed from the entire overpass data, and finite statistics incorporated to maintain composable security. An illustration of each loss contributor is provided in Fig. 7, with details for each loss contributor provided below.

Diffraction losses. A dominant contribution to loss is diffraction, which broadens the beam after the signal propagates through the satellite's transmitter aperture, T_X. The amount of beam broadening depends on a number of factors, including the channel range $R(t)$, T_X, and the source wavelength λ. Here, we take a standard approach to estimate diffraction losses by calculating the far-field Fraunhofer diffraction of a initial truncated Gaussian field distribution with a beam waist of w_0 at the transmission aperture. We calculate the probability that a single photon exiting the transmit aperture is collected by the receiver aperture from the ratio of the integrated power density across the transmitter aperture, P_T, and the receiver aperture, P_R,

$$\eta_{\text{diff}}(\lambda,\theta) = -10\log_{10}\left(\frac{P_R}{P_T}\right). \tag{5}$$

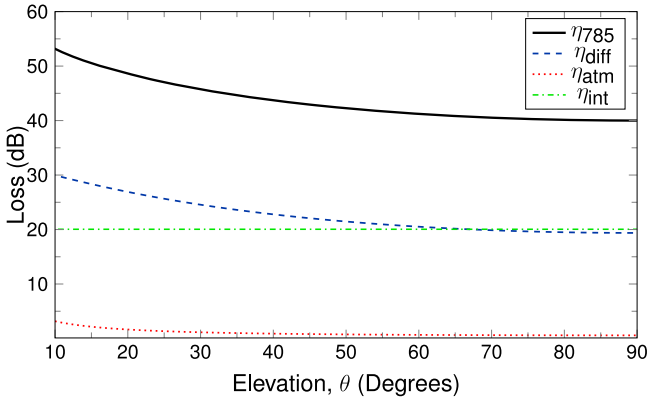

Fig. 7 Link efficiency as a function of elevation. Each contributor to the total loss is illustrated for $\lambda = 785$ nm. Both diffraction and atmospheric losses vary with elevation and increase with decreasing elevations. The solid black line illustrates the total link efficiency. The loss axis is truncated at 60 dB, with the worst link efficiency being $\eta_{785} = 87$ dB at 0°. The loss values in the grey region, where the elevation falls below 10° are not used in the key length simulations.

Since we are using a weak coherent pulse (WCP), there is no optimal beam waist provided there is no constraint on beam power[33]. For a downlink configuration with a WCP source, it is optimal to have the beam waist be as large as possible to achieve close to ideal far-field diffraction. However, practical constraints on the source power will impose a limit to flatness of the Gaussian across the transmission aperture. Therefore, we set the beam waist to be in the order of the transmitter aperture diameter, $w_0 = T_X/2$. The impact of a central beam obscuration due to secondary mirrors typical of Cassegrain-type reflecting telescopes could be considered[33] but has no significant impact on the analysis.

Atmospheric attenuation. The second contributor to the instantaneous link efficiency arises from atmospheric attenuation from absorption and scattering from molecules and particulate matter. The magnitude of these atmospheric losses depends on the wavelength and the satellite's elevation, which determines the length of the quantum channel through the atmosphere. We use MODTRAN to model atmospheric propagation and determine the transmissivity, $T_\lambda(\theta)$, for a given wavelength as a function of elevation. MODTRAN is a software that solves the radiative transfer equation to provide a standard atmospheric band model[32].

The atmospheric loss contribution is then calculated from the transmissivity,

$$\eta_{\text{atm}}(\lambda,\theta) = -10\log_{10}\left(T_\lambda(\theta)\right), \tag{6}$$

where the wavelength and elevation dependence is made clear.

'Intrinsic' system loss. The final loss contributor is denoted the 'intrinsic' system loss η_{int} that combines several sources. We simplify the analysis by taking this to be fixed, i.e. elevation/time independent. Within our loss budget, the intrinsic system loss combines two distinct loss contributors. First, we conservatively assign a fixed loss of 12 dB to the overall electro-optical inefficiency of the OGS system, which is comprised of 3 dB each from,

1. photon detection efficiency Si-SPAD,
2. quantum receiver optics,
3. collection telescope,
4. interface and adaptive/tip-tilt optics between telescope and quantum receiver.

We also lump together losses due to an imperfect, non-diffraction limited, beam (beam quality parameter $M^2 > 1$), turbulence induce beam wander and spreading, and transmitter pointing errors. For simplicity, we assign a fixed and conservative value of 8 dB to such non-ideal beam propagation induced losses. Therefore, in this work, we set

$$\eta_{\text{int}} = 20.0\,\text{dB}, \tag{7}$$

which brings the total minimum loss at zenith to $\eta_{\text{loss}}^{\text{sys}} = 40$ dB. Elevation dependence of the turbulence-induced losses has been considered in other works but is neglected for the moment in this work. More detailed modelling of turbulence and pointing losses can be found in ref. [59] and references therein. Underestimation of these losses is compensated in part by conservative estimates made elsewhere in η_{int}.

