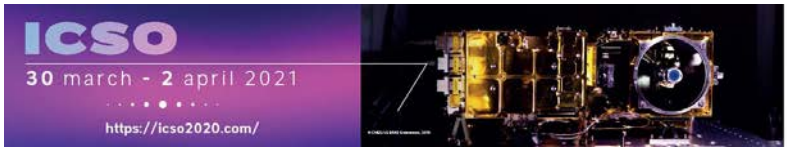
International Conference on Space Optics—ICSO 2020

Virtual Conference

30 March–2 April 2021

Edited by Bruno Cugny, Zoran Sodnik, and Nikos Karafolas



How to choose the best QKD network technology: three different satellite based scenarios compared

International Conference on Space Optics — ICSO 2020, edited by Bruno Cugny, Zoran Sodnik, Nikos Karafolas, Proc. of SPIE Vol. 11852, 118520Z · © 2021 ESA and CNES
CCC code: 0277-786X/21/$21 · doi: 10.1117/12.2599218

How to choose the best QKD network technology: Three different satellite based scenarios compared

Manuel Erhard[a], Armin Hochrainer[a], Matthias Fink[a], Johannes Handsteiner[a], Thomas Herbst[a], and Thomas Scheidl[a]

[a]Quantum Technology Laboratories GmbH, Wohllebengasse 4-4, 1040-Vienna, Austria

ABSTRACT

Quantum cryptography promises unconditionally secure communication. Today, there exists a vast array of different QKD protocols that claim to offer security. However, looking in more detail, many subtleties lead to different security levels, or in the worst-case to no security at all. Here, we introduce the most crucial QKD security properties, ranging from different attack schemes to actual implementation security considerations. We present three different QKD use-cases with different network topologies: one trusted-node-based scenario (BB84 decoy) and two trusted-node-free (entanglement-based BBM92 and twin-field QKD). Using our, in cooperation with the European Space Agency (ESA), in-house developed simulations package, we simulate all relevant performance parameters, including the expected finite secret-key-rate. Furthermore, we assess all simulated QKD protocols' applicability to satellite-based QKD networks and identify essential technologies. Interestingly, not the single-photon detection modules are the key drivers in terms of secure-key-rate performance, but the optical sending and receiving telescopes.

Keywords: Quantum Key Distribution, QKD, satellite-based QKD, QKD simulation

1. INTRODUCTION

Quantum key distribution (QKD) is a crucial technology for many countries and institutions, as it promises information-theoretically secure communication. From a scientific perspective, several different approaches on how such a quantum network could be set up exist.[1–3] From a practical point of view, the satellite-based DV-QKD networks represent a particularly promising variant.[4–6] They achieve distances and secure key rates previously unattainable and have already been successfully demonstrated between China and Austria.[5] Today European as well as international initiatives strive for a secure communication network based on quantum technology. An important question is how to choose the practically most secure and most efficient QKD network topology and technology from the vast number of scientific papers.

In this article, we investigate three different discrete variables (DV) QKD network scenarios. In doing so, we briefly review some critical properties of QKD protocols, such as their network topology, security, vulnerability to imperfect devices or side-channel attacks, and their achievable net key rate in the finite-sized key regime. We present a flow-down process starting with different user requirements and ending with actual technical specifications. To calculate the expected secure key rates in the various scenarios, we use the "Space-QKD-Simulator" software package developed by qtlabs in cooperation with the European space agency (ESA). This software tool enables us to simulate different satellite orbits, telescope sizes, and QKD protocols and compare the different application scenarios. Finally, a few key-technologies are identified that are necessary for high-performance satellite-based QKD networks.

Further author information: (Send correspondence to M.E. or T.S.)
M.E.: E-mail: manuel.erhard@qtlabs.at
T.S.: E-mail: thomas.scheidl@qtlabs.at

1.1 WHY SATELLITE BASED QKD NETWORKS?

Fiber technology is much more advanced than free-space optical communication technology. However, while in classical optical communications, repeaters or amplifiers can be used to overcome loss in optical fibers, such repeater technology does not yet exist for QKD applications. Quantum repeaters[7] would require quantum memories which are expected to be developed some time in the future, but are not yet practically useful.[8] An attractive alternative is free-space QKD since the losses of approximately 0.2dB/km from optical fibers are much smaller for free-space links. The Chinese Micius mission demonstrated trusted-node-free QKD over more than 1000km with a small, but positive secure key rate of 0.1 bits per second.[6] A fiber based system would experience approximately 200dB loss, which means that even at a repetition rate of sending 100GHz photon pairs per second it would take more than 200 years to send a single secure bit. This huge advantage in terms of achievable distance and the technological readiness makes satellite based QKD systems so attractive compared to fiber-based systems.

2. QKD NETWORK TOPOLOGY AND SECURITY

QKD networks are categorized in two distinct network topologies, the trusted-node-based, and the trusted-node-free topology. In the case of trusted-node-based topology, the secret key is always known to a trusted party. In contrast, the trusted-node-free scenario is designed such that only the two communication parties hold the secret key, no one else. Hence, from a security perspective, the trusted-node-free topology is favorable, since no trusted third party is involved. However, trusted-node-free topologies come at the prize of geographically limited coverage (depending on the orbit of the satellite) and lower secure key rates.

2.1 Theoretical security of QKD

Theoretically, a measure on how secure a QKD protocol is can be defined using the so-called security parameter $\epsilon_{\text{security}} = \epsilon_{\text{correct}} + \epsilon_{\text{secret}}$, which is composed of the failure probability $\epsilon_{\text{correct}}$ and the error probability of being leaked to an eavesdropper ϵ_{secure}. Typical values for the security parameter are $\epsilon_{\text{security}} = 10^{-10}$. It provides an upper bound of the probability that the secret key string fails, or the entire key is leaked to an adversary. A very important property of the security parameter is that it is universally composable.[9,10] It means that the generated secret key from the QKD protocol can be used in a classical encryption protocols such as the one-time pad, for example. This is called composability.

Besides the security parameter, the strength of the security proof against an eavesdroppers' attack strategy is also important. There are basically three different attack categories defined:

1. **Individual attack**
   This is the most constrained attack. Here, Eve attacks all systems going from Alice to Bob independently with the same strategy. Eve has no quantum memory available, which means she has to perform all her quantum operations before the classical post-processing. An important sub-family of individual attacks is the intercept-resend attack.

2. **Collective attack**
   In this attack scenario, Eve has access to a perfect* quantum memory which can store a complete sequence of n systems shared between Alice and Bob. However, here all quantum states are attacked identically using a collective operation.

