Satellite constellations for trusted node QKD networks

Vergoossen, T.; Loarte, S.; Bedington, R.; Kuiper, H.; Ling, A.

Publication date
2019

Document Version
Final published version

Published in
Proceedings of the International Astronautical Congress, IAC

Citation (APA)
Vergoossen, T., Loarte, S., Bedington, R., Kuiper, H., & Ling, A. (2019). Satellite constellations for trusted node QKD networks. In *Proceedings of the International Astronautical Congress, IAC* (Vol. 2019-October). (Proceedings of the International Astronautical Congress, IAC).

Satellite constellations for trusted node QKD networks

T Vergoossen[1]‡, S Loarte[1,2]§, R Bedington[1], H Kuiper[2] and A Ling[1,3]

[1] Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 120435

[2] Faculty of Aerospace Engineering, Delft University of Technology, Kluyverweg 1, 2629 HS Delft, The Netherlands

[3] Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117551

E-mail: cqttv@nus.edu.sg

March 2019

Abstract. Quantum key distribution from satellites becomes particularly valuable when it can be used on a large network and on-demand to provide a symmetric encryption key to any two nodes. A constellation model is described which enables QKD-derived encryption keys to be established between any two ground stations with low latency. This is achieved through the use of low earth orbit, trusted-node QKD satellites which create a buffer of keys with the ground stations they pass over, and geostationary relay satellites to transfer secure combinations of the keys to the ground stations. Regional and global network models are considered and the use of inter-satellite QKD links for balancing keys is assessed.

Keywords: QKD, Quantum cryptography, satellites, constellations, trusted node, BB84, LEO, Inter-satellite link

1. Introduction

Quantum key distribution (QKD) is a branch of quantum cryptography which describes methods for establishing highly secure symmetric keying material between separated users [1]. QKD processes use very weak optical signals so have fundamental distance limitations due to increased losses with increasing distances. To extend the separations possible between users repeater nodes can be used, either 'trusted nodes' or quantum repeaters. The most secure solution is to use quantum repeaters; these do not make a measurement on the QKD signals so the communicating parties are able to verify

‡ Author, Satellite-QKD model.

§ Constellation model and analysis in this work.

between themselves that the key they have established is secure. Quantum repeaters however have yet to be demonstrated in practical systems and are not ready to be considered for near term QKD networks. Present QKD networks accordingly use trusted nodes. In satellite QKD users establish keys with the satellite node, which then combines their keys as an XOR (exclusive OR operation) and broadcasts this publicly [2, 3]. The XOR key is meaningless to anyone except the two users who can use it to determine each others keys, which they can then use as secret key material for encryption purposes. In optical fibre networks, many trusted nodes can be connected together to create long connections such as the Beijing-Shanghai QKD link, which features 32 trusted nodes [4]. Since these nodes have full access to the keys passing through them they must be trusted to be secure, and the security can only come from conventional security methods—e.g. restricted access and trusted human guards. As a result, links with large numbers of nodes, and nodes based in foreign countries, are intrinsically harder to trust. Low earth orbit (LEO) satellite-based trusted nodes help address both of these issues by reducing the numbers of nodes required. Firstly, LEO satellites orbit the Earth continuously and pass over most places several times per day—rather than using a chain of nodes they can simply act as a store-and-forward device and wait until the desired recipient passes underneath them ‖. Secondly, they are likely to be harder to access and infiltrate than any ground-based facility.

Satellite QKD has been extensively discussed in terms of theoretical modelling descriptions [5], technology developments [6, 7], hardware demonstrations [8, 9, 10, 3] and in review articles [2, 11]. It is clear, and often stated, that the logical successor to single QKD satellites is a QKD constellation [12, 13], but how this could be implemented has yet to be investigated or defined in published literature. In this study we define a concept for a low earth orbit (LEO) trusted node QKD satellite and investigate its effectiveness in different constellation arrangements. In particular we assess the value of inter-satellite QKD links.

2. Methods

We describe a model capable of analysing the performance of satellite networks featuring satellite-to-ground and inter-satellite links, and a concept for a trusted node QKD constellation.

