Key generation analysis for satellite quantum key distribution

Jasminder S. Sidhu, Thomas Brougham, Duncan McArthur, Roberto G. Pousa, and Daniel K. L. Oi

SUPA Department of Physics, University of Strathclyde, Glasgow, G4 0NG, United Kingdom

ABSTRACT

Developing global quantum communication networks is integral to the realisation of the quantum internet, which is expected to impart a similar revolutionary impact on the technological landscape as the classical internet. Satellite-based quantum communications provides a practical route to global quantum networking. In this work, we model finite statistics to determine the finite secret key length generation in SatQKD systems that implement trusted-node downlink operation with weak coherent pulse sources. We optimise the finite key rate for different practical operations and determine the key generation footprints. Our work provides an essential guide for future satellite missions to establish performance benchmarks for both sources and detectors.

Keywords: Space quantum communications, satelite-based quantum key distribution, quantum networking, quantum internet, SatQuMA.

1. INTRODUCTION

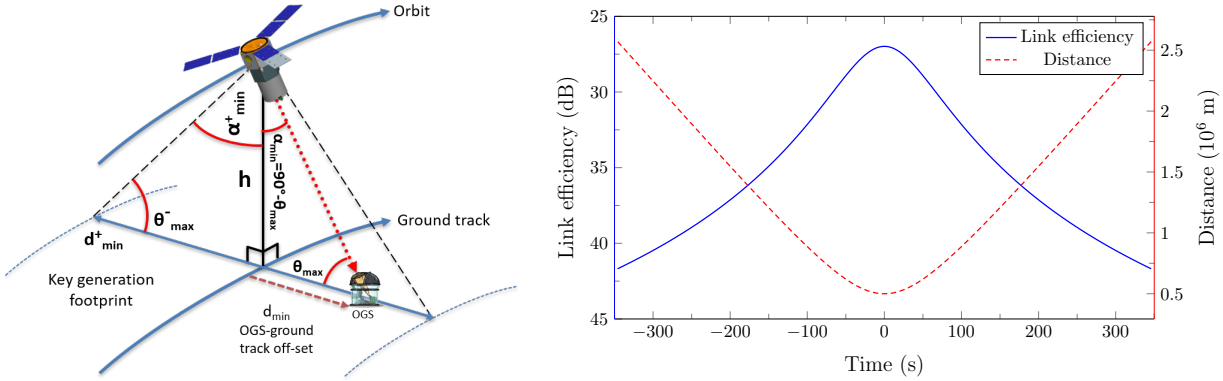
A fundamental difficulty in the vision of realising global quantum networking is the direct transmission range limitation of quantum resources.[1] Overcoming this limitation has driven extension efforts into realising quantum repeaters, which deliver limited improvements that fall short of global network requirements. Satellite-based quantum communication offers a more promising route to overcoming range limitations, and is quickly maturing into a necessary component to a future quantum internet,[2–6] following recent in-orbit demonstrations and feasibility studies by the Micius satellite.[7]

For satellite-based quantum key distribution (SatQKD) applications, an important limitation is the constrained time window to establish and maintain a quantum channel with an optical ground station (OGS), which constrains the amount of secret key that can be generated. In this regime of finite data sizes, statistical uncertainties in estimated parameters become important and must be accounted for in security analyses of the final distilled secret key.[8–10] In addition, the trade-off between the proportion of signals sacrificed for parameter estimation and post-processing becomes increasingly important and further strains the finite key generation.[11,12] We develop SatQuMA, an open source software[13] that applies recently developed tight bounds and small block length analyses in QKD,[12,14] to determine the finite-block composable secure key length attainable in SatQKD operations.

We apply SatQuMA to determine the optimised finite-block secret key length (SKL) for weak coherent pulse efficient two-decoy state BB84 protocols. Our analysis can determine the optimal QKD protocol parameter regimes that aid in the design and implementation of SatQKD operations. Specifically, we determine the impact of different system link efficiencies, background counts, source quality, and overpass geometries on the distillable finite key and the key generation footprint. We also provide a simple estimation method to determine the maximum expected long-term key volume at a particular OGS latitude. Our model and analysis may guide the design and specification of SatQKD systems, highlighting factors that limit secret key generation in the regime of high channel loss and limited pass duration.