Note that these are conservative estimates that may be more indicative of practical SatQKD systems. If we are able to engineer better performances and achieve highly optimised operation, then we can further reduce the receiver and transmitter apertures for increased portability, while maintaining the values of $\eta_{\text{loss}}^{\text{sys}}$

analysed here. These losses are consistent with the recent mobile OGS designed for the Micius mission[60].

The protocol and secret key length optimsation. In this section, we detail how to calculate the secret key length (SKL) and the optimisations considered in this work. The SKL achieved with the efficient BB84 protocol from a single overpass is calculated taking into account finite block size effects.

The BB84 protocol. The QKD protocol we investigate is efficient Bennett-Brassard (BB84) with two decoy states, i.e. three different pulse intensities[19,38,42–45]. In this protocol, the transmitter (Alice) and the receiver (Bob) encode bits within one of two polarisation bases, denoted X and Z. We adopt the convention that the X basis is used for key bits, while the Z-basis is used to detect an eavesdropper through the phase error rate. Alice prepares bits in the X-basis with probability P_{X}^{A}, while Bob measures within the X-basis with probability P_{X}^{B}. It is standard to take $P_{\mathsf{X}}^{A}=P_{\mathsf{X}}^{B}=P_{\mathsf{X}}$, however, in general it is possible that $P_{\mathsf{X}}^{A}\neq P_{\mathsf{X}}^{B}$, particularly if one probability is fixed due to practical considerations[31]. We consider phase-randomised coherent pulses where the intensity (mean photon number) $\mu_k\in\{\mu_1,\mu_2,\mu_3\}$ is randomly chosen with probability p_{μ_k}. There are alternative carriers to phase-randomised coherent pulses. True single-photon sources could be considered[61–64], amongst others[1], though these are at a much lower stage of maturity, for terrestrial or space applications, compared with WCP sources.

After the quantum signals are transmitted from Alice to Bob, they perform a standard reconciliation procedure to correlate detection events with transmitted pulses, basis matching, intensity announcement, and parameter estimation. Only the bits in the X-basis are used for the key, while the Z-basis bits are made public. The raw key is formed by performing error correction on the X-basis bits, which necessitates the public exchange of λ_{EC} bits in the information reconciliation phase. In practice, the value of λ_{EC} is known from the error correction communication, but for the purposes of modelling we use an estimate that varies with the block size, quantum bit error rate, and the required correctness parameter[47]. This estimate generates suitable values for the error correction efficiency for SatQKD data representative of current engineering efforts and capabilities (see Methods 'Error correction for one-way information reconciliation' for a detailed discussion and demonstration). The results for the Z-basis are used to estimate parameters such as the number of bits from vacuum events, $s_{\mathsf{X},0}$, the number of bits from single photon events $s_{\mathsf{X},1}$, and the phase error ϕ_{X}. The exact formulas for these terms are provided in ref. [29], which is based on refs. [19,42]. After privacy amplification, the final SKL, ℓ, is given by Eq. (2):

$$\ell=\left\lfloor s_{\mathsf{X},0}+s_{\mathsf{X},1}(1-h(\phi_{\mathsf{X}}))-\lambda_{\mathrm{EC}}-6\log_2\frac{21}{\epsilon_{\mathrm{s}}}-\log_2\frac{2}{\epsilon_{\mathrm{c}}}\right\rfloor,$$

where $h(x)=-x\log_2(x)-(1-x)\log_2(1-x)$ is the binary entropy function, and ϵ_{s} and ϵ_{c} are the composable security and correctness parameters, respectively[42,46].

We can maximise the SKL by optimising over the protocol parameters p_k, μ_k, and P_{X} for a given satellite-OGS overpass, system link efficiency, and system configuration (as in Table 1). The value of μ_3 is set to vacuum since this helps with the estimate of the vacuum counts, $s_{\mathsf{X},0}$[42]. The transmission time window from which the finite block is constructed is an additional optimisation parameter to maximise the achievable finite key[29]. This is because, under finite-size security analysis, higher QBER increases the minimum raw key length necessary for non-zero key length extraction due to less efficient reconciliation and post-processing overheads. However, taking the largest block size permitted by a satellite overpass is sometimes not the best strategy. This is since data from lower elevations have both smaller count rates and higher signal QBER, which increases the average channel QBER and may offset any improvements to the SKL from larger block sizes. We define the processing block transmission time window to run from $-\Delta t$ to $+\Delta t$, such that the total transmission time is $2\Delta t$ with $t=0$ corresponding to the time of highest elevation $\theta_{\max}$. The SKL in Eq. (2) is additionally optimised over discretised values for Δt, and the value for Δt chosen that yields the largest SKL. This full optimisation is performed in version 1.1 of the Satellite Quantum Modelling and Analysis (SatQuMA) software[30]. For more details on the software and the numerical optimisation, see refs. [29,30].

This fully optimised scenario yields an upper bound to SatQKD performance. In practice, these bounds may be difficult to achieve due to constraints and trade-offs in the mission design and operation. In the following Methods section 'Practical optimisation of the secret key length', we provide an overview of modifications to the optimisation problem with constraints that closely reflect operational considerations for the derivation of realistic performance bounds.