2.1. Satellite-QKD Links

Satellite-QKD links are modelled in Matlab using principles set forth by Bourgoin et al. [5]. Key rates are calculated from optical link parameters using the equations for weak and vacuum decoy-state BB84 provided by Xiongfeng Ma et al. [14]. To validate the model, the QKD demonstrations performed by the Micius satellite were modelled and

‖ QKD is a point to point service and it is assumed that the keying material is buffered for future use so the low latency of the store-and-forward technique is not an issue.

compared to the published results (input parameters are in Appendix A) [15]. Figure 1 shows that there is a lot more variability in the real-world results, but that the model results are placed convincingly within this variability.

Some simplifications of the model include assuming a constant pointing error and constant, but path length dependent, atmospheric losses rather than experiencing local weather effects. Furthermore the asymptotic key size assumption is used and intensity fluctuations of signal and decoy states are not considered. As a result error correction and privacy amplification losses are underestimated.

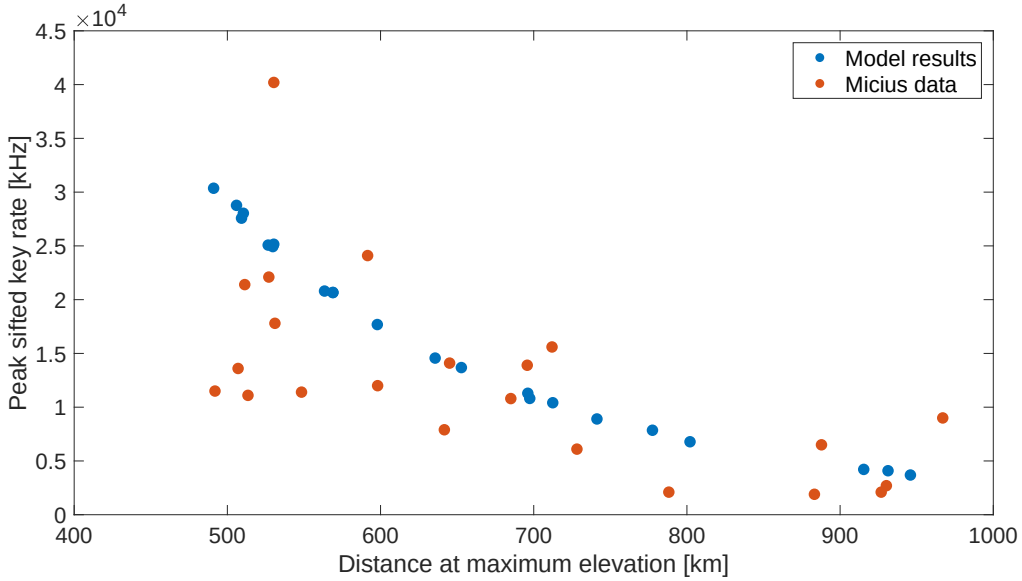

Figure 1. Comparison of our model results with Micius published data for specific passes between September 2016 and May 2017.

2.2. QKD trusted node constellation concept

In our constellation concept, satellites perform QKD with any ground station they pass over to generate a private symmetric key between that satellite and the ground station. Each satellite maintains a continuous classical radio link with the ground network, using relay nodes in higher orbits, e.g. in geostationary orbit [16]. When any two users on the ground (e.g. ground station A and B), need to communicate securely the network is queried for satellites that have keys shared with A and B on-board a secure key management module. Any such keys are combined using an XOR function and can be broadcast to A and B via the relay satellites with minimal latency. Station A and B can perform a reverse XOR operation to extract the key held by the other ground station and can now communicate securely. The used key for A and B is deleted from satellites.

We also propose an extension to the above configuration in which the LEO satellites have quantum inter-satellite links (ISL) that are used to re-distribute key across the constellation. This solves the problem where some satellites in the constellation have secure key established with station A, but none or not as much with station B; and

vice versa. In this situation these satellites either cannot create an XOR of key A and B, or they are constrained by the size of one of the keys. However, secure re-distribution of keys A and B between satellites would maximise the mutual key available on each satellite for XOR operations and optimise the constellation effectiveness. Inter-satellite links are feasible if the satellites are within close proximity of each other and have low relative angular motion. These operational requirements lead to two possible scenarios: ISL between satellites in different orbital planes (inter-planar) and a string-of-pearls configuration of satellites in the same plane (intra-planar ISL). This is illustrated in Figure 3d. In a string-of-pearls configuration satellites would have additional receivers/transmitters to perform QKD with satellites ahead of them or behind them, while the inter-planar case requires more capable link architectures to communicate over larger relative angles and distances. In addition, intra-planar links provide constant availability, provided they are in eclipse and so will outperform the inter-planar links. For these reason only the string-of-pearls configuration is discussed further in this paper.