3. **General or coherent attack**
   This attack family constitutes the most powerful attack strategy. Eve possess a perfect quantum memory and can entangle here quantum memory at will with the quantum signals and also use classical post-processing data by Alice and Bob to change the attack operation.

*meaning a quantum memory with unit efficiency and unit fidelity

A final important property of a QKD security proof is its capability to handle realistic scenarios of key length. No QKD session generates infinitely long keys. Thus, the security proof needs to be able to cope with finite key sizes and must take into account statistical fluctuations stemming from finite data collection.

Hence, an information-theoretically secure QKD proof must be universally composable, secure against coherent attacks, and valid in the finite key regime. Besides these important theoretical QKD proof properties, a physical system's actual practical implementation must be considered, as will be discussed in the next subsection.

2.2 Implementation security of QKD

As discussed in the previous sections, QKD promises information-theoretical security. However, we need to keep in mind that all QKD security proofs assume perfect devices and an identical implementation of the theoretical prescription in the practical QKD systems. In a real experimental scenario, there are no perfect devices. This leads to security loopholes, which differ in severity depending on the particular implementation and the QKD protocol. For example, in the BB84 protocol citeXXX, an attacker could use a tiny but detectable difference in wavelength present in the source for encoding the different quantum bits. Another famous hacking attack is the photon number splitting attack[11,12] which exploits the use of non-perfect single-photon sources, the detector inefficiency mismatch,[13] or blinding attack.[14] The exploitation of such unwanted information leakage or non-perfect behavior of devices due to realistic implementation is generally called "side-channel attacks". The theoretical security proof cannot, in principle, account for such hacking attacks. Fortunately, there are different strategies to cope with such vulnerabilities of QKD protocols. The most powerful is to minimize the theoretical assumptions within the security proof itself, which leads to device-independence[15] or partial device-independence such as source or measurement-device-independence (MDI).[16] The second approach is to take into account all known device imperfections at the privacy amplification step of the protocol. This approach requires the finding and patching of device imperfections and, as such, requires careful design and detailed monitoring throughout the complete planning, designing, building, and testing phases. A more detailed discussion on QKD protocols' implementation security is given in a white paper from the European Telecommunications Standards Institute (ETSI).[17]

3. FROM USER REQUIREMENTS TO BASELINE DESIGN FOR QKD NETWORKS

For any QKD network the most important requirements depend on the users needs. Thus it is of utmost importance to design and develop the complete QKD network from the viewpoint of the user. To simplify this process, we propose in Fig. 1 a three step flow-chart that allows a short and concise selection of the baseline design for a QKD network. First, the user defines whether a trusted-node-based or -free network topology is required. This choice determines the available QKD protocols. Finally, based on the geographical coverage requirements of the user, the orbital height for the satellite is selected.

For satellite based QKD networks in the trusted-node-free topology without relay satellites or quantum repeaters, operation can only be achieved within the possible geographical coverage of the satellite since simultaneous optical links of both ground stations with the satellite are necessary.

4. TECHNICAL IMPLEMENTATION OF QKD PROTOCOLS

As briefly discussed in the sections above, the actual technical implementation of a QKD protocol can have a severe impact on its security. Two equally important points to consider next to security are the performance in terms of secret key rates and long-distance capability of the QKD network. The proposed solution to enable long distance QKD networks here is to use a satellite-based approach. Especially for satellite-based QKD networks, the protocols' ability to handle high-loss scenarios is important.

4.1 HOW TO PHYSICALLY ENCODE QUANTUM INFORMATION

Photons are the ideal physical particles to transmit quantum information in a fast and reliable way. The reasons are that photons travel at the speed of light and do not interact with their environment easily. There are several degrees of freedom (DoFs) that allow encoding quantum information on a photon. The most widely used DoFs are polarization, time-bin, phase, and spatial modes, e.g., path or orbital angular momentum (OAM).

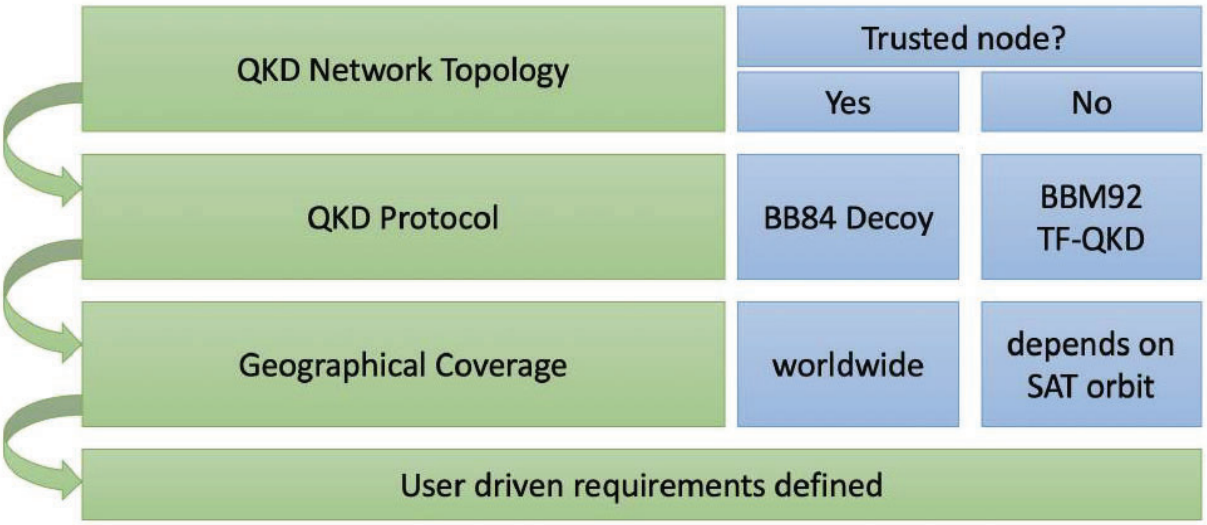


Figure 1. Description of a flow chart that results in user-driven requirements for a satellite-based QKD system. The most important property is the general QKD network topology. Here the potential user defines whether a trusted-node-based or -free QKD network is suited best. This network-topology choice then directly affects the available QKD protocols and also whether a global or Europe-wide operation is possible.

