npj | Quantum Information

www.nature.com/npjqi

REVIEW ARTICLE OPEN

Progress in satellite quantum key distribution

Robert Bedington[1], Juan Miguel Arrazola[1] and Alexander Ling[1,2]

Quantum key distribution (QKD) is a family of protocols for growing a private encryption key between two parties. Despite much progress, all ground-based QKD approaches have a distance limit due to atmospheric losses or in-fibre attenuation. These limitations make purely ground-based systems impractical for a global distribution network. However, the range of communication may be extended by employing satellites equipped with high-quality optical links. This manuscript summarizes research and development which is beginning to enable QKD with satellites. It includes a discussion of protocols, infrastructure, and the technical challenges involved with implementing such systems, as well as a top level summary of on-going satellite QKD initiatives around the world.

npj Quantum Information (2017)3:30 ; doi:10.1038/s41534-017-0031-5

INTRODUCTION

Quantum key distribution (QKD) is a relatively new cryptographic primitive for establishing a private encryption key between two parties. The concept has rapidly matured into a commercial technology since the first proposal emerged in 1984,[1] largely because of a very attractive proposition: the security of QKD is not based on the computational hardness of solving mathematical problems, but on physical processes that are not vulnerable to powerful computers. As an example, in public-key encryption, the public keys and message transcripts can be stored and subjected to cryptanalysis at any time, and while they might be secure now, they might not be secure against newer, more powerful computers at some point in the future. In contrast, if the key generated from a QKD protocol is secure today, it will remain secure against advances in computing power. This property, known as 'forward security', makes it an ideal solution to ensure the secrecy of sensitive data that must be kept confidential for long periods of time. Furthermore, as QKD is primarily an optical technology, it has the ability to automate the delivery of encryption keys between any two points that share an optical link, which is advantageous given the growth of optical communication networks. In particular, QKD has the potential to replace or augment existing trusted-courier systems for secure transmission of encryption keys.

There are a variety of optical techniques for implementing QKD. The most common class of solutions encode each bit of private information onto discrete degrees of freedom of optical signals, and hence is termed collectively as discrete-variable QKD (DV-QKD). An alternative approach employs coherent communication techniques to encode the private information, and is known as continuous-variable QKD (CV-QKD). Both approaches have seen dedicated engineering that has led to increased key generation rates and improved compatibility with current communications infrastructure.[2–4] However, both approaches face a similar obstacle when attempting to implement wide-scale deployment of QKD: physical communication channels introduce transmission losses that increase exponentially with distance, greatly limiting the secure key rates that can be achieved over long ranges.

For any pure-loss channel with transmittance η, it has been shown that the secure key rate per mode of any QKD protocol scales linearly with η for small η.[5, 6, 7] This places a fundamental limit to the maximum distance attainable by QKD protocols relying on direct transmission. To put this into perspective, consider that a conventional telecommunications fibre with an attenuation of 0.18 dB/km[8] stretching over 1000 km has a theoretical transmittance of precisely $\eta = 10^{-18}$ worse in real-world deployments–making the resulting key rates forbiddingly small. The problem remains even if using state-of-the-art fibres which can reach attenuations of 0.142 dB/km.[9] Experiments have been reported where QKD was performed for distances of up to 404 km,[10] but the resulting key rates remain several orders of magnitude smaller than the requirements for practicable deployment. Sufficiently large key rates can only be obtained over metropolitan-scale networks, where the range is within 100 km.

In principle, it is possible to extend the range of QKD by using quantum repeaters. Some proposals for quantum repeaters rely on heralded entanglement generation and purification,[11, 12] while other recent architectures employ logical qubits capable of quantum error-correction to overcome both operational errors[13, 14] and errors due to loss.[15, 16] The difficulty of constructing such systems, however, is comparable to the challenges faced in building universal quantum computers, with the required technology unlikely to be available in the near future.