We start with a background for the system model in Section 2, where we introduce our numerical toolkit to determine the optimised finite key length for SatQKD operations. We then details results in section 3, before concluding and summarising our results in Section 4.

Further author information: (Send correspondence to J. S.)
J. S.: E-mail: jasminder.sidhu@strath.ac.uk



(a) Orbital geometry (b) Link efficiency curve

Figure 1. **System configuration**. The overpass geometry for a satellite in a circular sun synchronous orbit at altitude h is shown in (a). When the satellite reaches a maximum elevation $\theta_{\max}$, its ground track passes the OGS with a minimum distance of $d_{\min}$. The smallest elevation for which a finite key can be generated is denoted $\theta^{-}_{\max}$, and defines the operational footprint of the SatQKD system. The link efficiency with satellite-OGS range in (b) illustrates the dynamic change to the overall link efficiency due to changes in diffraction and turbulence effects given varying atmospheric optical depths. The link efficiency peak, $\eta^{\text{sys}}_{\text{link}}$, occurs at zenith and characterises the system link performance. All elevation independent losses can be modelled by linearly scaling the link efficiency curve. This provides a general approach to modelling different SatQKD systems that vary in OGS receiver apertures and detector efficiencies.

2. BACKGROUND

We use empirically established performance data from the Micius satellite[15] to model the SatQKD channel, which can be linearly scaled to model other SatQKD configurations. We then use a theoretical analysis of secret key length generation in the finite regime to establish the security of satellite QKD in typical operating conditions.

2.1 System configuration

We consider a satellite in a circular low Earth Sun-synchronous orbit of altitude $h = 500$ km to model a downlink QKD operation during night overpasses of the optical ground station (OGS). For the satellite trajectory illustrated in Fig. 1a, we determine the elevation and distance of the satellite from the OGS as a function of time to generate expected detector count statistics. For any satellite trajectory, we simulate the time from when the satellite is first visible above 10° elevation until is passes below 10° to account for local horizon constraints around the OGS. The simplest type of orbit is the zenith orbit, where the satellite passes directly over the OGS and thus the maximum elevation is 90°.

We combine all losses into a single link efficiency value $\eta_{\text{link}} = -10\log_{10} p_{\text{d}}$ (dB) that characterises the probability, p_{d}, that a single photon transmitted by the satellite is detected. A lower dB value of η_{link} represents better total detection efficiency. This is determined by the transmit and receive aperture sizes, pointing accuracy, atmospheric absorption, turbulence, receiver internal losses, and detector efficiency. Transmitter internal optical inefficiencies are not included since they can be countered by adjusting the weak coherent pulse (WCP) source intensities to maintain the desired average photon number at the exit aperture.[16] For each elevation, we also do not consider explicit time-varying transmittance, changing channel loss is modelled as only due to changes in elevation with time.

Fig. 1b illustrates the representative link efficiency with time curve that we consider. It is worth noting that link efficiency vs elevation curves are highly dependent on system performance and OGS site conditions. Therefore, to allow a meaningful comparison of our simulated results with different performing SatQKD systems, we introduce a system link efficiency $\eta^{\text{sys}}_{\text{link}}$. This characterises the overall performance of the SatQKD system, which we define as the link efficiency at zenith. The nominal value for $\eta^{\text{sys}}_{\text{link}}$ considered is 27 dB. For greater constant losses, the per pass secret key length can be determined using worse (i.e. higher) plotted $\eta^{\text{sys}}_{\text{link}}$ values. Assuming the long term average ground spot size at minimum range is much larger than the OGS diameter D_r,

Table 1. **Reference system parameters**. We take published information of the Micius satellite and OGS system as representing an empirically derived set point for our finite key analysis. We assign a system link efficiency $\eta_{\text{link}}^{\text{sys}}$ of 27 dB to this reference system and linearly scale this efficiency to model other systems with smaller OGSs or differing source rates. Typical SatQKD operate at $\eta_{\text{link}}^{\text{sys}} = 37$ dB and $\eta_{\text{link}}^{\text{sys}} = 40$ dB, owing to imperfect optics, worse APT pointing, and less than ideal OGS siting.