In this survey, we focus on DV encoding based on single-photon detection. Recently, CV-QKD was considered for use in satellite-based QKD.[18–20] While academically interesting, we think it is practically not applicable in a satellite scenario for the following reasons: The expected total loss of satellite-based QKD networks is usually above 10dB. However, CV-QKD security proofs considering realistic implementation schemes[†] and an excess noise level of 0.01 shot-noise-units are secure only below 5dB total loss.[21] More recent studies, claiming long-distance capability, ignore this fact and use security proofs that do not adequately describe the physical system employed, leading to implementation security loopholes. Since CV-QKD relies on homo- or heterodyne measurement techniques[‡], adaptive optical systems are unavoidable in satellite-based scenarios. While this is not impossible to implement, it certainly goes beyond standard telecom equipment. It hence renders the main argument against the use of DV-QKD, namely being cost-effective invalid. Nevertheless, this does not apply in general for fiber-based intra-city QKD networks (20km diameter), where the expected optical losses are below 5dB. We thus conclude that CV-QKD is best suited for fiber-based systems in short-range intra-city QKD networks and DV-QKD for long-range satellite-based QKD networks.

For DV-QKD, the polarization degree-of-freedom of single photons is arguably the best choice for free-space satellite-based QKD systems. The first reason is that polarization is insensitive to atmospheric turbulence (see Micius mission). The second reason is that the two mutually unbiased quantum measurements are perfectly suitable for free-space links without the necessity of adaptive optical systems (in contrast to time-bin or OAM, as detailed below). Furthermore, the polarization measurements can be performed with 100% efficiency, unlike the time-bin DoF, which is limited by 50% for the passive measurement setup, see below. Additionally, the key rate per pulse is maximized for polarization since every pulse contains one bit.

Encoding a quantum bit in the time-bin DoF is an attractive option since it is robust against atmospheric turbulences in principle. Time-bin QKD is especially advantageous using fiber-based systems since the measurement requires interferometers, and the spatial modes are automatically matched in optical fibers. However, this is not the case for free-space applications, and specifically designed unbalanced interferometers using 4f-optical

[†]such as approximate and discrete Gaussian modulation of the random sampling for the coherent states, and without taking finite key sizes into account

[‡]which is interference between the quantum signal and a local oscillator

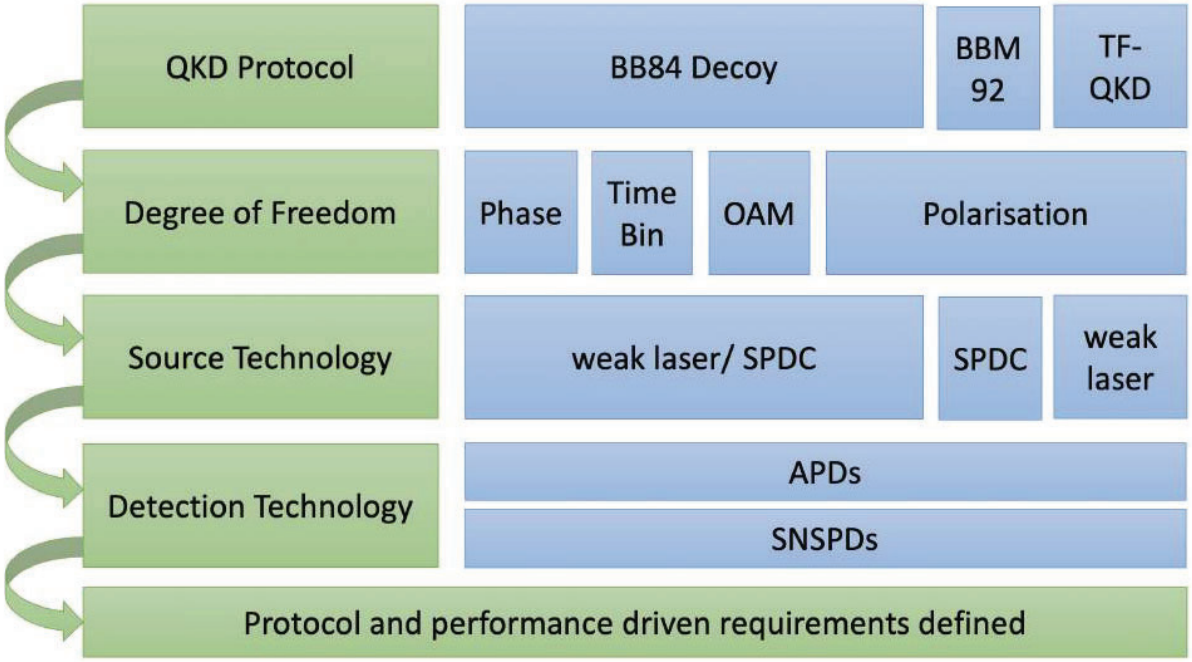


Figure 2. Description of a flow chart that results in protocol and performance-driven requirements for a satellite-based QKD system. First, a physical degree-of-freedom (DoF) to encode a quantum bit on a photon is choosen. The most frequently used DoFs are polarisation, time-bin, phase and orbital-angular-momentum (OAM). Except for the phase encoding, all other DoFs can be used for either BB84-Decoy or BBM92 protocols. Phase encoding is applicable to BB84 and TF-QKD. The chosen QKD protocol also determines the source technology, weak coherent pulses can be used in BB84-Decoy and TF-QKD, while BBM92 is based on entangled photon sources using spontaneous parametric down conversion (SDPC). Lastly, the detection technology is to be determined. Two fundamentally different technologies are available, avalanche photon detectors (APDs) and superconducting nanowire single photon detectors which can both be used for all QKD protocols.

systems are needed to compensate for the angle-of-arrival fluctuations from the free-space optical link. We should also mention that time-bin encoding requires two pulses to encode one bit. This fact results in only half the information capacity compared to polarization DoF per pulse. While it is possible to design a 100% efficient detection scheme in principle, it is technologically very demanding, since switching must be performed between two consecutive pulses (1ns). For those reasons, we do not consider time-bin as the best possible choice in our use-cases.

The orbital-angular-momentum DoF of single photons is mostly used in high-dimensional QKD applications due to its possibility of encoding higher-dimensional information. This allows to surpass the usual information capacity per pulse beyond 1bit and promises higher resilience to noise. However, in practice, the higher resilience to noise can also be mitigated by using a DoF insensitive to atmospheric turbulence (e.g. polarization). Furthermore, OAM modes are susceptible to atmospheric turbulence since their information is contained in the optical beam's spatial structure. Thus, without the use of an AO system, OAM cannot be utilized in practice with high key rates. OAM DoF's measurement also exploits interferometric techniques, which are possible in the laboratory under well-controlled conditions, but not suited for free-space links without AO systems.