2.3. Constellation Modelling

The satellite QKD Matlab model was integrated with STK's orbit modelling capabilities and extended to model constellations with satellite-to-ground and inter-satellite links. Additionally, cloud coverage predictions per pass are calculated based on historical cloud statistics [17]. The model architecture is shown in Figure 2.

The terminals are assumed to only be able to perform QKD at night so the model is configured to perform QKD only during passes where both the satellite and the ground station are in eclipse. They are assumed to convert and store sufficient solar power in the rest of the orbit that they can perform QKD continuously when in eclipse. Satellites have one Micius-type Earth-pointing terminal, and where specified another terminal available for inter-satellite links. In the case of overlapping ground station passes, i.e. when ground stations are close together and are simultaneously in view of the satellite, the satellite will choose to perform QKD with the less cloudy one.

Two example ground station networks are considered in this analysis to demonstrate how global and regional networks can have different considerations. The global example uses nodes in the G20 cities (Brussels is considered to serve all Western European cities), the regional example is of an Indo-ASEAN network, see appendix B. The satellite networks only consist of quasi-circular orbits and combinations of orbital planes at the same altitude.

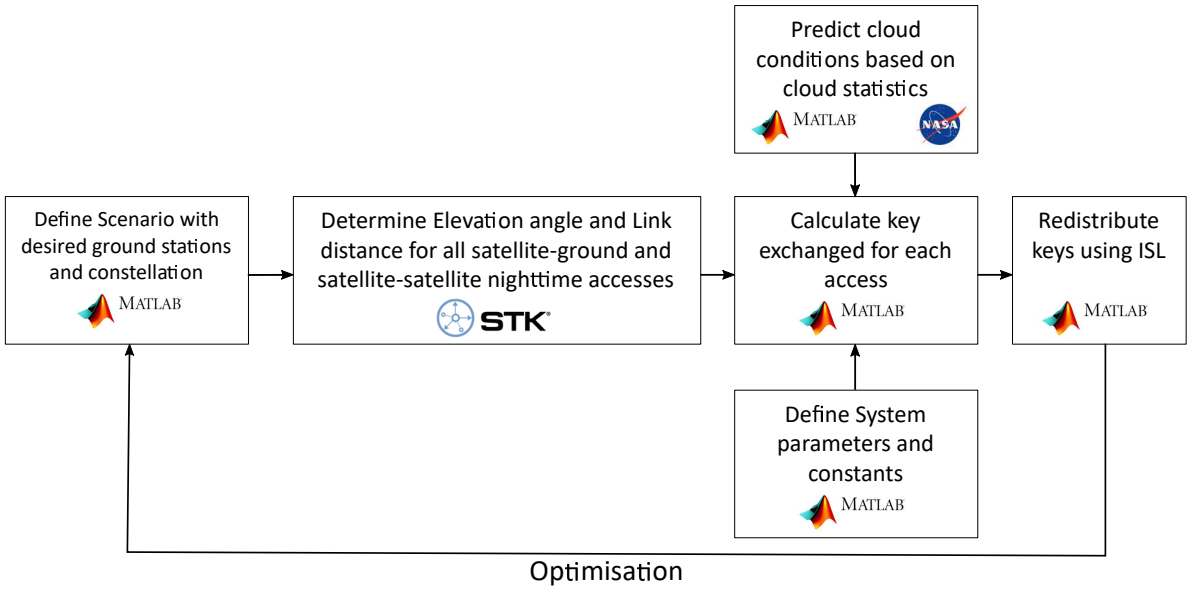

Figure 2. Architecture of the toolkit for modelling QKD constellations

3. Results

First, total access times for single-plane constellations at different inclination angles were evaluated in Figure 3a and b. Second, key rates for multi-plane constellations were investigated where all planes have the same inclination angle but are spaced evenly around the globe.

There are many different potential use cases for QKD networks, and thus many different ways to optimise and compare implementations. In this study we use as our figure of merit, the maximum message size that could be sent out to all of the other stations in the network using one-time-pad (bit for bit encrypting) and using each key only once. This 'embassy model' is the scenario for example if a country wanted to send out the same secret message to all of its overseas embassies.

Table 1 and Table 2 show the maximum distributed messages nodes can send for different constellation configurations. In practice this is limited by how much key other nodes hold. The default number of satellites used for simulations is six, and the ISL configurations use the optimal number of satellites as established in Figure 3c.

