Modelling of satellite constellations for trusted node QKD networks

Vergoossen, Tom; Loarte, Sergio; Bedington, Robert; Kuiper, Hans; Ling, Alexander

DOI
10.1016/j.actaastro.2020.02.010

Publication date
2020

Document Version
Final published version

Published in
Acta Astronautica

Acta Astronautica 173 (2020) 164–171

Contents lists available at ScienceDirect

Acta Astronautica

journal homepage: www.elsevier.com/locate/actaastro

Research paper

Modelling of satellite constellations for trusted node QKD networks

Tom Vergoossen[a,1,*], Sergio Loarte[c,2], Robert Bedington[a], Hans Kuiper[c], Alexander Ling[b,d]

[a] SpeQtral Pte Ltd., Cintech 1, 73 Science Park Drive, 118254, Singapore
[b] Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 120435, Singapore
[c] Faculty of Aerospace Engineering, Delft University of Technology, Kluyverweg 1, 2629, HS Delft, the Netherlands
[d] Department of Physics, National University of Singapore, 2 Science Drive 3, 117551, Singapore

ARTICLE INFO

Keywords:
QKD
Quantum cryptography
Satellites
Constellations
Trusted node
BB84
LEO
Inter-satellite link

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.

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 and so have fundamental distance limitations due to losses increasing with increasing distances. Repeater nodes can be used to extend the separations possible between users, 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 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 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.[3] 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], conceptual studies [6], technology developments [7,8], hardware demonstrations [3,9–11] and in review articles [2,12]. It is clear, and often stated, that the logical successor to single QKD satellites is a QKD constellation [13,14], 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.

* Corresponding author.
E-mail address: tom@speqtral.space (T. Vergoossen).
[1] Author of paper and created Satellite-QKD model while at CQT, Singapore.
[2] Created constellation model and performed analysis in this work at CQT for his TU Delft Master's thesis.
[3] 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.

https://doi.org/10.1016/j.actaastro.2020.02.010
Received 3 July 2019; Received in revised form 30 December 2019; Accepted 4 February 2020
Available online 18 February 2020

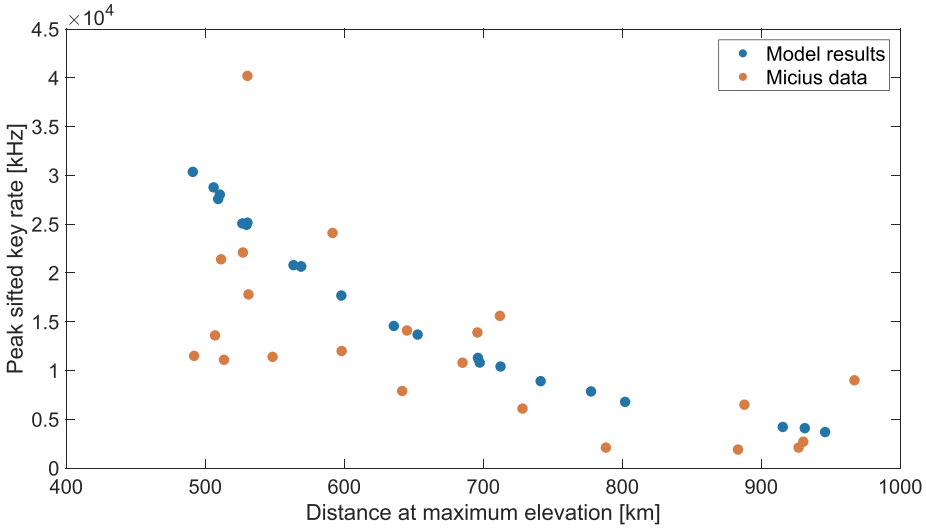

Fig. 1. Comparison of our model results with Micius published data for specific passes between September 2016 and May 2017.

2. Material and 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. [15]. To validate the model, the QKD demonstrations performed by the Micius satellite were modelled and compared to the published results (input parameters and results are shown in Appendix A) [16]. Fig. 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. Differences could in principle arise from any parameter in the link budget changing. Local weather conditions change from pass to pass and affect the atmospheric absorption value in the link budget. The error of the bi-directional pointing and tracking link established by the spacecraft and the ground station depends on the angular velocity of the spacecraft as reported by the Micius team [16]. As a result at the closest approach between 500 and 700 km the variability in peak sifted key rate is expected to be greatest. These effects could be considered in the model in future work by including simulated pointing errors and incorporating local weather data (if available). 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 (see Appendix A).