We summarize the most important properties of all DoFs for free-space optical QKD scenarios in table 1 and note that our analysis here specifically applies to free-space optical links. The situation might very well be different for a fiber optical QKD network.

DoF	Information capacity [bits/pulse]	AO system required	measurement technology	measurement efficiency	suitable QKD protocols
Polarization	1	no	polarizing beam splitter & half-wave-plate	passive 100%	BB84/BBM92
Time-Bin	0.5	no	interferometer	passive 50%	BB84/BBM92
Phase	0.5	no	interferometer	passive 50%	BB84/TF-QKD
OAM	1	yes	interferometer	passive 100%	BB84/BBM92

Table 1. Comparison of different degrees of freedom (DoFs) to encode quantum information using photons.

5. THREE CASE STUDIES

In this section, we present three case studies based on three potential use cases. The first use-case regards a customer that demands a trusted-node-based and world-wide operating QKD system. For example, the customer could be the European Union that hosts a LEO satellite constellation that keeps all trusted nodes exclusively within the organization and provides a world-wide operation to connect all the embassies securely. Hence, from Fig. 1 it is clear that for that case, that we select the BB84-Decoy protocol. Further details are presented in section 5.1.

The second use-case regards a public QKD network provider with government or private customers. To ensure the highest security, the public QKD network provider demands a trusted-node-free QKD network topology. We, therefore, follow the flow chart depicted in Fig. 1 and choose either an entanglement-based BBM92 or twin-field TF-QKD protocol. Since both these protocols are trusted-node-free and require simultaneous connection to the satellite, the geographical coverage is limited by the chosen orbital height, as detailed in section 5.2. The main technical difference between BBM92 and TF-QKD is that the latter requires optical up-links, significantly increasing the expected optical channel losses. However, due to its unique physical security principle, only one optical link loss counts. A remarkable property of the BBM92 protocol is that it is compatible with a trusted-node-based BB84 (Decoy) QKD network.

5.1 BB84 Vacuum+Weak Decoy

In our first use-case, we study a QKD network based on trusted-nodes hosted by LEO satellites. A trusted-node QKD scenario is especially suited for an organization such as the European Union since it allows world-wide operation with trusted-nodes that are entirely under the organization's control. Furthermore, physical access is almost impossible at satellites which reduces the risk of hacking trusted-nodes significantly.

In the vacuum+weak decoy BB84 scenario, we consider a satellite that sends two different weak coherent laser pulses (different mean photon number) and a vacuum pulse with four different polarization states (H, V, D, A) to one optical ground station. As mentioned already, the satellite is considered secure and plays the role of the trusted node. We simulate the estimated secure-key-rate (SKR) for a LEO orbit at 500km height and several different sending and receiving (Tx, Rx) telescope sizes.

The source on the satellite for the vacuum+weak decoy BB84 QKD protocol consists of a quasi-pulsed weak coherent laser capable of producing two different mean-photon-number pulses with each four different polarization states. These two different mean-photon-number pulses, called signal (u) and decoy (v), occur with different ratios r_u and r_v for signal and decoy pulses, respectively. The vacuum pulses with 0 mean-photon-number pulses occur with probability $1 - r_u - r_v$. The signal and decoy pulses must be perfectly indistinguishable in all DoFs, including time, frequency, spatial modes, and polarization modes, to avoid side channel attacks. This perfect indistinguishability must be monitored and guaranteed at all stages of the development process. Another parameter that heavily influences the BB84 QKD protocol's performance in terms of achievable secure-key-rate is the repetition rate of the optical pulses Rep_rate. Here we assume a repetition rate of 1GHz.

The optical down-link loss simulations take diffraction of the Gaussian spatial modes, pointing jitter of the telescopes and reflection and transmission losses of the sending and receiving telescope and the atmosphere into account. The basic simulations follow the analysis given in.[22,23] In the optical downlink scenario, we do not need

Source Parameters:	**Down-Link Parameters**
Rep_rate=1e9 Hz	orbit=500km
u=optimized	wavelength=800*1e-9 m
v=optimized	pointingError_jitter_fullAngle=1e-6 rad
ru=0.75	linkLosses_atmosphere=1 dB
rv=0.125	linkLosses_dB_space=0 dB
Detector Parameters:	linkLosses_dB_ground=1 dB
eta_det=0.5	groundTerminalObscurationRatio=0.333
DCR=1000 Hz	**Post-processing parameters:**
Err_det=0.01	Effi_EC=1.1
tau_coinc=250e-12 s	epsilon_sec=1e-10
	blockSize=1e6 bits

Table 2. Simulation-parameter settings for the vacuum+weak decoy BB84 QKD protocol.

to take atmospheric turbulence into account since the angle-of-arrival fluctuations can be absorbed without loss by a proper design of the receiving telescope combined with the single-photon detection module without the need of any AO systems. Despite the orbital height and the respective sizes of the sending and receiving telescopes, the wavelength strongly influences the beam's geometrical divergence. Here we choose 800nm because of the smaller divergence angle as for 1550nm. The pointing-error-jitter is assumed to be 1μrad. The atmospheric losses are approximated with 1dB. The link losses in space can be set to zero because they can be measured in advance, and the mean-photon-numbers per pulse can be adapted to the losses. The ground station losses are estimated to be 1dB. The obscuration ratio between primary and secondary mirrors at the OGSs is set to 1/3.

For the detector parameter we choose values that are within reach for avalanche photo diode (APD) based single-photon detectors. Besides the single-photon detection efficiency (eta_det), the dark-count-rate (DCR) plays an important role. Here, the DCR includes the detector DCR and other sources of dark counts, such as stray light and light pollution in large cities. The detection error (Err_det) accounts for errors in the polarization detection system. Besides, errors stemming from imperfect sources, errors introduced in the optical transmission channel, and telescopes can be absorbed by this parameter. Using low timing-jitter detectors makes it possible to artificially shorten the detection window using ultra-fast-timing logic circuits and thus lower the impact of dark-counts. This time window is called tau_coinc.

The error correction efficiency (Effi_EC) is a value larger than 1, whereby 1 describes the Shannon limit. The security parameter (epsilon_sec) represents the probability of failure of the final key. The blockSize parameter defines the number of bits used for error-correction from the sifted key. The larger the block-size, the smaller the statistical fluctuations and thus the higher the secure-key-rate.