4. Discussion

The following sections discuss how these results impact the design of a constellation and the relevance of inter-satellite links.

4.1. Constellation design

Satellites in low inclination orbits pass up to 16 times per day over low latitude ground stations, while ground stations at high latitude typically only see satellites in high

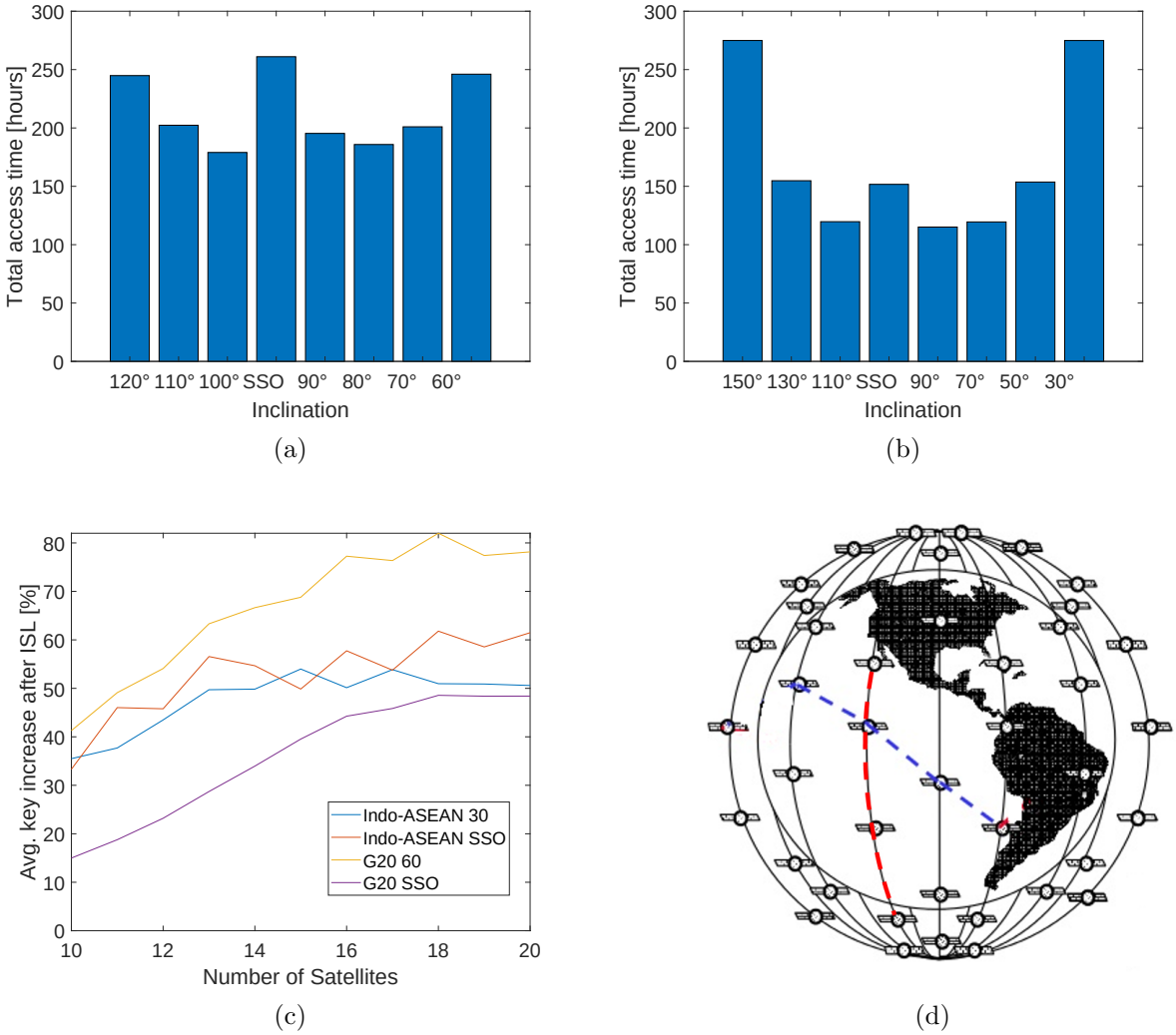

Figure 3. (a) Total access time of 6 satellites equally distributed in a single-plane over one year for the G20 network. SSO refers to a noon-midnight Sun-Synchronous Orbit and corresponds to an inclination of 96-100 degrees depending on altitude (b) for the Indo-ASEAN network (c) Diminishing return of increasing number of satellites with ISL in constellation leads to optimum size of constellation. Essentially, there is no need for satellite to share keys in excess of the key material they need to re-distribute. (d) Possible types of ISL. Only intra-planar (red) links are considered in this paper as they are less complex and have higher link availability.