Practical optimisation of the secret key length. The original protocol parameter optimisation problem is modified to handle different numerical investigations. Though classical communication constraints are important for SatQKD operations, we do not consider these limitations (see ref. [29] for a brief discussion). First, subsection 'Source rate' of Results introduces the source-rate normalised SKL to illustrate the impact of finite-key effects on the SKL and to provide an informed decision on the source rate to consider for the remainder of the work. Second, subsection 'Impact of parameter fixing' of Results fixes the values of the signal intensity μ_1, decoy intensity μ_2, and the receiver basis bias P_{X}^{B}, since it may not be practical to change these parameters on a pass-by-pass basis in an operational system. The transmitter and receiver basis biases are allowed to differ, i.e. $P_{\mathsf{X}}^{A}\neq P_{\mathsf{X}}^{B}$, to model a fixed OGS basis bias and adjustable transmitter bias. The SKL is then maximised over the remaining protocol parameter space defined by the set $\{P_{\mathsf{X}}^{A},p_{\mu_1},p_{\mu_2},\Delta t\}$. The fixed values for P_{X}^{B}, μ_1, and μ_2 are set to those that maximise the expected annual SKL through a procedure detailed in Methods ('General approach optimisation of fixed parameter values'). Third, subsection 'QRNG subsystem limitations' of Results explores the impact of QRNG subsystem limitations that may constrain the number of signals that can be transmitted during an overpass. This is modelled using a finite-sized onboard random number memory store, corresponding to an associated transmission cutoff time, from which we determine the reduction in long-term average key generation rate. We also determine the minimum memory buffer required to generate non-zero SKL. Finally, in subsection 'Source intensity uncertainties' of Results, we consider the effect of pulse intensity uncertainties on the secure key that can be extracted taking into account reduced intensity knowledge. For this, the signal and decoy state intensities are sampled between a range that depends on the uncertainty percentage of the intended intensity values.

Error correction for one-way information reconciliation. An important step for any QKD protocol is error correction, which identifies and corrects errors due to vacuum events and transmission errors. For this step, Alice and Bob publicly announce λ_{EC} bits that are assumed known to Eve through a round of classical communication. The number of bits λ_{EC} depends on the error rate, which is a practical implementation we estimate during the parameter estimation stage. For our simulation, we use an estimate of λ_{EC} that varies with the quantum bit error rate (QBER), Q, and the data block size, n_{X}. A common approach to modelling the number of error correction bits required during information reconciliation is through $f_{\mathrm{EC}}n_{\mathsf{X}}h(Q)$, where f_{EC} is the reconciliation factor efficiency and we recall that $h(x)$ is the binary entropy function. The value for f_{EC} is crucially larger than unity, and often chosen within the range 1.05 to 1.2, to account for inefficiencies in the error correction protocol. While this approach is well-suited to determining the optimal secret key length, it is assumed that the reconciliation factor efficiency is independent of Q, n_{X}, and the required correctness ϵ_{c}. Since SatQKD operates within the finite-key regime, these parameters can vary significantly, however. An improved estimate of the reconciliation factor efficiency would enable a higher SKL under finite statistics.

The amount of information leaked to the eavesdropper during information reconciliation is usually impossible to determine exactly. Therefore it is often upper bounded by $\log|\mathcal{M}|$, where $\mathcal{M}$ denotes the error syndrome. For one-way reconciliation, the size of this error syndrome (in bits) has the following tight lower bound[47]

$$\begin{aligned}\lambda_{\mathrm{EC}}=&\,n_{\mathsf{X}}h(Q)+n_{\mathsf{X}}(1-Q)\log\left[\frac{(1-Q)}{Q}\right]\\&-\left(F^{-1}(\epsilon_{\mathrm{c}};n_{\mathsf{X}},1-Q,)-1\right)\log\left[\frac{(1-Q)}{Q}\right]\\&-\frac{1}{2}\log(n_{\mathsf{X}})-\log(1/\epsilon_{\mathrm{c}}),\end{aligned}\tag{8}$$

where F^{-1} is the inverse of the cumulative distribution function of the binomial distribution. We use this estimate for the number of error correction bits to determine the optimised SKL. We note that for large block sizes

$$\lim_{n_{\mathsf{X}}\to\infty}\frac{\lambda_{\mathrm{EC}}}{n_{\mathsf{X}}}=h(Q),\tag{9}$$