2.2. Constellation modelling

The satellite QKD MATLAB model was integrated with AGI System Tool Kit's orbit modelling capabilities and extended to model constellations with satellite-to-ground and inter-satellite links.[4] The work flow is indicated in Fig. 2. An input script in MATLAB defines the scenario that is to be considered by specifying a time period, number of satellites and their orbits, and the location of the ground stations. The main script calls on this input script and passes these values to STK where, for the given time period, all passes of the satellites over the specified ground stations and satellite to satellite passes are found by numerical propagation of the initial orbit state. STK returns a matrix containing elevation angles and link distances with a specified time step. In MATLAB the secret key exchanged for each pass can now be calculated. Additionally, cloud coverage predictions per pass are calculated based on historical cloud statistics [17]. Redistribution of keys using inter-satellite links is performed given available shared keys between satellites. The model is capable of using results to start another run given a specific optimisation method (so far implemented: genetic algorithms and simulated annealing). However, optimisation proved computationally intensive for large satellite constellations so the efficiency of the code could be improved or the model could be written in a lower level programming language (e.g. C+).

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 such 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.

3. Results

3.1. Orbit selection

First, total access times for single-plane constellations at different inclination angles were evaluated in Fig. 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 encryption) and using each key only once. This

[4] MATLAB version MATLAB R2018b and AGI STK PRO 11.5 were used for the analysis presented here.

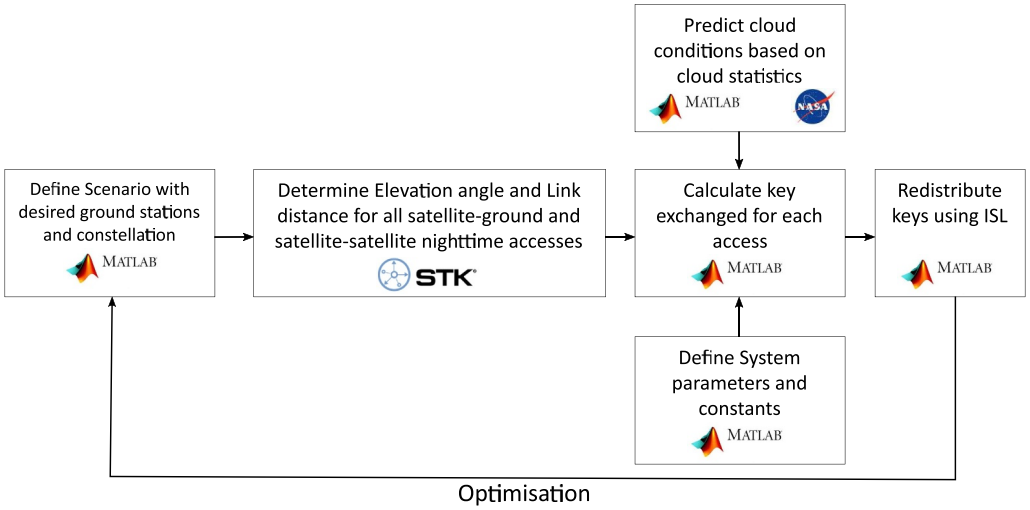

Fig. 2. Architecture of the toolkit for modelling QKD constellations.