inclination orbits twice a day. Maximum latitudes in the G20 and Indo-ASEAN network are around 60 and 30 degrees, respectively. When restricted to a single orbital plane, maximising passes in the network is achieved by setting the inclination of the plane equal to the maximum latitude. This is illustrated in Figure 3b. However, not all passes occur during nighttime. Figure 3a shows that a noon-midnight sun-synchronous orbit, while having fewer passes overall, maximises useful accesses because of the long and consistent passes at nighttime it provides. Constellations with satellites spread over multiple orbital planes do not improve key sizes although the time between passes for

G20	6 satellites					16 satellites			
Location	Message size [Mbit]					Message size [Mbit]			
	SSO	60deg 2p/3s	60 deg 3p/2s	60 deg 16p/1s		SSO 1p/16s	SSO 1p/16s ISL	60 deg	60deg 1p/6s ISL
Ankara	49.55	40.86	38.47	39.97		129.73	182.76	102.43	157.91
Beijing	42.01	34.48	35.37	34.38		106.62	170.66	94.54	157.91
Brasilia	41.81	37.00	36.58	38.55		109.64	182.76	102.06	157.91
Brussels (Europe)	23.82	26.97	26.72	27.92		61.68	122.57	72.53	143.71
Bueno Aires	45.48	39.02	38.44	39.58		121.02	182.76	99.46	157.91
Canberra	43.61	39.31	38.44	37.43		118.44	182.13	104.22	157.91
Delhi	42.50	37.54	36.10	36.79		112.53	178.17	97.34	157.91
Jakarta	24.89	22.43	22.40	22.94		66.49	131.33	59.02	118.03
Mexico City	51.99	46.07	47.02	47.28		143.21	182.76	124.05	157.91
Moscow	17.83	26.90	25.85	27.24		47.05	94.10	74.31	146.06
Ottawa	32.51	30.11	31.10	28.59		87.89	140.69	79.39	155.66
Pretoria	54.26	48.42	48.69	47.47		143.50	182.76	125.99	157.91
Riyadh	68.12	59.46	59.39	58.74		182.76	182.76	157.91	157.91
Seoul	37.91	34.36	34.69	32.16		99.07	151.31	90.08	157.91
Tokyo	33.65	29.60	28.87	31.56		90.37	143.32	80.14	156.34
Washington	37.97	34.77	34.16	35.86		108.45	178.29	93.76	157.91
Average	40.49	36.71	36.39	36.65		108.03	161.82	97.33	153.55

Table 1. Distributed message size after 1 year for the G20 network of ground stations for constellations of 6 and 16 satellites. For example, over one year Ankara could send 49.55 Mbits of secure messages to all cities in this list, provided the cities have enough key of their own. SSO refers to a noon-midnight Sun-Synchronous Orbit. The notation [60 deg 2p] indicates that the constellation is distributed equally over 2 orbital planes with an inclination of 60 degrees. Within one plane the argument of periapsis of the 3 satellites is 360/3 = 120 degrees apart. The longitude of the ascending node of the orbital planes themselves is 360/2=180 degrees apart. The colours are a visual aid for identifying key sizes (from red to green).

individual ground stations may be reduced due to the improved temporal coverage [18]. Some ground stations consistently perform poorly due to clouds (modelled with a 0.1 longitude by 0.1 degree latitude resolution). While this emphasizes the need for choosing appropriate ground station locations, this is not necessarily problematic as any satellite-QKD network should interface with ground-based fibre networks that could cover the most cloudy areas.