such that $\lambda_{\mathrm{EC}}^{\infty}=n_{\mathsf{X}}h(Q)$, which is the minimum possible bits allowed by information theory. This suggests that the information reconciliation (IR) factor efficiency tends towards unity $f_{\mathrm{EC}}=1$, which is optimistic even for optimised low-density parity-check (LDPC) codes that can achieve high reconciliation efficiencies and require few rounds of communications[65]. For application in SatQKD, the IR efficiency does not approach this asymptotic limit over QBERs and data block sizes typical of realistic operation. To demonstrate this, we investigate how the IR efficiency estimate varies for the different memory buffers considered in the 'QRNG subsystem limitations' subsection in Results. Specifically, the finite-size estimate for the IR efficiency provided by Eq. (8) can be determined from the ratio $f_{\mathrm{EC}}^{\mathrm{est}}=\lambda_{\mathrm{EC}}/n_{\mathsf{X}}h(Q)$. Figure 8 illustrates this ratio as a function of satellite overpasses with maximum elevation angle $\theta_{\max}$ for different memory buffers m_b. Note that the data block sizes increase with an increasing memory buffer, leading to better $f_{\mathrm{EC}}^{\mathrm{est}}$ that approaches unity. We observe that the estimated efficiency dips below the lower quoted value of 1.05 in the literature[47], which is indicated by the grey region. Recall from the 'QRNG subsystem limitations' subsection in Results, that a memory buffer of 64 GB achieves near-optimal performance corresponding to the highly optimised scenario. Therefore, the correction estimate in Eq. (9) does not approach the asymptotic limit of unit efficiency for SatQKD data representative of current engineering efforts and capabilities and is well-suited to explore the engineering constraints that are the focus in this work.

Before concluding, we make two observations. First, a simple remedy to the error correction estimate that would hold for any data block size would be to switch to an updated model whenever the reconciliation efficiency estimated by Eq. (9) falls below 1.05. That is, we can estimate the number of error correction bits required from

$$\lambda_{\mathrm{EC}}^{\mathrm{new}}=f_{\mathrm{EC}}n_{\mathsf{X}}h(Q),\tag{10}$$

where f_{EC} takes values that reflect achievable efficiencies, whenever

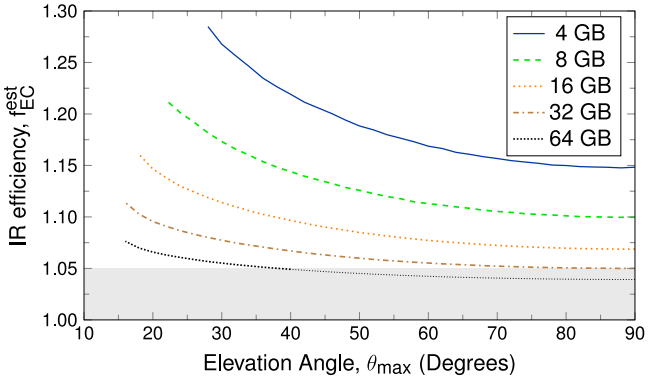

Fig. 8 One-way information reconciliation (IR) efficiency. We estimate f_{EC}^{est} as a function of satellite overpasses with maximum elevation angle θ_{max} for different memory buffers m_b. For data representative of current engineering efforts, f_{EC}^{est} remains larger than 1.05, which is the lowest quoted achievable efficiency in the literature and is illustrated by the grey region corresponding to optimistic efficiencies.

$\lambda_{EC} < 1.05 n_X h(Q)$. Second, here we do not consider bi-directional error correction information reconciliation for SatQKD such as CASCADE[66]. Although it may lead to improved reconciliation efficiencies, the complexity of classical communication protocols and operations, and demands for on-board data processing are significantly greater. Hence, it may be more practical to implement one-way IR in SatQKD to simplify operations and reduce system cost and complexity using schemes such as low-density parity check (LDPC) codes[67].

General approach to optimisation of fixed parameter values. The fully optimised finite SKL is difficult to achieve since it requires active control of the entire parameter space, which may be difficult to engineer. In the 'Impact of parameter fixing' subsection of Results, we explored the impact of fixing the receiver basis bias P_X^B, and the two intensity values μ_1 and μ_2 that are particularly challenging to change. This naturally raises the question *what fixed values should a SatQKD system implement*? Here, we outline a general method to determine fixed values for the set $\mathcal{F} \in \{P_X^B, \mu_1, \mu_2\}$.

Our method follows from maximising $\overline{\text{SKL}}_{\text{year}}$, which is proportional to the integrated area under the SKL vs ground track distance curves, SKL_{int}[29]. We first establish the fully optimised SKL as a function of d_{min}, corresponding to optimising the full parameter space. For each point j along the optimised curve, we extract the set, $\mathcal{F}^{\text{opt}}_{d_{\text{min}}(j)}$, of the optimal values for P_X^B, μ_1, and μ_2 for $d_{\text{min}}(j)$ (in units of 10^6 m). Now fixing $\mathcal{F}^{\text{opt}}_{d_{\text{min}}(j)}$, we optimise the SKL over the remaining parameter space to determine the SKL as a function $d_{\text{min}}(j)$, hence SKL_{int}. This procedure is repeated for each optimised point j. We then choose the fixed set $\mathcal{F}^{\text{opt}}_{d_{\text{min}}(k)}$ that maximises SKL_{int} as the best compromise of fixed parameters. This procedure is summarised in Fig. 9.