Description	**Notation**	**Value**
Intrinsic QBER	QBER_{I}	5×10^{-3}
Afterpulse probability	p_{ap}	1×10^{-3}
Extraneous count probability	p_{ec}	5×10^{-7}
Source repition rate	N	10^8 Hz
Error correction parameter	ϵ_{cor}	10^{-15}
Secrecy parameter	ϵ_{sec}	10^{-9}
Satellite altitude	h	500 km
Minimum elevation constraint	θ_{min}	10°
Total nominal loss	$\eta_{\text{link}}^{\text{sys}}$	27 dB

we model the scaling of the link efficiency with OGS aperture size as $20\log_{10}(D_r/D_r^0)$ (dB) where D_r^0 denotes the reference OGS diameter which is taken as 1.2 m corresponding to the OGS at Delingha for the Micius satellite. The use of a 0.432 m telescope instead corresponds to an 8.9 dB increase in $\eta_{\text{link}}^{\text{sys}}$, all other things the same. We round this up to arrive at an optimistic ROKS $\eta_{\text{link}}^{\text{sys}} = 37$dB. We also consider a more conservative system performance level with $\eta_{\text{link}}^{\text{sys}} = 40$ dB.

We consider errors arising from dark counts and background light combining together. The probability of any extraneous count is p_{ec}. This is assumed to be constant and independent of elevation. In practice, it will depend strongly on the environment of the OGS and light from celestial bodies. All other error terms, such as misalignment, source quality, imperfect detection, are combined into an intrinsic quantum bit error rate QBER_{I} independent of channel loss/elevation. All of the nominal system parameters are summarised in Table 1.

2.2 SatQKD key length analysis toolkit

The efficient BB84 protocol[17] encodes signals in X and Z bases with unequal probabilities p_{X} and $1-p_{\mathsf{X}}$ respectively. We use the X basis for key generation and the Z basis for parameter estimation. For the two decoy-state WCP BB84 protocol, the sender randomly transmits one of three intensities μ_j for $j \in \{1,2,3\}$ with probabilities p_j. For the purposes of the security proof, we assume the intensities satisfy $\mu_1 > \mu_2 > \mu_3 = 0$. The finite block secret key length is then given by,[9]

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

where $s_{\mathsf{X},0}$, $s_{\mathsf{X},1}$ and ϕ_{X}, are the vacuum yield, single-photon yield, and the phase error rate associated with the single-photon events respectively. For SatQKD, we construct block sizes by processing overpass data as a single block without segmentation $\text{SKL}_{\text{finite}} = \text{SKL}\left(\{n_k^\mu, m_k^\mu\}\right)$ where $\{n_k^\mu, m_k^\mu\}$ denote agglomerated observed counts without partitioning into sub-segments. This is more practical than combining small data blocks with similar statistics from different passes, since it avoids the need to track and store a combinatorially large number of link segments until each has attained a sufficiently large block size for asymptotic key extraction

Since finite data generates observed statistics that deviate from asymptotic expectations, we employ correction terms $\delta^{\pm}_{\mathsf{X}(\mathsf{Z}),k}$ that relate the expected and observed statistics for bases $\mathsf{X}(\mathsf{Z})$ with a k-photon state, using the tight multiplicative Chernoff bound.[12] These correction terms quantify finite effects and maintain the composable security of the optimised key. In the finite key regime, the optimal number of bits publicly announced during privacy amplification is upper bounded $\lambda_{\text{EC}} \leq \log|\mathcal{M}|$, where $\mathcal{M}$ characterises the error syndromes for reconciliation.[11]

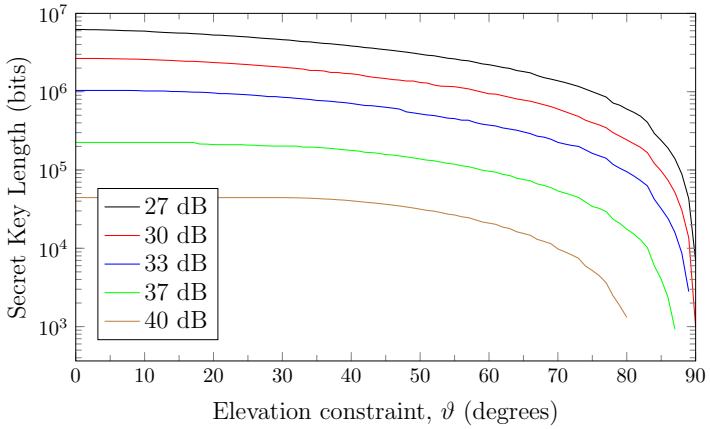


Figure 2. **SKL as a function of the elevation constraint**: $\vartheta \in \{0, 90\}$ for a zenith overpass. The lower and upper limits to this constraint correspond taking all and none of the transmitted bits respectively to construct the finite key.