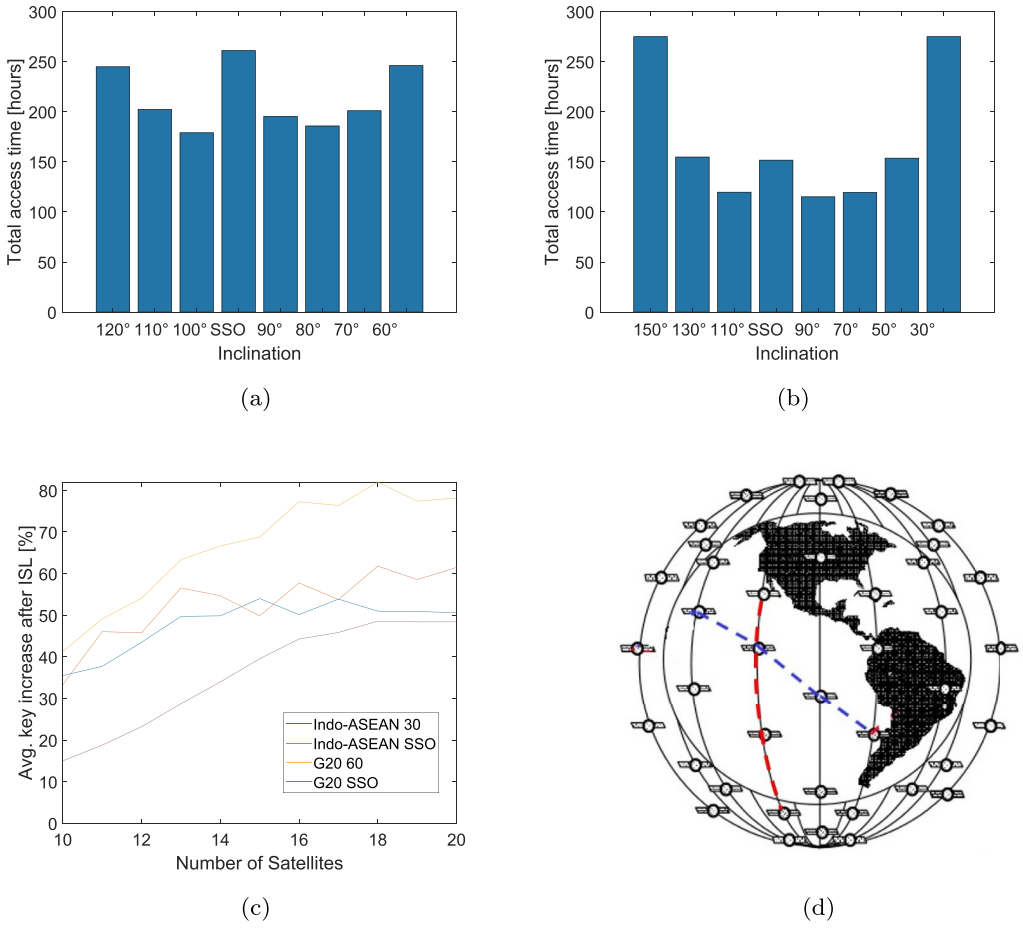

Fig. 3. (a) Total access time of 6 satellites equally distributed in a single-plane over one year for the G20 network. SSO refers to a noon-midnight Sun-Synchronous Orbit and corresponds to an inclination of 96–100° depending on altitude (b) for the Indo-ASEAN network (c) Diminishing return of increasing 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. (For interpretation of the references to colour in this figure legend, the reader is referred to the Web version of this article.)

'embassy model' is the scenario for example if a country wanted to send out the same secret message to all of its overseas embassies. The details of this embassy model are explained in Appendix C.

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 Fig. 3c.

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°. Within one plane the argument of periapsis of the 3 satellites is 360/3 = 120° apart. The longitude of the ascending node of the orbital planes themselves is 360/2 = 180° apart. The colours are a visual aid for identifying key sizes (from red to green).

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

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 inclination orbits twice a day. Maximum latitudes in the G20 and Indo-ASEAN network are around 60 and 30°, 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 Fig. 3b. However, not all passes occur during nighttime. Fig. 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 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° 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.

4.2. Inter-satellite links

Results in Tables 1 and 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 is not within the scope of this work: A trade-off between simply launching more satellites versus increasing the complexity of individual satellites is required. Interestingly, there is, a

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.

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

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. Conclusions

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 do this by building a buffer of keys on board that can be quickly combined by an XOR operation and delivered to ground stations via a (classical communications) relay satellite. To optimize encryption key delivery such satellites are best launched into a sun-synchronous 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.

Acknowledgments

Sergio Loarte performed the bulk of the analysis for this work at the Centre for Quantum Technologies during an exchange stay. Hans Kuiper supervised Sergio 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 Minister's 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).

Appendix A

Table 3
Inputs for the key rate calculation.