The simulation results presented in Fig. 3 are generated by the "Space-QKD-Simulator" package and the vacuum+weak decoy BB84 protocol analysis follows Ma *et al.*[24]

The simulation results presented in Fig. 3 show the dependence of the achievable secure-key-rate per second for different sending (Tx) and receiving (Rx) telescope diameters and elevation angles for a low altitude LEO orbit of 500km. As indicated by the results, the sizes of the sending and receiving telescopes heavily influence the performance of the vacuum+weak decoy BB84 QKD protocol. The reason is that the telescope sizes govern the free-space optical losses and the performance of all QKD protocols is determined by the losses of the quantum signal. For example, a sending telescope diameter of 0.35m in space in combination with a 0.4m telescope on ground allows a net secure-key-rate between 10^5 and 10^6 bits per second. This key rate includes error-correction, privacy amplification and takes a finite key block size of 10^6 bits and a security parameter of 10^{-10} into account. Furthermore, to achieve the 0.1-1Mbit/sec net SKR only standard APDs with an efficiency of 50% at 800nm and a source repetition rate of 1GHz are assumed. We note that while this simulation does not take into account all parameters and only roughly estimates the SKR of the protocol, the order of magnitude ???

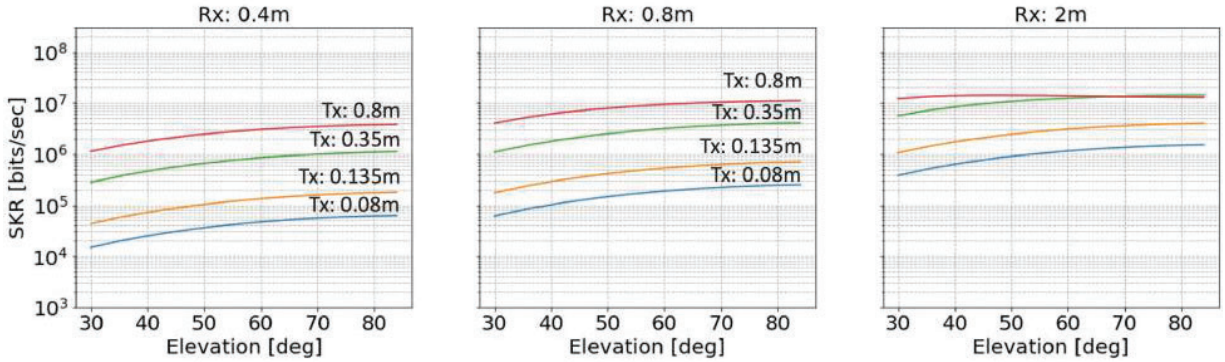


Figure 3. Simulation results from "Space-QKD-Simulator" package for the vacuum+weak decoy BB84 QKD protocol for various transmission (Tx) telescope sizes on the satellite and receiving telescope (Rx) sizes at the optical-ground-station. Note, for every elevation angle the optimal signal and decoy intensities are used.

5.2 BBM92 SPDC

As mentioned in the introduction, here we analyse a trusted-node-free entanglement-based BBM92 QKD network. Since this protocol requires the simultaneous connection of two optical-ground-stations to the satellite, the geographical coverage possible depends on the orbital height of the satellite. In Fig. 4 a couple of European capitals and their geographical location is shown. The respective distances are given in Table 3. If the QKD network provider's primary market is within the European Union, then the desired distances are up to 3300km, which corresponds to the distance between Lisboa and Helsinki, see Table 3. In order to guarantee the simultaneous visibility of the satellite to both optical-ground-stations (OGSs) located in Helsinki and Lisboa, a certain orbital height is necessary. Furthermore, we choose a minimum elevation angle of 30^o, and hence find according to the right part of Fig. 4 a required orbital height of approximately 1500km.

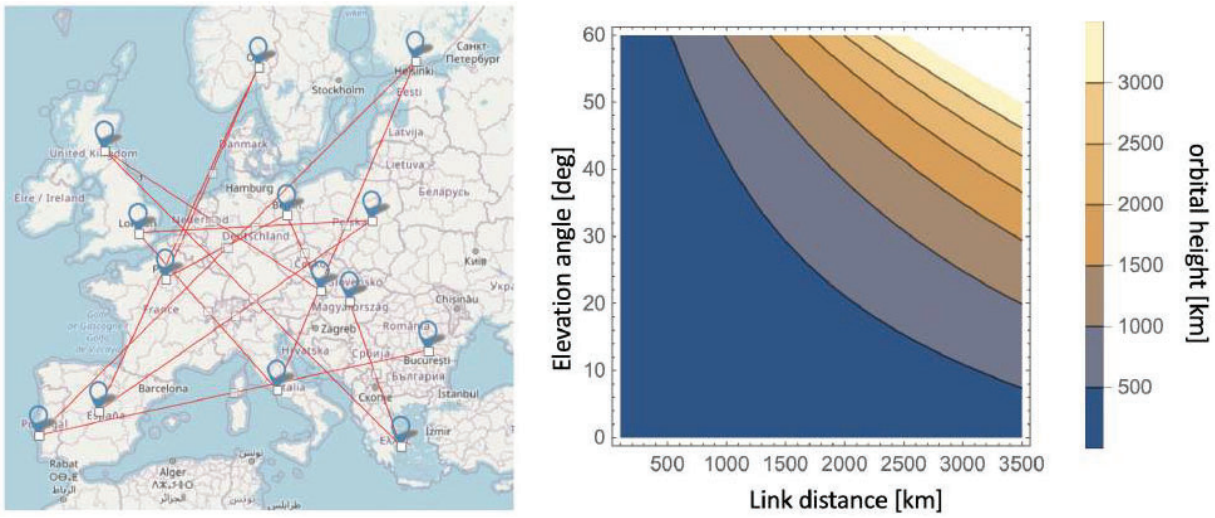


Figure 4. Geographical locations of some European capitals and their relative distance is presented in Table 3. The right inset shows the dependence of the achievable link distance, which is the distance between two ground-stations, with respect to the elevation angle and the orbital height. For example, to connect two OGSs that are 2000km apart with a minimum elevation angle of 20^o, an orbital height of >500km is required.

Since the QKD protocol and the orbital height is set to 1500km, the next step according to the flow chart in

Capital A	Capital B	Distance
Lisboa	Helsinki	3300km
Athen	Oslo	2600km
Athen	Edinbourgh	2800km
London	Vienna	1200km
Warsaw	Lisboa	2800km
London	Paris	350km
Paris	Berlin	900km
Berlin	Rome	1200km

Table 3. Distances of some European capitals depicted in Fig. 4.