For a defined SatQKD system, we optimise the finite key length in Eq. (1) by optimising 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 optimise over the portion of the overpass data used for key generation. To efficiently handle this optimisation, we developed a numerical toolkit to numerically analyse different SatQKD systems. The satellite quantum modelling & analysis (SatQuMA) software helps develop an intuition on the effects of different operational scenarios on the key rate and inform the development of source and receiver systems for future satellite missions.[13]

3. RESULTS

We consider the attainable finite secret key lengths (SKL) for two link efficiencies 37 dB and 40 dB that are typical of QKD operation utilising small satellites and/or small OGSs. The difference between these two system link efficiencies could be the difference in the performance of the transmission system or difference in atmospheric conditions at the location of the OGS. For both system efficiencies, we determine how the SKL depends on the elevation angle, different system losses, and different BB84 variants.

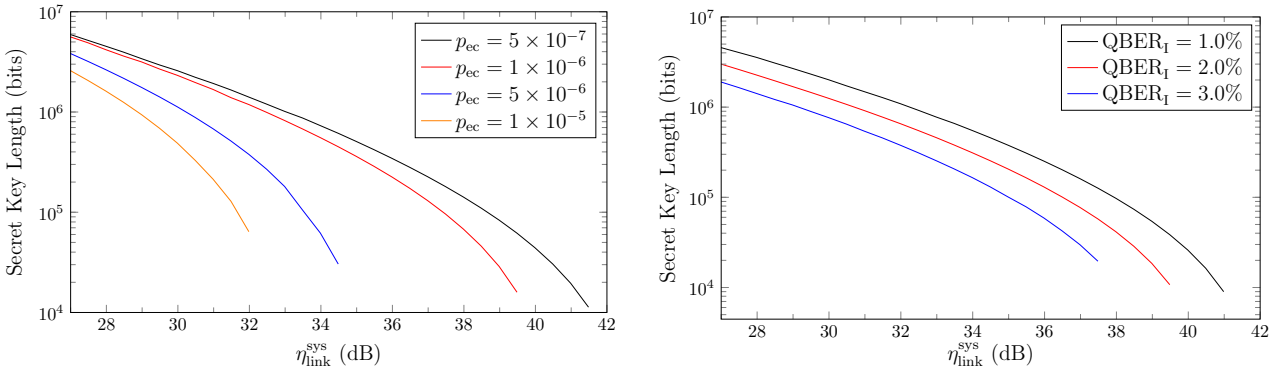
3.1 Effect of elevation constraint

For practical reasons, it will be difficult to construct the finite key from data collected from a horizon to horizon overpass. This reflects the difficulty of establishing quantum transmission at local horizon due to the requirement of initiation and stabilisation of tracking, handshake protocols, and local skyline obstructions. For this reason, we impose a minimum satellite elevation ϑ for any satellite pass above which transmitted data is used to construct finite keys. This allows for post-processing and finalisation of all reconciliation steps before the end of the overpass.

For the nominal system configuration, we look at the effect of imposing different elevation constraints on the attainable SKL. Fig. 2 illustrates this effect for different system losses. As expected, increasing the elevation constraint decreases the attainable SKL. More important to note is that for elevation constraints up to $\vartheta = 20°$ effect little change to the SKL for all system losses. This provides a comfortable window of opportunity to establish the quantum transmission link and perform all data post-processing. Advanced SatQKD systems have implemented key generation with $\vartheta = 5°$.[18] In the remainder of this report, we consider a minimum elevation of $\vartheta = 10°$.

3.2 Sensitivity to different errors

We determine the sensitivity of the optimised finite key length on the extraneous counts and the intrinsic quantum bit errors for a range of different system link efficiencies $\eta_{\text{link}}^{\text{sys}}$, corresponding to differently performing SatQKD systems. For each $\eta_{\text{link}}^{\text{sys}}$, we numerically optimise the finite key length.