An alternative, which is viable with the present level of technology, is to use satellites as intermediate trusted nodes for communication between locations on the ground. By placing a satellite above the Earth's atmosphere, direct links can be established between ground stations and the satellite, thus enabling communication between distant points on the planet. Atmospheric attenuation in free space is less significant than in fibre, where for instance values of 0.07 dB/km can be achieved at

[1]Centre for Quantum Technologies, National University of Singapore, S15-02-10, 3 Science Drive 2, Singapore 117543, Singapore and [2]Department of Physics, 2 Science Drive 3 Blk S12, Level 2, Singapore 117551, Singapore
Correspondence: Robert Bedington (r.bedington@nus.edu.sg)
Robert Bedington, Juan Miguel Arrazola and Alexander Ling contributed equally to this work

Received: 5 March 2017 Revised: 7 July 2017 Accepted: 7 July 2017
Published online: 09 August 2017

2400 m above sea-level,[17] with higher attenuations at lower altitudes and negligible attenuation in the vacuum above the Earth's atmosphere. Dominant sources of loss in this case occur due to beam diffraction and the limited size of telescopes at the receiver. However, the overall effect is a greatly reduced amount of loss compared with ground-level transmission, making satellite QKD a promising route to enable secure key generation across global distances. Consequently, a number of efforts are under way to raise the technology readiness level of satellite QKD. These projects range from truck-based tests of pointing and tracking mechanisms,[18] to in-orbit testing of quantum light sources,[19] to full QKD demonstrations using orbiting satellites.[20] Altogether, these efforts will enable global QKD services as well as advanced fundamental experiments.[21]

In this review, we give an overview of the advances, challenges, and future directions of satellite-based QKD. We begin by discussing the basic concepts for performing QKD with satellites, regarding both protocols and infrastructure. We continue by discussing the technical challenges and progress towards realization in more detail. We conclude by giving a summary of existing quantum satellite initiatives around the world.

QKD PROTOCOLS

In this section, we give a brief overview of QKD, as well as the most commonly deployed protocols, which can be skipped by experts in the field. An in-depth review of QKD can be found in ref. 22 while a discussion of the frontiers of research in practical QKD appears in ref. 23.

QKD is a scheme for enabling two parties, commonly referred to as Alice and Bob, to derive a private and symmetric encryption key. As discussed in the previous section, QKD protocols can be divided into two main classes: DV-QKD or CV-QKD. In CV-QKD, information is encoded in the quadratures of randomly selected coherent states, which are then measured using either homodyne or heterodyne detection.[24, 25] From an implementation perspective, the optical tools are already very mature and widely used in conventional coherent communication schemes. However, significant challenges remain, such as in the need to decrease the classical communication between the two parties when establishing the final, secret key.[23, 25, 26] Most satellite QKD projects have chosen to implement discrete-variable schemes, and this paper will concentrate on DV-QKD concepts and technical solutions.

DV-QKD systems can be subdivided into prepare-and-measure or entanglement-based protocols. In a generic prepare-and-measure protocol,[1, 27, 28] Alice encodes each classical bit into an individual optical signal before transmitting it to Bob, who performs a prescribed set of measurements on each of the incoming signals in order to retrieve the classical data encoded in their states.

In the BB84 protocol,[1] which is the most widely deployed prepare-and-measure protocol, each classical bit is encoded into the polarization of an individual photon. Alice prepares the photon states by randomly choosing between the horizontal/vertical Z basis $\{|H\rangle, |V\rangle\}$ and the $+45°/-45°$ X basis $\{\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)\}$, where $|H\rangle$, $|V\rangle$ are single-photon states of horizontal and vertical polarization. The states in each basis are assigned bit values of 0 and 1 respectively, from which the encryption key can be established.

Once Alice has selected the basis, she randomly selects one of the two states and sends it to Bob. Upon receiving a signal from Alice, Bob randomly selects one of the two bases and performs a corresponding projective measurement, recording his outcome as a classical bit. After many signals have been sent, Alice and Bob publicly announce the basis they have chosen for each signal and they discard all cases, when they chose a different basis. Finally, they select a random subset of their data to estimate their relative errors. If the error rate is sufficiently low, they apply error-correction and privacy amplification to their data to reach a final shared secret key. An important consideration is that the transmitter, Alice, must have access to an active source of good random numbers in order to make both the basis choice and state choice. The recipient, Bob, needs also to be able to make a random choice on the measurement set, but this can be done passively, using beamsplitters.[29]

Due to a lack of robust, true single-photon sources, Alice's states are usually weak coherent states produced from laser sources, where each pulse has a finite probability of containing more than a single photon. To be more resilient against photon-number splitting attacks, an important innovation has been the creation of 'decoy-states',[30, 31] where Alice also chooses randomly between two intensities of her coherent state signals, which she reveals publicly to Bob after the quantum communication has been completed. The use of an additional degree-of-freedom, such as the intensity leads to improved tolerance to losses compared to regular BB84. Notably, these protocols can be currently deployed with commercial off-the-shelf components.