Algorithm 1 $\mathcal{F}^{\text{opt}}_{d_{\min}(k)} = \text{FIXED\_OPTIMAL\_PARAMETERS}\ (\{\mathcal{F}^{\text{opt}}_{d_{\min}(j)}\})$

$C_1 \leftarrow 0 < P_X^A < 1$
$C_{2,3} \leftarrow 0 < p_j < 1$ for $j = 1, 2$
$f_s \leftarrow 500$ MHz
$\text{QBER}_I \leftarrow 0.5\%$
$p_{ec} \leftarrow 10^{-7}$
$t(\theta) \leftarrow$ time when satellite at elevation θ
annualSKL $\leftarrow \mathbf{0}$ (vector of length $\{\mathcal{F}^{\text{opt}}_{d_{\min}(j)}\}$)

for all $j = 1$ to $\text{len}(\{\mathcal{F}^{\text{opt}}_{d_{\min}(j)}\})$ **do**
  $\mathcal{F}_{d_{\min}(j)} = \{P_X^B(j), \mu_1(j), \mu_2(j)\} \leftarrow$ optimal values $\mathcal{F}^{\text{opt}}_{d_{\min}(j)}$
  $\xi_{\max}(j) \leftarrow$ max offset with non-zero key for set $\mathcal{F}_{d_{\min}(j)}$ with $\theta_{\max} \geq 10^\circ$
  $\boldsymbol{v} \leftarrow \mathbf{0}$ (vector of zeros such that $\text{len}(\boldsymbol{v}) = \xi_{\max}(j)$)

  for all $\xi = 0$ to $\xi_{\max}(j)$ **do**
    for all $\Delta t = 0$ to $t(10^\circ)$ **do**

—Determine max SKL for overpass ξ—

      $\ell[\xi, \mathcal{F}_{d_{\min}(j)}, \Delta t] \leftarrow$ Finite SKL Eq. (2)
      Max $\ell[\xi, \mathcal{F}_{d_{\min}(j)}, \Delta t]$ subject to constraints $\{C_1, C_2, C_3\}$
    $v_\xi \leftarrow \{\xi, \max_{\Delta t} \ell[\xi, \mathcal{F}_{d_{\min}(j)}, \Delta t]\}$ ▷ List for plots
  $\text{annualSKL}_j \leftarrow \int_0^{\xi_{\max}(j)} d\xi\ \max_{\Delta t} \ell[\xi, \mathcal{F}_{d_{\min}(j)}, \Delta t]$

—Find the (annual) optimal fixed point $\mathcal{F}^{opt}_{d_{min}(k)}$—

$\text{annualSKL}_k \leftarrow \text{Max}\{\text{annualSKL}_j\}$
$\mathcal{F}^{\text{opt}}_{d_{\min}(k)} \leftarrow \{P_X^B(k), \mu_1(k), \mu_2(k)\}$ ▷ Optimal parameter choice
Return $\mathcal{F}^{\text{opt}}_{d_{\min}(k)}$

Fig. 9 Pseudocode to determine the ideal fixed parameter set. We denote $\mathcal{F}^{\text{opt}}_{d_{\min}(k)} = \{P_X^B(k), \mu_1(k), \mu_2(k)\}$ as that which maximises the performance of a SatQKD system through the expected annual SKL, which is determined from the parameter set $\mathcal{F}^{\text{opt}}_{d_{\min}(j)}$ that are sampled from the fully optimised SKL vs d_{min} plot. The list ν_ξ is used to generate the plots in this work. This algorithm can be generalised to determining the ideal values for any fixed parameter set.

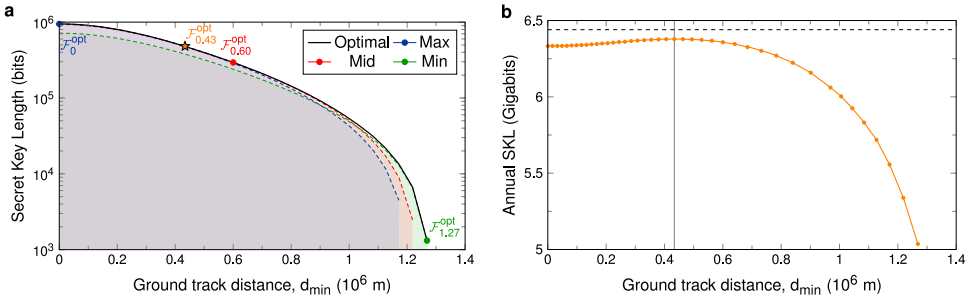

Fig. 10 SKL vs $d_{\min}$ for fixed $\mathcal{F}$. a The fully optimised SKL is illustrated in black, with each fixed point j along the optimal curve generating the set $\mathcal{F}^{\text{opt}}_{d_{\min}(j)}$, corresponding to the optimal fixed parameter values at ground track distance $d_{\min}(j)$ (in units of 10^6 m). The SKL for three illustrative fixed sets, $\mathcal{F}^{\text{opt}}_0$, $\mathcal{F}^{\text{opt}}_{0.60}$, and $\mathcal{F}^{\text{opt}}_{1.27}$, are optimised over the remaining parameter space with their corresponding areas shaded to determine the expected annual SKL. The ideal fixed data set is highlighted with an orange star at $d_{\min} = 0.43 \times 10^6$ m. **b** Variation in the expected annual SKL for each fixed set $\mathcal{F}^{\text{opt}}_{d_{\min}(j)}$. The vertical solid line corresponds to the parameter set that maximises the estimated annual SKL and the horizontal dashed line to the annual SKL with no constraints.