Fig. 2 is to choose a DoF to encode the quantum information, an appropriate source, and detection technology. A public QKD provider is interested in the most flexible and cost-effective structure. Thus, we choose the polarization DoF because it is also perfectly compatible with a BB84-Decoy protocol and thus can be operated in a trusted-node-based mode around the world and can be implemented without the need of complex and expensive AO systems.

Since BBM92 relies on the distribution of entangled photon pairs, a source that can provide such entangled photon pairs in the polarization DoF is required. A perfectly suited technology here is spontaneous-parametric-down-conversion (SPDC).[25] Such sources can be characterized by three main parameters: the produced pair rate, the coupling efficiency, and the quality (fidelity) of the entangled states.

We basically follow the link loss simulations from the BB84-Decoy section here, except that for the BBM92 protocol we have two optical down-links simultaneously. The same also holds for the detection and post-processing parts of the simulation. The detailed simulation parameters are presented in Table 4.

Source Parameters:	**Down-Link Parameters:**
R_pair=1e9 Hz	orbit=1500 km
Coup_eff= 70%	wavelength=800*1e-9 m
Visibility H/V & D/A: 99%	pointingError_jitter_fullAngle=1e-6 rad
Detector Parameters:	linkLosses_atmosphere_dB= 1 dB
eta_det_A=50%	linkLosses_dB_space= 0.5 dB
eta_det_B=50%	linkLosses_dB_ground=1 dB
DCR_A=1000 Hz	groundTerminalObscurationRatio=.333
DCR_B=1000 Hz	**Post-processing parameters:**
Err_det_xx=0.2%	Effi_EC=1.1
Err_det_zz=0.2%	epsilon_sec=1e-10
tau_coinc=250e-12 s	blockSize=1e4 bits

Table 4. Simulation-parameter settings for the entanglement- based BBM92 SPDC QKD protocol.

The simulation results presented in Fig. 5 are generated by our "Space-QKD-Simulator" package, according to the simulation parameters defined in Table 4. The basic estimation of the secure-finite key follows the analysis given in Ma *et al.*[26]

The simulations results presented in Fig. 5 show the dependence of the achievable secure-key-rate per second for different sending (Tx) and receiving (Rx) telescope diameters and elevation angles for a high altitude LEO orbit of 1500km.

5.3 Measurement Device Independent TF-QKD

The twin-field (TF) phase-matching QKD protocol is based on single-photon interference on a beam-splitter hosted by the satellite. TF-QKD requires two optical links similar to the BBM92 protocol. In contrast to the BBM92 SPDC protocol, the TF-QKD protocol requires an optical uplink scenario, which inherently introduces

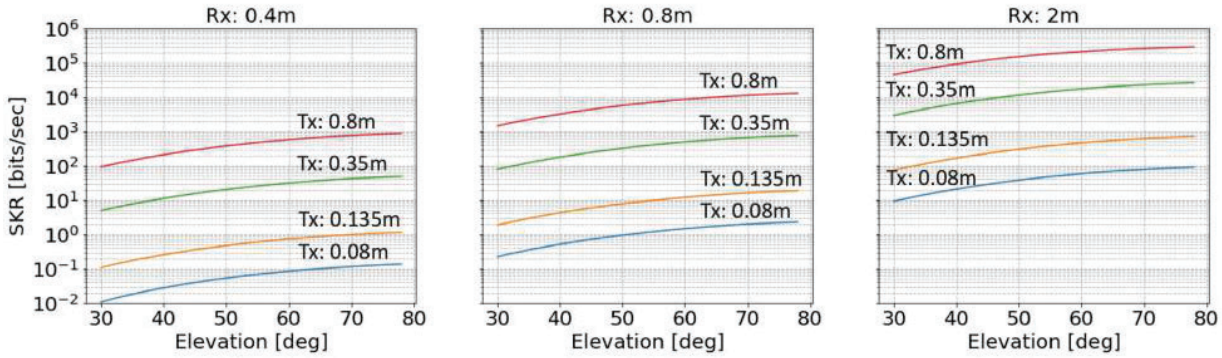


Figure 5. Simulation results from "Space-QKD-Simulator" package for the entanglement-based BBM92 SPDC QKD protocol for various transmission (Tx) telescope sizes on the satellite and receiving (Rx) telescope sizes at the optical-ground-station.

higher optical losses due to atmospheric turbulence close to the sender. Here, we take the atmospheric turbulence into account using the Fried-parameter and simulate different sending (Tx) and receiving (Rx) telescope diameters. Since MDI-QKD also represents a trusted-node-free network topology, we choose the same orbital height as the BBM92 protocol. This enables a comparison of the two protocols with regards to the achievable SKR.

Note, the blockSize does not refer to the detected signals but to the generated pulses. Hence, a blockSize of 10^{12} takes 10^3 seconds to accumulate at a repetition rate of 1 GHz. The detection error increases to a challenging but reasonable value of Err_det=3%. This error rate corresponds to of 94% interference visibility at the satellite of the two weak coherent pulses.

Source Parameters:	**Up-Link Parameters**
Rep_rate=1e9 Hz	orbit=1500km
u=0.09 mean photons/pulse	wavelength=800*1e-9 m
v=0.03 mean photons/pulse	pointingError_jitter_fullAngle=1e-6
ru=70%	linkLosses_atmosphere_dB=1
rv=25%	linkLosses_dB_space=1
D=16	linkLosses_dB_ground=0
Detector Parameters:	groundTerminalObscurationRatio=.333
eta_det=50%	**Post-processing parameters:**
DCR=1000 Hz	Effi_EC=1.1
Err_det=3%	epsilon_sec=1e-10
tau_coinc=250e-12 s	blockSize=100*1e10

Table 5. Simulation-parameter settings for the measurement-device-independent twin-field QKD protocol.