Entanglement-based protocols[32, 33] differ from prepare-and-measure systems by removing the need for an active choice when encoding states into the photons. Instead, both parties are recipients who share a source of maximally entangled photon pairs. Typical implementations utilize photon pairs entangled in the polarization degree of freedom, and the photon pair is split such that one photon is transmitted to Alice, while its twin is transmitted to Bob. Both parties make independent measurement choices on the photons, and decide to measure them in either the X or Z basis. In the most popular entanglement-based protocol known as BBM92,[32] Alice and Bob perform parameter estimation, error correction, and privacy amplification in the same manner as in the BB84 protocol. This protocol has the advantage that no active random number generators are required for preparing the source, and that the measurement devices for Alice and Bob are identical.

In an alternative entanglement-based approach, the E91 protocol,[33] the measurement scheme must result in a statement on whether the photon-pair correlations between Alice and Bob violate the Bell inequality. This protocol is the precursor of device-independent QKD schemes proposed much more recently.[34] From a practical perspective, the measurement scheme in E91 is less efficient in its use of photon pairs as the Bell inequality test requires more polarization settings to be monitored.[35]

CONCEPTS FOR SATELLITE QKD

In this section, we provide a high-level description of some different conceivable approaches for performing satellite QKD, which can be classified depending on the types of communication links that can be established, as well as the orbit of the satellite.

From a general perspective, most projects envision the satellite as a flying trusted-node (see Fig. 1). In this scenario, the satellite carries out QKD operations with distinct ground stations to establish independent secret keys with each of them. The satellite holds all keys, while the stations only have access to their own keys. To enable any pair of stations–for example, station A and B–to share a common key, the satellite combines their respective keys K_A and K_B and broadcasts their bit-wise parity $K_A \oplus K_B$. Using this announcement, the stations can retrieve each other's keys because $K_A \oplus (K_A \oplus K_B) = K_B$ and $K_B \oplus (K_A \oplus K_B) = K_A$. Since the original keys are independent secret strings, their bit-wise parity is just a uniformly random string, so the parity announcement does not reveal any useful information to potential eavesdroppers. However, since the satellite holds all keys, access to the data obtained by the satellite would give an adversary complete knowledge of the key. Therefore, in this setting, the satellite must be trusted.

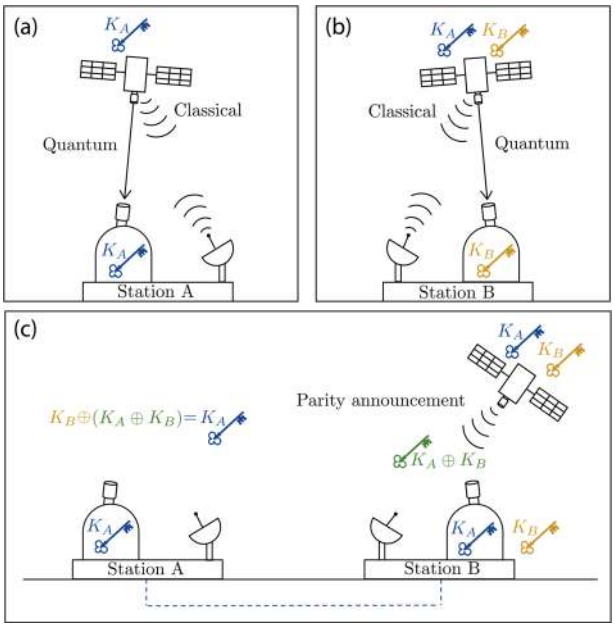

Fig. 1 Illustration of the most common satellite QKD scheme: the flying trusted-node. In step **a**, the satellite establishes a shared secret key K_A with station A by running a QKD protocol, which requires both classical and quantum communication. This step is repeated in **b** to establish a shared secret key K_B, this time with station B located further away. At the end of these steps, the satellite holds both keys, while each station knows only their own. Finally, in step **c**, the satellite publicly announces the parity of both keys $K_A \oplus K_B$. This allows station B to determine key K_A, which can then be used to encrypt private communications to A and vice versa

Trusted-node topologies are being built for fibre networks,[36] but ground-based nodes are fixed locations that can be subject to constant surveillance and probes. Side-channel attacks on QKD hardware that require access to the optical link[37] can face significant challenges in satellite scenarios where the optical link is moving relatively quickly. Most side-channel attacks are aimed at retrieving the key, and are distinct from denial-of-service attacks where the goal is to disable the satellite receiver, e.g., by aiming a sufficiently intense beam at the satellite optical transceiver. Denial-of-service attacks may be less of an issue if the satellite is only a transmitter. Additional research is needed however, to better understand potential vulnerabilities in satellite QKD.