Figure 10 illustrates this procedure for choosing the ideal fixed set $\mathcal{F}^{\text{opt}}_{d_{\min}(k)}$ that optimises $\overline{\text{SKL}}_{\text{year}}$. In Fig. 10a, the optimal SKL is illustrated in black. Three illustrative fixed sets $\mathcal{F}_{d_{\min}(j)}$ are sampled to correspond to the maximum, median, and minimum non-zero SKLs values and are shown in dashed blue, dashed red, and dashed green, respectively. We first note that fixing the values for $\mathcal{F}$ has little impact on the SKL over the entire range of satellite overpass trajectories. This reassuringly demonstrates that SatQKD systems operating with a fixed subset of parameters $\mathcal{F}$ do not lead to a large departure from the optimal performance with only a small observed impact on the SKL generation performance. Second, it is possible to improve the SKL by carefully choosing the fixed values for $\mathcal{F}$. The ground track distanced furthest away from the sampled point j along the optimal curve deviates most from the optimal performance. This suggests that the fixed parameter set should be chosen closer to the centre of the curve, since this would maximise the robustness of the SatQKD systems to the widest variety of satellite overpasses leading to the largest annual expected SKL. This specific dependence on the fixed parameter set and the annual SKL is illustrated in Fig. 10b. The peak annual SKL corresponds to the ideal fixed set $\mathcal{F}^{\text{opt}}_{0.43} = \{0.841, 0.709, 0.139\}$. This establishes the fixed values used in the 'Impact of parameter fixing' subsection in Results. Our method is general and can be extended to determining the ideal values for any alternative subset of fixed parameter sets. Finally, we reassuringly find that despite the constrained parameter space, the estimated annual SKL with these fixed parameters is close to the fully optimised case, shown with the dashed horizontal line in (b).

We note that there is the possibility that a greater $\overline{\text{SKL}}_{\text{year}}$ could be achieved with a parameter set outside of the per-pass optima but as the presented procedure closely approaches the upper bound, a search for such values may not be worthwhile.

Data availability

The raw output files generated from simulations and used to generate display items in this work are archived at https://doi.org/10.5281/zenodo.8101679. All additional material requests should be made to J.S.S.

Code availability

The SatQuMA v1.1 simulation Python suite is available at ref. [30]. Modified code used to generate all results in this work is accessible on GitHub https://github.com/cnqo-qcomms/SatQuMA/. It implements a minor modification of SatQuMA v1.1 to handle fixed parameters that have currently not been released as a stand-alone package.

Received: 31 January 2023; Accepted: 5 July 2023;
Published online: 10 August 2023