(a) Sensitivity to p_{ec} (b) Sensitivity to QBER$_{\text{I}}$

Figure 3. **Single-pass SKL sensitivity with different errors**. The SKL with link efficiency is shown for different extraneous count rates in (a) with QBER$_{\text{I}}$ is 0.5%, and for different values of QBER$_{\text{I}}$ in (b) with $p_{\text{ec}} = 5 \times 10^{-7}$. A satellite pass over zenith is considered for both plots with an after pulse probability 0.1%.

First, the effect of different extraneous count rates on the optimised SKL is illustrated in Fig. 3a. Note that in the high loss regime, an increase in extraneous count can result in no finite key being generated. This indicates that extraneous counts have a strong influence on the QBER, when $\eta_{\text{link}}^{\text{sys}}$ becomes worse. Second, the effect of different intrinsic errors is illustrated in Fig. 3b illustrates the effect of different intrinsic system errors on the optimised SKL. We observe that the finite key length is not as susceptible to changes in the QBER$_{\text{I}}$ as compared with p_{ec}.

In Fig. 4, we show the relative effects of both the extraneous count rates and the intrinsic errors on the SKL for a large system link efficiency of $\eta_{\text{link}}^{\text{sys}} = 37$ and $\eta_{\text{link}}^{\text{sys}} = 40.5$ dB. This clearly illustrates that extraneous counts have a more dominant effect on the SKL. Specifically, zero finite key is returned for the parameter space sampled for p_{ec}. This indicates that future SatQKD missions should prioritise improvements to background light and detector dark count over source fidelities and satellite alignment to enhance attainable key rates. This helps identify the focused improvements for future SatQKD missions.

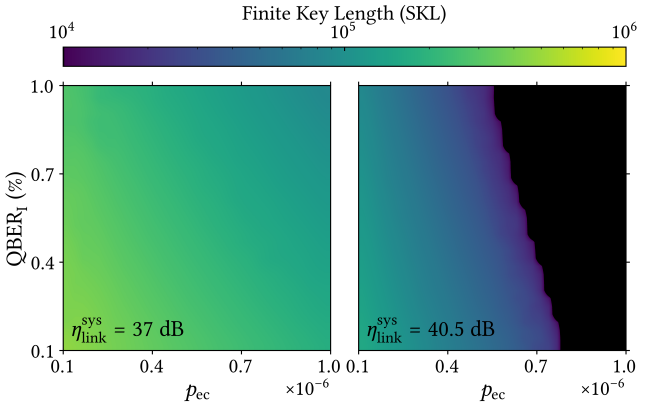


Figure 4. **SKL sensitivity with errors**. The x-axis shows variation with the extraneous count rates and the y-axis variation with intrinsic errors for a zenith pass. The system link efficiencies considered are $\eta_{\text{link}}^{\text{sys}} = 37$ dB (left) and $\eta_{\text{link}}^{\text{sys}} = 40.5$ dB (right). The black region indicates regions in the parameter space where zero finite key is attained.

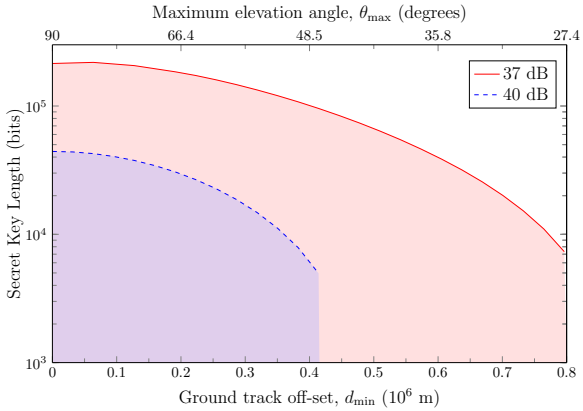


Figure 5. **Per-pass SKL for non-ideal overpasses**. Finite key length with different maximum elevation for $\eta_{\text{link}}^{\text{sys}}$=37 dB and 40 dB. The system parameters used here are $p_{\text{ec}} = 5 \times 10^{-7}$ and QBER$_{\text{I}}$ = 0.5%. The key generation footprint is given by the maximum d_{min} that generates non-zero finite key.

Table 2. **Expected yearly average finite SKL attainable**. We consider two practical system link efficiencies of $\eta_{\text{link}}^{\text{sys}} = 37$ dB and $\eta_{\text{link}}^{\text{sys}} = 40$ dB. The quoted SKL_{int} corresponds to the integrated area under each SKL vs ground track distance curve in Fig. 5 and has units of bit-metres (bm).