IndoASEAN	6 satellites					16 satellites			
Location	Message size [Mbit]					Message size [Mbit]			
	SSO 1p/6s	30deg 2p/3s	30 deg 3p/2s	30 deg 6p/1s		SSO 1p/16s	SSO 1p/16s ISL	30 deg 1p/16s	30deg 1p/16s ISL
Singapore	10.13	16.33	15.84	14.98		28.36	56.71	40.46	80.92
Jakarta	37.13	59.00	60.34	58.11		98.43	178.76	159.49	317.59
Delhi	49.49	162.59	158.37	149.78		170.08	179.29	404.61	509.18
Mumbai	63.57	135.02	132.86	132.16		179.22	179.29	351.62	509.18
Bengaluru	39.86	67.50	66.80	66.76		113.12	179.29	182.95	364.19
Calcutta	40.37	109.76	105.97	104.98		119.41	179.29	286.56	509.18
Kuala Lumpur	15.52	20.51	23.17	23.93		36.22	71.95	60.31	120.62
Chennai	23.55	44.36	43.12	42.47		62.61	124.36	113.99	226.32
Bangkok	29.75	50.83	52.05	50.35		78.42	155.45	138.20	273.55
Ho Chi Minh	21.59	33.96	34.00	33.33		57.61	115.22	91.77	183.54
Manila	25.36	46.48	41.81	44.37		69.80	139.21	116.90	232.79
Average	32.39	67.85	66.76	65.57		92.12	141.71	176.99	302.46

Table 2. Distributed message size for the Indo-ASEAN network of ground stations for constellations of 6 and 16 satellites. See caption of Table 1 for explanation of the notation.

4.2. Inter-satellite links

Results in Table 1 and Table 2 illustrate that inter-satellite links can provide a 20-100% increase in message size for all ground stations for the two networks studied here under the embassy model assumption. It should be noted that for the chosen figure of merit there can be improvements in stored key even for the ground stations that originally have the most key. This is evident in the results for the Indo-ASEAN constellation, where the initial differences are very large, but not in the G20 constellation. Re-distribution is currently based on a simple algorithm that only copies keys from one satellite to the next etc. so further improvements in equalising key material can be envisaged. Whether ISL QKD is cost-effective was not considered within the scope of this work: a trade-off between simply launching more satellites versus increasing the complexity of individual satellites would be required. However, there is a number of satellites for a given network that makes optimum use of ISL, as the required shared key between satellites is determined by the size of the key that is to be re-distributed. Presently, the operational requirements of ISL do not lead to sub-optimal constellation choices, however more exotic constellation types may be derived that cannot feature ISLs.

5. Conclusion

LEO constellations of trusted-node QKD satellites, continually performing QKD with the ground stations they fly over, can be used to provide low-latency, symmetric keys on demand between any two ground stations. They can do this by building a buffer of keys on board that can be quickly combined by an XOR operation and delivered to ground station via an RF (classical communications) relay satellite. The QKD satellites are best launched into SSO orbit or an orbit with an inclination equal to the latitude of the ground station farthest from the equator.

Inter-satellite links can improve the efficiency with which encryption keys are used, an average message size increase of 50-70% in our examples, but whether this is cost-effective remains an open question.

6. Acknowledgments

Sergio Loarte performed the bulk of this work at the Centre for Quantum Technologies during an exchange stay. Hans Kuiper supervised Serio at TU Delft. With thanks to Abhijit Mitra and Sanat Biswas from IIIT Delhi who mooted the concept of an Indo ASEAN QKD network with us.

This work is partially supported by the National Research Foundation, Prime Ministers Office, Singapore (under the Research Centres of Excellence programme and through Award No. NRF-CRP12-2013-02) and by the Singapore Ministry of Education (partly through the Academic Research Fund Tier 3 MOE2012-T3-1-009).

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Reviews of Modern Physics* **74** 145–195 ISSN 0034-6861 URL https://link.aps.org/doi/10.1103/RevModPhys.74.145

[2] Bedington R, Arrazola J M and Ling A 2017 *npj Quantum Information* **3** 30 ISSN 2056-6387 URL http://www.nature.com/articles/s41534-017-0031-5

[3] Liao S K, Cai W Q, Handsteiner J, Liu B, Yin J, Zhang L, Rauch D, Fink M, Ren J G, Liu W Y, Li Y, Shen Q, Cao Y, Li F Z, Wang J F, Huang Y M, Deng L, Xi T, Ma L, Hu T, Li L, Liu N L, Koidl F, Wang P, Chen Y A, Wang X B, Steindorfer M, Kirchner G, Lu C Y, Shu R, Ursin R, Scheidl T, Peng C Z, Wang J Y, Zeilinger A and Pan J W 2018 *Physical Review Letters* **120** 30501 ISSN 0031-9007 (*Preprint* 1801.04418) URL http://arxiv.org/abs/1801.04418