Link parameters	Value	Source parameters	Value
Orbit altitude [km]	500	Quantum signal wavelength [nm]	848.6
Divergence transmitting telescope full-angle [murad]	10	Weak coherent pulse source frequency [Mhz]	100
Pointing error of pointing and tracking system [murad]	1.2	Signal state mean photon number [−]	0.8
Diameter of receiving telescope [m]	1	Weak decoy state mean photon number [−]	0.1
Atmospheric absorption loss at zenith [dB]	−3.2	Vacuum decoy state mean photon number [−]	0
Detector dead time [ns]	100	Fraction of pulses that are signal [−]	0.5
Efficiency detectors [−]	0.5	Fraction of pulses that are weak decoys [−]	0.25
Dark counts [cps]	25	Gate time [ns]	2
Optical efficiency [−]	0.16	Basis reconciliation factor [−]	0.5
		Error correction efficiency [−]	1.4742

Table 4
Detailed comparison of Micius pass on December 19, 2016.

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

Appendix B

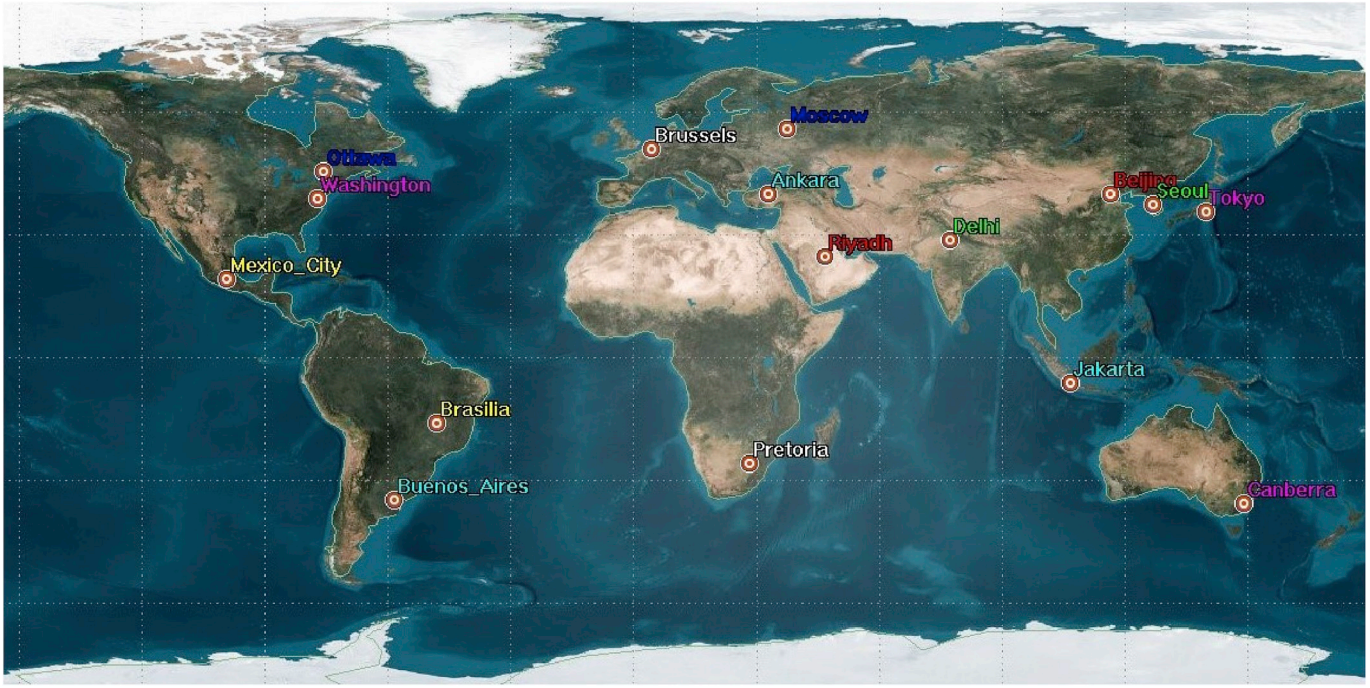

Fig. 4. G20 ground stations