References

1. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012–1236 (2020).
2. Sidhu, J. S. et al. Advances in space quantum communications. *IET Quantum Commun.* **2**, 182–217 (2021).
3. Liorni, C., Kampermann, H. & Bruß, D. Quantum repeaters in space. *New J. Phys.* **23**, 053021 (2021).
4. Wallnöfer, J. et al. Simulating quantum repeater strategies for multiple satellites. *Commun. Phys.* **5**, 169 (2022).
5. Yimsiriwattana, A. & Lomonaco Jr, S. J. in *Quantum Information and Computation II* (eds Donkor, E., Pirich, A. R. & Brandt, H. E. eds.), Vol. 5436, 360–372 (SPIE, 2004).
6. Van Meter, R. & Devitt, S. J. The path to scalable distributed quantum computing. *Computer* **49**, 31–42 (2016).
7. Giovannetti, V., Lloyd, S. & Maccone, L. Advances in quantum metrology. *Nat. Photon.* **5**, 222–229 (2011).
8. Sidhu, J. S. & Kok, P. Quantum metrology of spatial deformation using arrays of classical and quantum light emitters. *Phys. Rev. A* **95**, 063829 (2017).
9. Sidhu, J. S. & Kok, P. Quantum Fisher information for general spatial deformations of quantum emitters. Preprint at https://arxiv.org/abs/1802.01601 (2018).
10. Moreau, P.-A., Toninelli, E., Gregory, T. & Padgett, M. J. Imaging with quantum states of light. *Nat. Rev. Phys.* **1**, 367–380 (2019).
11. Sidhu, J. S. & Kok, P. Geometric perspective on quantum parameter estimation. *AVS Quantum Sci.* **2**, 014701 (2020).
12. Polino, E., Valeri, M., Spagnolo, N. & Sciarrino, F. Photonic quantum metrology. *AVS Quantum Sci.* **2**, 024703 (2020).
13. Sidhu, J. S., Ouyang, Y., Campbell, E. T. & Kok, P. Tight bounds on the simultaneous estimation of incompatible parameters. *Phys. Rev. X* **11**, 011028 (2021).
14. Liao, S.-K. et al. Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47 (2017).
15. Yin, J. et al. Satellite-based entanglement distribution over 1200 kilometers. *Science* **356**, 1140–1144 (2017).
16. Kerstel, E. et al. Nanobob: a CubeSat mission concept for quantum communication experiments in an uplink configuration. *EPJ Quant. Technol.* **5**, 6 (2018).
17. Mazzarella, L. et al. QUARC: quantum Research Cubesat—a constellation for quantum communication. *Cryptography* **4**, 7 (2020).
18. Villar, A. et al. Entanglement demonstration on board a nano-satellite. *Optica* **7**, 734–737 (2020).
19. Yin, J. et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature* **582**, 501–505 (2020).
20. Gündoğan, M. et al. Proposal for space-borne quantum memories for global quantum networking. *npj Quantum Inf.* **7**, 128 (2021).
21. Belenchia, A. et al. Quantum physics in space. *Phys. Rep.* **951**, 1–70 (2022).
22. Gündoğan, M. et al. Topical white paper: a case for quantum memories in space. Preprint at https://arxiv.org/abs/2111.09595 (2021).
23. Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: a vision for the road ahead. *Science* **362**, eaam9288 (2018).
24. Jianwei, P. Progress of the quantum experiment science satellite (QUESS) Micius project. *Chin. J. Space Science* **38**, 604–609 (2018).
25. Lu, C.-Y., Cao, Y., Peng, C.-Z. & Pan, J.-W. Micius quantum experiments in space. *Rev. Mod. Phys.* **94**, 035001 (2022).
26. Islam, T. et al. Finite resource performance of small satellite-based quantum key distribution missions. Preprint at https://arxiv.org/abs/2204.12509 (2022).
27. Sidhu, J. S., Brougham, T., McArthur, D., Pousa, R. G. & Oi, D. K. L. in *Quantum Technology: Driving Commercialisation of an Enabling Science II* (eds. Padgett, M. J., Bongs, K., Fedrizzi, A. & Politi, A.), Vol. 11881, 1–8 (SPIE, 2021).
28. Sidhu, J. S., Brougham, T., McArthur, D., Pousa, R. G. & Oi, D. K. L. in *Quantum Computing, Communication, and Simulation III* (eds. Hemmer, P. R. & Migdall, A. L.) Vol. 12446, 124460M (International Society for Optics and Photonics, SPIE, 2023).
29. Sidhu, J. S., Brougham, T., McArthur, D., Pousa, R. G. & Oi, D. K. L. Finite key effects in satellite quantum key distribution. *npj Quantum Inf.* **8**, 18 (2022).