[4] Courtland R 2016 *IEEE Spectrum* **53** 11–12 ISSN 0018-9235 URL http://ieeexplore.ieee.org/document/7607012/

[5] Bourgoin J P, Meyer-Scott E, Higgins B L, Helou B, Erven C, Hübel H, Kumar B, Hudson D, D'Souza I, Girard R, Laflamme R and Jennewein T 2013 *New Journal of Physics* **15** 023006 ISSN 1367-2630 (*Preprint* 1211.2733) URL http://arxiv.org/abs/1211.2733http://dx.doi.org/10.1088/1367-2630/15/2/023006http://stacks.iop.org/1367-2630/15/i=2/a=023006?key=crossref.e2000769db1ac53dcdfd7826a722c51a

[6] Steinlechner F, Trojek P, Jofre M, Weier H, Perez D, Jennewein T, Ursin R, Rarity J, Mitchell

M W, Torres J P, Weinfurter H and Pruneri V 2012 *Optics express* **20** 9640–9 ISSN 1094-4087 (*Preprint* 1204.5330) URL http://www.ncbi.nlm.nih.gov/pubmed/22535055

[7] Naughton D, Bedington R, Barraclough S, Islam T, Griffin D and Smith B 2019 *Optical Engineering* **58** 1 ISSN 0091-3286 URL https://www.spiedigitallibrary.org/journals/optical-engineering/volume-58/issue-01/016106/Design-considerations-for-an-optical-link-supporting-intersatellite-quantum-key/10.1117/1.OE.58.1.016106.full

[8] Takenaka H, Carrasco-Casado A, Fujiwara M, Kitamura M, Sasaki M and Toyoshima M 2017 *Nature Photonics* **11** 502–508 ISSN 1749-4885 URL http://www.nature.com/doifinder/10.1038/nphoton.2017.107

[9] Vallone G, Bacco D, Dequal D, Gaiarin S, Luceri V, Bianco G and Villoresi P 2015 *Physical Review Letters* **115** 040502 ISSN 0031-9007 URL https://link.aps.org/doi/10.1103/PhysRevLett.115.040502

[10] Grieve J A, Bedington R, Tang Z, Chandrasekara R C and Ling A 2018 *Acta Astronautica* **151** 103–106 ISSN 00945765 (*Preprint* 1710.05487) URL http://arxiv.org/abs/1710.05487http://dx.doi.org/10.1016/j.actaastro.2018.06.005https://linkinghub.elsevier.com/retrieve/pii/S0094576518304405

[11] Khan I, Heim B, Neuzner A and Marquardt C 2018 *Optics and Photonics News* **29** 26 ISSN 1047-6938 URL https://www.osapublishing.org/abstract.cfm?URI=opn-29-2-26

[12] Skander A, Abderraouf M, Malek B, Nadjim M and Al-Harthi M M 2010 Study of LEO satellite constellation systems based on quantum communications networks *2010 5th International Symposium On I/V Communications and Mobile Network* (IEEE) pp 1–4 ISBN 978-1-4244-5996-4 URL http://ieeexplore.ieee.org/document/5656276/

[13] Elser D, Seel S, Heine F, Scheidl T, Ursin R, Sodnik Z and Peev M 2012 *Proc. International Conference on Space Optical Systems and Applications (ICSOS) 2012, Post-1, Ajaccio, Corsica, France, October 9-12 (2012)* **12** URL http://icsos2012.nict.go.jp/pdf/1569657077.pdf{\%}5Cnpapers3://publication/uuid/470A1984-5B03-48DD-BF63-8E096AC4CF6F

[14] Ma X, Qi B, Zhao Y and Lo H K 2005 *Physical Review A - Atomic, Molecular, and Optical Physics* **72** 1–15 ISSN 10502947 (*Preprint* 0503005)

[15] Liao S K, Cai W Q, Liu W Y, Zhang L, Li Y, Ren J G, Yin J, Shen Q, Cao Y, Li Z P, Li F Z, Chen X W, Sun L H, Jia J J, Wu J C, Jiang X J, Wang J F, Huang Y M, Wang Q, Zhou Y L, Deng L, Xi T, Ma L, Hu T, Zhang Q, Chen Y A, Liu N L, Wang X B, Zhu Z C, Lu C Y, Shu R, Peng C Z, Wang J Y and Pan J W 2017 *Nature* **549** 43–47 ISSN 0028-0836 URL http://www.nature.com/doifinder/10.1038/nature23655