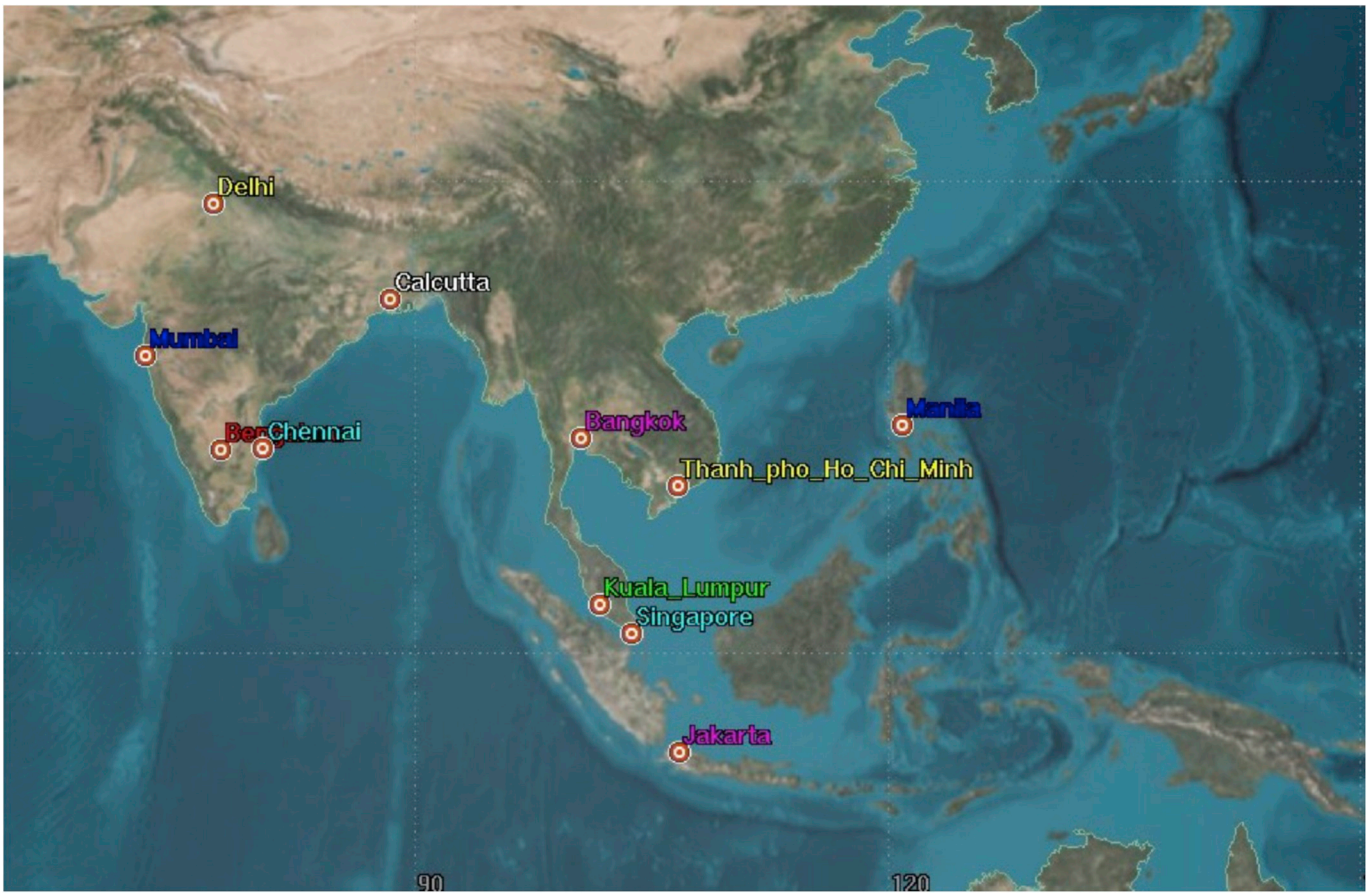

Fig. 5. Indo-ASEAN ground stations

Appendix C

The embassy model is a specific use case for encryption keys that applies to an embassy sending a distributed message to embassies in major cities around the world. A simple case is illustrated here: Embassy A intends to send a message to embassies B,C,D and E. The most secure use of keys is one-time pad encryption, meaning that the key held by embassy A (key A is simply the key shared between embassy A and a satellite), must be split into four equal parts because any section of key material can only safely be used once. It now depends on the amount of key each embassy shares with the satellite: either embassy A limits the size of the message, or one of the receiving embassies does. These cases are shown here in Fig. 6 and Fig. 7, respectively. This process is repeated for all satellites in the constellation resulting in the final distributed message that embassy A can send securely.