Total Loss	$\mathbf{SKL_{int}}$	$\overline{\mathbf{SKL}}_{\mathbf{year}}^{\mathbf{55^\circ N}}$
37 dB	8.75×10^{10} bm	21.4 Mb
40 dB	1.13×10^{10} bm	2.80 Mb

3.3 General satellite overpass geometries

A satellite in a zenith overpass defines an ideal trajectory owing to a longer transmission time window and smaller count rates due to worse average QBER. While this overpass delivers a larger single pass finite key, alternative overpass geometries are more likely. Fig. 5 illustrates how the optimised finite SKL for different overpass geometries parameterised through its maximum elevation angle θ_{max}. As expected, the attainable finite key decreases monotonically with decreasing θ_{max}, due to an increased average overpass QBER and drops to zero when the satellite passes below a critical elevation θ_{max}^{-}. This critical point defines the key generation footprint of a SatQKD mission.

The integrated area under the SKL vs. ground track distance plot can be used to determine the expected yearly average secret finite key length attainable at a defined longitude point for general satellite trajectories.[5] Considering a line of longitude at the position of Glasgow (55.9° N), table 2 summarises the expected yearly average SKL for system link efficiencies of 37 dB and 40 dB. Specifically, we expect 21.4 Mb and 2.8 Mb of finite keys at 37 dB and 40 dB respectively. One way of improving the finite key length volume is to collate and process data from multiple passes and calculate the key length on the combined data.[5] This improvement stems from larger block sizes and smaller statistical uncertainties in the estimated parameters that results in larger attainable SKLs.

4. CONCLUSION AND FUTURE WORK

In this study, we develop a satellite quantum modelling and analysis (SatQuMA) toolkit for the analysis of satellite QKD (SatQKD) systems that implement a weak-coherent pulse decoy state BB84 protocol in downlink configuration. Our numerical optimisation takes into account recent developments in finite key effects to model limited data block sizes arising from limited transmission time windows in SatQKD. We use SatQuMA to provide meaningful conclusions for system designs that could improve the performance of SatQKD missions.

We find the finite SKL has a pronounced sensitivity to changes in the extraneous count rate in comparison to changes in the intrinsic QBER. This suggests that future SatQKD missions should prioritise improvements to detectors over source fidelities to improve the achievable finite SKL per overpass. For system link efficiencies of 37 dB and 40 dB, which are representative of typical SatQKD operation, we determine the expected annual SKL generation is Mb and Mb respectively. Generally, high system link efficiencies generate worse average QBERs, which strains the achievable key generation volumes due to the increasing impact of statistical uncertainties in the estimated parameters. A route to overcome this impact is to collect data from multiple overpasses, but potential security vulnerabilities of increased latency in data accumulation must be considered. Finally, in previous work, we have concluded it is possible to expand the key generation footprint of SatQKD operations by implementing an efficient BB84 protocol.

Our numerical toolkit provides a range of interesting avenues for future work. For example, it would be important to account for dynamic atmospheric effects that will provide a more accurate loss model. MODTRAN would be a suitable tool to address this. Also, we are able to address a range of questions that directly address open questions on the engineering interface of realising SatQKD systems. Most immediately, we can extend our work to consider different sized systems to evaluate their feasibility in generating secret keys.

ACKNOWLEDGMENTS

We acknowledge support from the UK NQTP and the Quantum Technology Hub in Quantum Communications under EPSRC Grant number EP/T001011/1. 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), QTSPACE (COST CA15220), Innovate UK project AirQKD (Project number: 45364), the Innovate UK project ViSatQT (Project number: 43037), and the EPSRC Research Excellence Award (REA) Studentship.

REFERENCES

[1] Boaron, A., Rusca, D., Boso, G., Houlmann, R., Grünenfelder, F., Vulliez, C., Caloz, M., Perrenoud, M., Gras, G., Autebert, C., et al., "Progress on quantum key distribution using ultralow loss fiber," in [*Optical Fiber Communication Conference*], M4A–5, Optical Society of America (2020).

[2] Oi, D. K. L., Ling, A., Vallone, G., Villoresi, P., Greenland, S., Kerr, E., Macdonald, M., Weinfurter, H., Kuiper, H., Charbon, E., and Ursin, R., "Cubesat quantum communications mission," *EPJ Quantum Technology* **4**(1), 6 (2017).