The simulation results presented in Fig. 6 are generated by our "Space-QKD-Simulator" package, according to the simulation parameters defined in Table 5. The basic estimation of the secure-finite key follows the analysis given in Ma *et al.*[27]

The simulation results for the satellite based MDI TF-QKD are presented in Fig. 6. In contrast to the previously investigated BB84 and BBM92 protocol, the TF-QKD protocol requires two simultaneous optical uplinks. The atmospheric turbulence cannot be neglected and is considered by different Fried-parameters ranging from 0.1m to 0.85m. The results in the first row in Fig. 6 represent a ground station telescope diameter of 0.8m and various receiving telescope diameters in space. For Fried-parameters below 0.35m, no SKR can be achieved. Hence, without adaptive optical systems, there is no realistic chance of gaining a positive SKR with TF-QKD. If a high-quality AO system is used that is capable to achieve an observable Fried-parameter of 0.35m or higher,

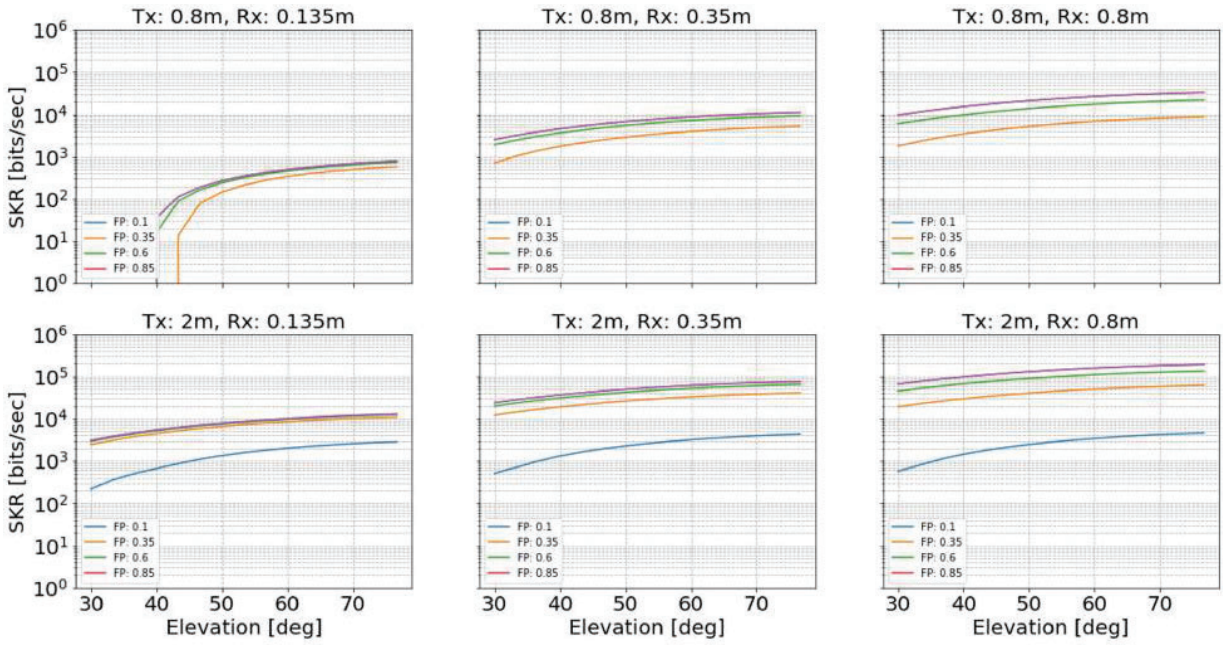


Figure 6. Simulation results from "Space-QKD-Simulator" package for the measurement device independent (MDI) twin-field (TF) QKD protocol for various transmission (Tx) telescope sizes at the optical-ground-station and receiving (Rx) telescope sizes at the satellite. Note, TF-QKD requires two simultaneous optical uplinks to one satellite. Hence, atmospheric turbulence plays an important role. We simulate different Fried-parameters, ranging from 0.1m, 0.35m, 0.65m, and 0.85m, to estimate the expected uplink losses and thereby the expected performance of MDI TF-QKD.

SKR between 1kHz and 10kHz can be expected. Note, these estimations assume a single photon interference visibility of 94% or higher. Using a very big sending telescope size on earth with a diameter of approximately 2m might allow to circumvent the use of AO systems, as depicted in the second row of Fig. 6.

To conclude this specific use-case we note that TF-QKD promises great resilience against loss especially in fiber QKD networks. In free-space applications, however, it requires the use of AO systems. This fact makes the overall system much more complicated. Hence, a final conclusion regarding TF-QKD vs. BBM92 cannot be drawn and a more detailed study is necessary.

6. CONCLUSION AND DISCUSSION

In conclusion, we used the "Space-QKD-Simulator" software package by qtlabs to simulate three different QKD protocols in various scenarios. The results, summarized in table 6, show that the optical space and ground telescopes play a decisive role in the QKD network's overall performance since their diameters govern the channel losses. Hence, in addition to developing sources and detectors, it is also of utmost importance to develop high-quality and precise (pointing $< 1\mu rad$) space telescopes with diameters larger than 0.35m. Similarly, it is also necessary for the optical-ground-stations to develop differently sized (0.4m, 0.8m) telescopes, including the required measurement apparatuses. In the selected case of polarization encoding, the measurement apparatuses are identical for both QKD network topologies (trusted-node-based and -free), do not require an adaptive optical system, and work 100% efficiently with standard optical devices. The selected APD technology is standard in a range of applications today. Note, the assumed specifications of 50% efficiency (at 800nm central wavelength) and a detection timing-jitter of 250ps are standard APD specifications and represent off-the-shelf products. Nevertheless, better single-photon detection specifications always increase performance. Especially low timing-jitters are desired to increase the effective repetition rate and thus increase the secret key rate.

	BB84-Decoy	BBM92 SPDC	TF-QKD
network topology	trusted-node-based	trusted-node-free	trusted-node-free
composable security†	yes	yes	yes
implementation security#	realistic	realistic	realistic
source techn.	weak laser	SPDC	weak laser
geographical coverage	World-Wide	Europe (3500km)	Europe (3500km)
space telescope diameter	0.35m	0.35m	0.35m
ground telescope diameter	0.8m	0.8m	0.8m
AO required	no	no	yes FP>0.5m
detector techn.	APD	APD	APD
post-proc. blocksize	1,00E+06	1,00E+04	1,00E+12
secure key rate	1-10Mbit/sec	0.1-1kbit/sec	1-10kbit/sec

Table 6. Summary of the main properties and results of the three different use-cases.
† composable security here refers to composable security proofs against general attacks
# with *realistic* we describe an almost perfect implementation of the security proof assumptions or the adequate inclusion of deviations thereof into the privacy amplification.