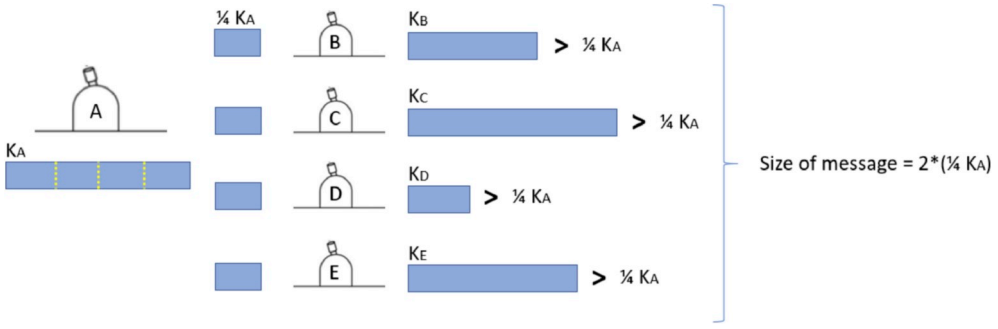

Fig. 6. Use of key material for distributed message not limited by receiving embassies [18]

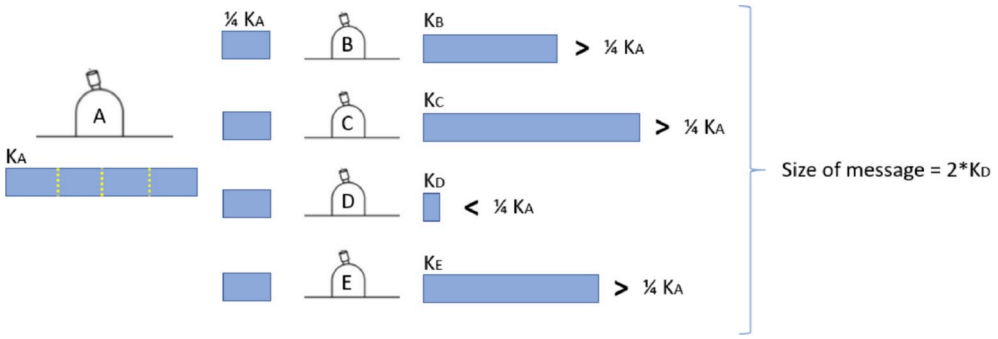

Fig. 7. Use of key material for distributed message restricted by one of the receiving embassies [18]

References

[1] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography, Rev. Mod. Phys. 74 (1) (2002) 145–195, https://doi.org/10.1103/RevModPhys.74.145 https://link.aps.org/doi/10.1103/RevModPhys.74.145.

[2] R. Bedington, J.M. Arrazola, A. Ling, Progress in satellite quantum key distribution, NPJ Quant. Inform. 3 (1) (2017) 30, https://doi.org/10.1038/s41534-017-0031-5 http://www.nature.com/articles/s41534-017-0031-5.

[3] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, J.-W. Pan, Satellite-relayed intercontinental quantum network, Phys. Rev. Lett. 120 (3) (2018) 30501, https://doi.org/10.1103/PhysRevLett.120.030501 http://arxiv.org/abs/1801.04418.

[4] R. Courtland, China's 2,000-km quantum link is almost complete [News], IEEE Spectrum 53 (11) (2016) 11–12, https://doi.org/10.1109/MSPEC.2016.7607012 URL http://ieeexplore.ieee.org/document/7607012/.

[5] J.-P. Bourgoin, E. Meyer-Scott, B.L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, T. Jennewein, Review A comprehensive design and performance analysis of low Earth orbit satellite quantum communication, New J. Phys. 15 (2) (2013) 023006, , https://doi.org/10.1088/1367-2630/15/2/023006 http://arxiv.org/abs/1211.2733 http://stacks.iop.org/1367-2630/15/i=2/a=023006?key=crossref.e2000769db1ac53dcdfd7826a722c51a.