[16] Addvalue GEO communications relay URL https://www.addvaluetech.com/category/connection-to-space/idrs/

[17] NASA Cloud statistics database (1 month - terra/modis) URL https://neo.sci.gsfc.nasa.gov/view.php?{\%}0AdatasetId=MODAL2{_}M{_}CLD{_}FR

[18] Loarte S 2019 *Towards a global space-based QKD network* Master thesis Delft University of Technology URL http://resolver.tudelft.nl/uuid:d8a391e8-d21a-4f37-95ec-467a49d391ea

Appendix A

Parameter	Micius data	Model results	Units
Closest approach	645	635.7	km
Sifted key rate at 1200 km	1	1.2	kbit/s
Sifted key rate at 645 km	12	13.8	kbit/s
Experiment duration	273	273	s
Total detection events	3,551,136	3,926,729	bits
Sifted key size	1,671,072	1,963,364	bits
Average Quantum Bit Error Rate	1.1	1.2	%
Secret key size	300,939	521,513	bits
Average secret key rate	1102	1910	bits/s

Table 3. Detailed comparison of Micius pass on 19th of December 2016

Appendix B

Figure 4. G20 ground stations

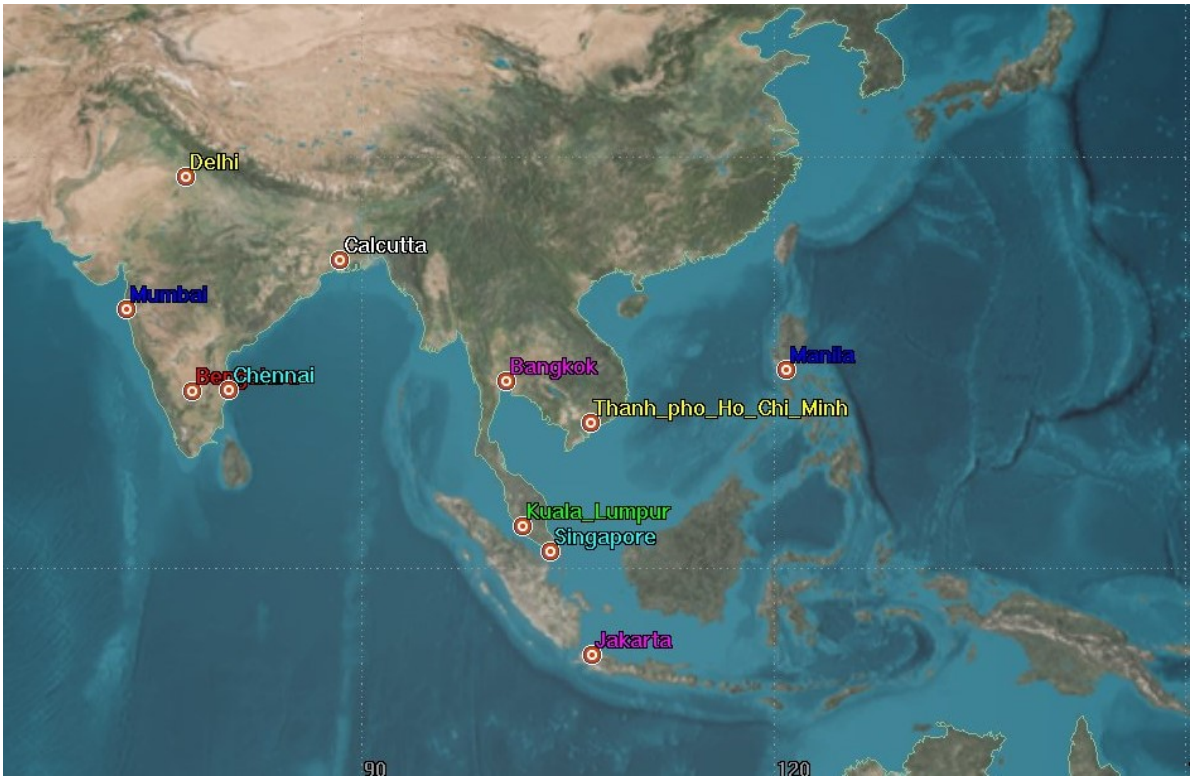

Figure 5. Indo-ASEAN ground stations