The source technology for BB84 decoy-based networks consists of standard telecom components but still needs further development to achieve a space-qualified technical readiness level (TRL). This also includes fast true quantum random number generators. For BBM92 entanglement-based protocols, probabilistic entanglement sources based on SPDC are currently well developed in terms of quality and performance. However, it is necessary to improve their TRL from basic laboratory demonstrations to space readiness. The last use-case study concerned a measurement-device-independent twin-field QKD protocol. Since this protocol also allows for a trusted-node-free operation, it can be compared to the BBM92 protocol. TF-QKD indeed promises a higher secure key rate than BBM92. However, it is necessary to use adaptive optical (AO) systems to keep the optical losses in the uplink scenario at a reasonably low level. Besides, it also requires two distributed coherent laser sources, and single-photon visibility of 94% was assumed. To verify these results and perform a realistic comparison, a much more detailed study beyond this activity is necessary.

Finally, the presented simulation results in Fig. 3, 5 and in Table 6 show that secure key rates around 1Mbit per second for trusted-node-based and 1kbit for trusted-node-free satellite-based DV-QKD networks are realistic. These simulation results are valid in the finite key-size regime with standard single-photon detectors. More detailed studies to be conducted in the future should also consider realistic weather conditions as well as real data for background dark-counts in populated urban areas.

ACKNOWLEDGMENTS

This work was funded by the European Space Agency (ESA) under contract number 4000128302/19/UK/AB. We thank Joan Fort Alsina (ESA), Luigi d'Arcio (ESA), Clemens Heese (ESA), and Jorge Piris (ESA) for their support and fruitful discussions throughout the activity.

REFERENCES

[1] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H., "Quantum cryptography," *Reviews of modern physics* **74**(1), 145 (2002).
[2] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M., "The security of practical quantum key distribution," *Reviews of modern physics* **81**(3), 1301 (2009).
[3] Xu, F., Ma, X., Zhang, Q., Lo, H.-K., and Pan, J.-W., "Secure quantum key distribution with realistic devices," *Reviews of Modern Physics* **92**(2), 025002 (2020).
[4] 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., et al., "Satellite-to-ground quantum key distribution," *Nature* **549**(7670), 43–47 (2017).
[5] Liao, S.-K., Cai, W.-Q., Handsteiner, J., Liu, B., Yin, J., Zhang, L., Rauch, D., Fink, M., Ren, J.-G., Liu, W.-Y., et al., "Satellite-relayed intercontinental quantum network," *Physical review letters* **120**(3), 030501 (2018).

[6] 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).

[7] Sangouard, N., Simon, C., De Riedmatten, H., and Gisin, N., "Quantum repeaters based on atomic ensembles and linear optics," *Reviews of Modern Physics* **83**(1), 33 (2011).

[8] Yu, Y., Ma, F., Luo, X.-Y., Jing, B., Sun, P.-F., Fang, R.-Z., Yang, C.-W., Liu, H., Zheng, M.-Y., Xie, X.-P., et al., "Entanglement of two quantum memories via fibres over dozens of kilometres," *Nature* **578**(7794), 240–245 (2020).

[9] Ben-Or, M., Horodecki, M., Leung, D. W., Mayers, D., and Oppenheim, J., "The universal composable security of quantum key distribution," in [*Theory of Cryptography Conference*], 386–406, Springer (2005).

[10] Renner, R. and König, R., "Universally composable privacy amplification against quantum adversaries," in [*Theory of Cryptography Conference*], 407–425, Springer (2005).

[11] Lütkenhaus, N., "Security against individual attacks for realistic quantum key distribution," *Physical Review A* **61**(5), 052304 (2000).

[12] Brassard, G., Lütkenhaus, N., Mor, T., and Sanders, B. C., "Limitations on practical quantum cryptography," *Physical review letters* **85**(6), 1330 (2000).

[13] Makarov, V., Anisimov, A., and Skaar, J., "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Physical Review A* **74**(2), 022313 (2006).

[14] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., and Makarov, V., "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature photonics* **4**(10), 686–689 (2010).

[15] Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., and Scarani, V., "Device-independent security of quantum cryptography against collective attacks," *Physical Review Letters* **98**(23), 230501 (2007).

[16] Lo, H.-K., Curty, M., and Qi, B., "Measurement-device-independent quantum key distribution," *Physical review letters* **108**(13), 130503 (2012).

[17] Alléaume, R., "Implementation security of quantum cryptography: Introduction, challenges, solutions," *ETSI White Paper* **27**, 28 (2018).

[18] Dequal, D., Vidarte, L. T., Rodriguez, V. R., Vallone, G., Villoresi, P., Leverrier, A., and Diamanti, E., "Feasibility of satellite-to-ground continuous-variable quantum key distribution," *npj Quantum Information* **7**(1), 1–10 (2021).

[19] Kish, S. P., Villaseñor, E., Malaney, R., Mudge, K. A., and Grant, K. J., "Feasibility assessment for practical continuous variable quantum key distribution over the satellite-to-earth channel," *Quantum Engineering* **2**(3), e50 (2020).

[20] Pirandola, S., "Satellite quantum communications: Fundamental bounds and practical security," *arXiv preprint arXiv:2012.01725* (2020).

[21] Ghorai, S., Grangier, P., Diamanti, E., and Leverrier, A., "Asymptotic security of continuous-variable quantum key distribution with a discrete modulation," *Physical Review X* **9**(2), 021059 (2019).

[22] Belland, P. and Crenn, J., "Changes in the characteristics of a gaussian beam weakly diffracted by a circular aperture," *Applied Optics* **21**(3), 522–527 (1982).

[23] Khwaja, T. S. and Reza, S. A., "Power transmittance of a laterally shifted gaussian beam through a circular aperture," *arXiv preprint arXiv:1605.04241* (2016).

[24] Ma, X., Qi, B., Zhao, Y., and Lo, H.-K., "Practical decoy state for quantum key distribution," *Physical Review A* **72**(1), 012326 (2005).

[25] Cao, Y., Li, Y.-H., Zou, W.-J., Li, Z.-P., Shen, Q., Liao, S.-K., Ren, J.-G., Yin, J., Chen, Y.-A., Peng, C.-Z., et al., "Bell test over extremely high-loss channels: towards distributing entangled photon pairs between earth and the moon," *Physical review letters* **120**(14), 140405 (2018).

[26] Ma, X., Fung, C.-H. F., and Lo, H.-K., "Quantum key distribution with entangled photon sources," *Physical Review A* **76**(1), 012307 (2007).

[27] Ma, X., Zeng, P., and Zhou, H., "Phase-matching quantum key distribution," *Physical Review X* **8**(3), 031043 (2018).