30. Sidhu, J. S., Brougham, T., McArthur, D., Pousa, R. G. & Oi, D. K. L. Satellite quantum modelling & analysis software version 1.1: documentation. Preprint at https://arxiv.org/abs/2109.01686 (2021).
31. Brougham, T. & Oi, D. K. L. Modelling efficient BB84 with applications for medium-range, terrestrial free-space QKD. *New J. Phys.* **24**, 075002 (2022).
32. Berk, A. et al. MODTRAN6: a major upgrade of the MODTRAN radiative transfer code. in *Proc. SPIE*, Vol. 9088, 6 (2014).
33. Bourgoin, J.-P. et al. A comprehensive design and performance analysis of low earth orbit satellite quantum communication. *New J. Phys.* **15**, 023006 (2013).
34. Usenko, V. C. et al. Entanglement of Gaussian states and the applicability to quantum key distribution over fading channels. *New J. Phys.* **14**, 093048 (2012).
35. Hosseinidehaj, N., Walk, N. & Ralph, T. C. Composable finite-size effects in free-space continuous-variable quantum-key-distribution systems. *Phys. Rev. A* **103**, 012605 (2021).
36. Colquhoun, C. D. et al. Responsive operations for key services (ROKS): a modular, low SWaP quantum communications payload. Preprint at https://arxiv.org/abs/2210.11285 (2022).
37. Podmore, H. et al. QKD terminal for Canada's Quantum Encryption and Science Satellite (QEYSSat). in *International Conference on Space Optics - ICSO 2020* (eds. Cugny, B., Sodnik, Z. & Karafolas, N.), Vol. 11852, 118520H (International Society for Optics and Photonics, SPIE, 2021).
38. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
39. Chen, Y. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589**, 214 (2021).
40. Zhang, Z., Zhao, Q., Razavi, M. & Ma, X. Improved key-rate bounds for practical decoy-state quantum-key-distribution systems. *Phys. Rev. A* **95**, 012333 (2017).
41. Toyoshima, M. et al. Polarization measurements through space-to-ground atmospheric propagation paths by using a highly polarized laser source in space. *Opt. Express* **17**, 22333–22340 (2009).
42. Lim, C. C. W., Curty, M., Walenta, N., Xu, F. & Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89**, 022307 (2014).
43. Lo, H.-K., Chau, H. F. & Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.* **18**, 133–165 (2005).
44. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
45. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
46. Renner, R. *Security of Quantum Key Distribution*. PhD thesis, Swiss Federal Institute of Technology, Zurich (2006).
47. Tomamichel, M., Martinez-Mateo, J., Pacher, C. & Elkouss, D. Fundamental finite key limits for one-way information reconciliation in quantum key distribution. *Quant. Inf. Proc.* **16**, 280 (2017).
48. Ceccarelli, F. et al. Recent advances and future perspectives of single-photon avalanche diodes for quantum photonics applications. *Adv. Quantum Technol.* **4**, 2000102 (2021).
49. Holzman, I. & Ivry, Y. Superconducting nanowires for single-photon detection: progress, challenges, and opportunities. *Adv. Quantum Technol.* **2**, 1800058 (2019).
50. Gryszka, K. From biased coin to any discrete distribution. *Period. Math. Hung.* **83**, 71–80 (2021).
51. Ma, X. et al. Quantum random number generation. *npj Quantum Inf.* **2**, 16021 (2016).
52. Quantis QRNG chips - ID Quantique. https://www.idquantique.com/random-number-generation/products/quantis-qrng-chips/. (2010).
53. Lucamarini, M. et al. Efficient decoy-state quantum key distribution with quantified security. *Opt. Express* **21**, 24550–24565 (2013).
54. Yoshino, K.-i et al. Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses. *npj Quant. Inf.* **4**, 8 (2018).
55. Wang, X.-B. Decoy-state quantum key distribution with large random errors of light intensity. *Phys. Rev. A* **75**, 052301 (2007).
56. Wang, X.-B., Peng, C.-Z., Zhang, J., Yang, L. & Pan, J.-W. General theory of decoy-state quantum cryptography with source errors. *Phys. Rev. A* **77**, 042311 (2008).
57. Hu, J.-Z. & Wang, X.-B. Reexamination of the decoy-state quantum key distribution with an unstable source. *Phys. Rev. A* **82**, 012331 (2010).
58. Wang, Y., Bao, W.-S., Zhou, C., Jiang, M.-S. & Li, H.-W. Tight finite-key analysis of a practical decoy-state quantum key distribution with unstable sources. *Phys. Rev. A* **94**, 032335 (2016).
59. Trinh, P. V. et al. Statistical verifications and deep-learning predictions for satellite-to-ground quantum atmospheric channels. *Commun. Phys.* **5**, 225 (2022).
60. Ren, J.-G. et al. Portable ground stations for space-to-ground quantum key distribution. Preprint at https://arxiv.org/abs/2205.13828 (2022).
61. Morrison, C. L. et al. Single-emitter quantum key distribution over 175 km of fibre with optimised finite key rates, *Nat. Commun.* **14**, 3573 (2023).
62. Al-Juboori, A. et al. Quantum key distribution using a quantum emitter in hexagonal boron nitride. Preprint at https://arxiv.org/abs/2302.06212 (2023).
63. Murtaza, G. et al. Efficient room-temperature molecular single-photon sources for quantum key distribution. *Opt. Express* **31**, 9437–9447 (2023).
64. Abasifard, M. et al. The ideal wavelength for daylight free-space quantum key distribution. Preprint at https://arxiv.org/abs/2303.02106 (2023).
65. Elkouss, D., Leverrier, A., Alleaume, R. & Boutros, J. J. Efficient reconciliation protocol for discrete-variable quantum key distribution. in *2009 IEEE International Symposium on Information Theory* 1879–1883 (2009).
66. Brassard, G. & Salvail, L. Secret-key reconciliation by public discussion. in *Advances in Cryptology-EUROCRYPT'93: Workshop on the Theory and Application of Cryptographic Techniques Lofthus, Norway, May 23–27, 1993 Proceedings 12*, 410–423 (Springer, 1994).
67. Johnson, J. S., Grimaila, M. R., Humphries, J. W. & Baumgartner, G. B. An analysis of error reconciliation protocols used in quantum key distribution systems. *J. Def. Model. Simul.* **12**, 217–227 (2015).

Acknowledgements

We acknowledge support from the UK NQTP and the EPSRC Quantum Technology Hub in Quantum Communications (grant: EP/T001011/1), and the EPSRC International Network in Space Quantum Technologies (grant: EP/W027011/1). We also acknowledge support from the UK Space Agency (NSTP3-FT-063, NSTP3-FT2-065, NSIP ROKS Payload Flight Model), the Innovate UK project ReFQ (Project number: 78161), Innovate UK project AirQKD (Project number: 45364), the Innovate UK project ViSatQT (Project number: 43037), EU QTSPACE (COST CA15220), and the EPSRC Research Excellence Award (REA) Studentship.

Author contributions

J.S.S. conceptualised the main ideas together with D.K.L.O., steered the direction of research, and wrote the initial draft. J.S.S., T.B., and D.M. wrote the initial version of the code (SatQuMA v1.1) that is openly available, with modifications made by J.S.S. and T.B. to obtain numerical results presented in this work. R.G.P. conducted background literature reviews. D.K.L.O. obtained funding and initiated the research. All authors contributed to selecting relevant literature, proofreading, and editing the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to Jasminder S. Sidhu.

Peer review information *Communications Physics* thanks Anton Trushechkin, Wei Li and the other, anonymous, reviewer(s) for their contribution to the peer review of this work.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.