[6] E. Kerstel, A. Gardelein, M. Barthelemy, T.C. Team, Nanobob : A Cubesat Mission Concept for Quantum Communication Experiments in an Uplink Configuration, (2017), pp. 1–37 arXiv (November).

[7] F. Steinlechner, P. Trojek, M. Jofre, H. Weier, D. Perez, T. Jennewein, R. Ursin, J. Rarity, M.W. Mitchell, J.P. Torres, H. Weinfurter, V. Pruneri, A high-brightness source of polarization-entangled photons optimized for applications in free space, Optic Express 20 (9) (2012) 9640–9649, https://doi.org/10.1364/OE.20.009640 http://www.ncbi.nlm.nih.gov/pubmed/22535055.

[8] D. Naughton, R. Bedington, S. Barraclough, T. Islam, D. Griffin, B. Smith, Design considerations for an optical link supporting intersatellite quantum key distribution, Opt. Eng. 58 (1) (2019) 1, https://doi.org/10.1117/1.OE.58.1.016106 https://www.spiedigitallibrary.org/journals/Optical-Engineering/volume-58/issue-1/016106/Design-considerations-for-an-optical-link-supporting-intersatellite-quantum-key/10.1117/1.OE.58.1.016106.full.

[9] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, M. Toyoshima, Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite, Nat. Photon. 11 (8) (2017) 502–508, https://doi.org/10.1038/nphoton.2017.107 http://www.nature.com/doifinder/10.1038/nphoton.2017.107.

[10] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, P. Villoresi, Experimental satellite quantum communications, Phys. Rev. Lett. 115 (4) (2015) 040502, , https://doi.org/10.1103/PhysRevLett.115.040502 https://link.aps.org/doi/10.1103/PhysRevLett.115.040502.

[11] J.A. Grieve, R. Bedington, Z. Tang, R.C. Chandrasekara, A. Ling, SpooQySats: CubeSats to demonstrate quantum key distribution technologies, Acta Astronaut. 151 (September) (2018) 103–106, https://doi.org/10.1016/j.actaastro.2018.06.005 http://arxiv.org/abs/1710.05487 https://linkinghub.elsevier.com/retrieve/pii/S0094576518304405.

[12] I. Khan, B. Heim, A. Neuzner, C. Marquardt, Satellite-based QKD, Optic Photon. News 29 (2) (2018) 26, https://doi.org/10.1364/OPN.29.2.000026 https://www.osapublishing.org/abstract.cfm?URI=opn-29-2-26.

[13] A. Skander, M. Abderraouf, B. Malek, M. Nadjim, M.M. Al-Harthi, Study of LEO satellite constellation systems based on quantum communications networks, 2010 5th International Symposium on I/V Communications and Mobile Network, IEEE, 2010, pp. 1–4, , https://doi.org/10.1109/ISVC.2010.5656276 http://ieeexplore.ieee.org/document/5656276/.

[14] D. Elser, S. Seel, F. Heine, T. Scheidl, R. Ursin, Z. Sodnik, M. Peev, Network architectures for space-optical quantum cryptography service, Proc. International Conference on Space Optical Systems and Applications (ICSOS) 2012, Post-1, Ajaccio, Corsica, France, October 9-12 (2012) 12, 2012 http://icsos2012.nict.go.jp/pdf/1569657077.pdf.5Cnpapers3://publication/uuid/470A1984-5B03-48DD-BF63-8E096AC4CF6F.

[15] X. Ma, B. Qi, Y. Zhao, H.K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A Atom. Mol. Optic. Phys. 72 (1) (2005) 1–15, https://doi.org/10.1103/PhysRevA.72.012326 arXiv:0503005.

[16] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, J.-W. Pan, Satellite-to-ground quantum key distribution, Nature 549 (7670) (2017) 43–47, https://doi.org/10.1038/nature23655 http://www.nature.com/doifinder/10.1038/nature23655.

[17] NASA, Cloud statistics database (1 month - terra/modis), https://neo.sci.gsfc.nasa.gov/view.php.0AdatasetId=MODAL2_M_CLD_FR.

[18] S. Loarte, Towards a Global Space-Based QKD Network, Master Thesis, Delft University of Technology, 2019, http://resolver.tudelft.nl/uuid:d8a391e8-d21a-4f37-95ec-467a49d391ea.