[3] Villar, A., Lohrmann, A., Bai, X., Vergoossen, T., Bedington, R., Perumangatt, C., Lim, H. Y., Islam, T., Reezwana, A., Tang, Z., et al., "Entanglement demonstration on board a nano-satellite," *Optica* **7**(7), 734–737 (2020).

[4] Gündoğan, M., Sidhu, J. S., Henderson, V., Mazzarella, L., Wolters, J., Oi, D. K., and Krutzik, M., "Proposal for space-borne quantum memories for global quantum networking," *npj Quantum Information* **7**, 128 (August 2021).

[5] Sidhu, J. S., Brougham, T., McArthur, D., Pousa, R. G., and Oi, D. K. L., "Finite key effects in satellite quantum key distribution," *arXiv e-prints* , 2012.07829 (2020).

[6] Sidhu, J. S., Joshi, S. K., Gündoğan, M., Brougham, T., Lowndes, D., Mazzarella, L., Krutzik, M., Mohapatra, S., Dequal, D., Vallone, G., Villoresi, P., Ling, A., Jennewein, T., Mohageg, M., Rarity, J. G., Fuentes, I., Pirandola, S., and Oi, D. K. L., "Advances in space quantum communications," *IET Quantum Communication* , 1–36 (2021).

[7] Jianwei, P., "Progress of the quantum experiment science satellite (QUESS) Micius project," *Chin. J. Space Science* **38**(5), 604–609 (2018).

[8] Tomamichel, M., Lim, C. C. W., Gisin, N., and Renner, R., "Tight finite-key analysis for quantum cryptography," *Nat. Commun.* **3**, 634 (January 2012).

[9] Lim, C. C. W., Curty, M., Walenta, N., Xu, F., and Zbinden, H., "Concise security bounds for practical decoy-state quantum key distribution," *Phys. Rev. A* **89**, 022307 (February 2014).

[10] Rusca, D., Boaron, A., Grünenfelder, F., Martin, A., and Zbinden, H., "Finite-key analysis for the 1-decoy state QKD protocol," *Appl. Phys. Lett.* **112**, 171104 (April 2018).

[11] Tomamichel, M., Martinez-Mateo, J., Pacher, C., and Elkouss, D., "Fundamental finite key limits for one-way information reconciliation in quantum key distribution," *Quant. Inf. Proc.* **16**, 280 (October 2017).

[12] Yin, H.-L., Zhou, M.-G., Gu, J., Xie, Y.-M., Lu, Y.-S., and Chen, Z.-B., "Tight security bounds for decoy-state quantum key distribution," *Sci. Rep.* **10**, 14312 (August 2020).

[13] Sidhu, J. S., Brougham, T., McArthur, D., Pousa, R. G., and Oi, D. K. L., "Satellite Quantum Modelling & Analysis Software Version 1.0: Documentation," *arXiv e-prints* , 2109.01686 (2021).

[14] Lim, C. C.-W., Xu, F., Pan, J.-W., and Ekert, A., "Security analysis of quantum key distribution with small block length and its application to quantum space communications," *Phys. Rev. Lett.* **126**, 100501 (Mar 2021).

[15] Yin, J., Li, Y.-H., Liao, S.-K., Yang, M., Cao, Y., Zhang, L., Ren, J.-G., Cai, W.-Q., Liu, W.-Y., Li, S.-L., et al., "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature* **582**(7813), 501–505 (2020).

[16] Bourgoin, J.-P., Meyer-Scott, E., Higgins, B. L., Helou, B., Erven, C., Huebel, H., Kumar, B., Hudson, D., DSouza, I., Girard, R., Laflamme, R., and Jennewein, T. D., "A comprehensive design and performance analysis of low earth orbit satellite quantum communication," *New Journal of Physics* **15**(2), 023006 (2013).

[17] Lo, H.-K., Chau, H. F., and Ardehali, M., "Efficient quantum key distribution scheme and a proof of its unconditional security," *Journal of Cryptology* **18**(2), 133–165 (2005).

[18] Chen, Y.-A., Zhang, Q., Chen, T.-Y., Cai, W.-Q., Liao, S.-K., Zhang, J., Chen, K., Yin, J., Ren, J.-G., Chen, Z., et al., "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature* **589**, 214–219 (January 2021).