Quantum communication links with a satellite can be classified either as uplinks–where the ground station sends signals to a receiver in space–or downlinks, where the satellite sends the signals to the ground. Correspondingly, there are several possible configurations for performing QKD with satellites depending on the types of links that are used.[21, 38–41] These are illustrated in Fig. 2.

There are advantages and disadvantages associated with each configuration, but the more commonly recommended scenario for operational QKD–and the only one that has thus far been demonstrated[42]–is to use downlinks. This is because downlinks always have lower losses for any ground-satellite segment. This arises because atmospheric properties such as turbulence cause the optical beam to wander, which translates into a less accurate ground transmitter compared to a space-based transmitter. This is discussed in more detail in Section 'Optical links'.

The main advantage of using an uplink is that it is not necessary to locate a (potentially complex) quantum light source in space, but only to place a receiver on board the satellites.[43, 44] It also makes attacks that target receivers significantly more difficult.[45]

It is also possible to achieve a downlink by using retro-reflectors on the satellite, which modulate signals sent from the ground as they bounce off back to a receiver also on the ground.[46] The challenge here is to develop fast modulating retro-reflectors, and to develop countermeasures that prevent an eavesdropper from sampling the state of the retro-reflector while QKD is being carried out.

Using downlinks also gives rise to the possibility of option 4 in Fig. 2. A source of entangled photon pairs can be located in the satellite, and all of the photon pairs transmitted to ground—one photon in each pair to one ground station, and the other in each pair to a second ground station.[20, 41] This configuration allows the realization of entanglement-based QKD directly between the ground stations, without using the satellite as a trusted node. The Chinese Micius satellite[47] has successfully demonstrated entanglement swapping over 1200 km to two mountain-top observatories using this, option 4, configuration. The 64–70 dB losses they experience are comparable with those predicted in studies[48] but make practicable QKD challenging.

In the Micius demonstration a Bell inequality test between the two ground stations proves that the photons are entangled. Since the photons are entangled, no other party, including the satellite, has made a measurement on them previously. This scenario only works when both ground stations simultaneously have line-of-sight to the satellite. Also at wider separations slant angles would be low, so the optical link would have to traverse longer distances, and thus more atmosphere, than a direct, overhead pass. The losses are so high because the losses in both arms are effectively combined since only photon pairs that arrive at both stations can be used.

It has also been suggested that sources of entangled photons in space could be employed as quantum repeater stations, enabling entanglement swapping among more distant locations on the ground.[49] As more quantum ground stations come online more complex network architectures will become necessary[50] and will likely include inter-satellite quantum links.[51]

The characteristics of the communication links are themselves dependent on the specific orbit of the satellite.[40] Orbital altitudes are classified into three main categories: Low Earth orbit (LEO), Medium Earth orbit (MEO), and Geostationary orbit (GEO).[52] LEO are situated between 160 to 3000 km in altitude (usually below 900 km), GEO has an altitude of precisely 35,786 km, while MEO correspond to all orbits between LEO and GEO. For satellite QKD applications, LEO and GEO are the two most suitable options. Although most current programmes opt for LEO, future projects might seek higher altitudes.[50] A satellite in LEO benefits from proximity to the surface which significantly reduces losses due to beam diffraction. The drawbacks in this case are the high speed of the satellite relative to surface of the Earth, which makes it challenging to achieve accurate pointing during signal transmission, as well as the fact that QKD can only be performed during the limited flyover time of the satellite. On the other hand, the situation is essentially reversed in GEO; the satellite is at rest relative to the ground, but it is located at a much higher altitude, where QKD can in principle be run continuously, but at the expense of much higher losses.

Polar LEO will pass ground stations at the poles with every orbit and equatorial LEO will pass ground stations on the equator with every orbit, but other orbital inclinations and ground station locations will have less regular passes. The time of day of the flyovers will also vary unless the orbit is specially chosen to be sun synchronous. The Micius satellite for example is in a 500 km sun synchronous orbit so that it passes over the Xinglong ground station for 5 min every night at around 0050 h local time.[42] In comparison, a night-time-operating QKD satellite in the International Space Station orbit–which is partway between a polar and an equatorial orbit–would have about 150 usable night time passes over a ground station at 40° latitude during a period of 12 months.[53]

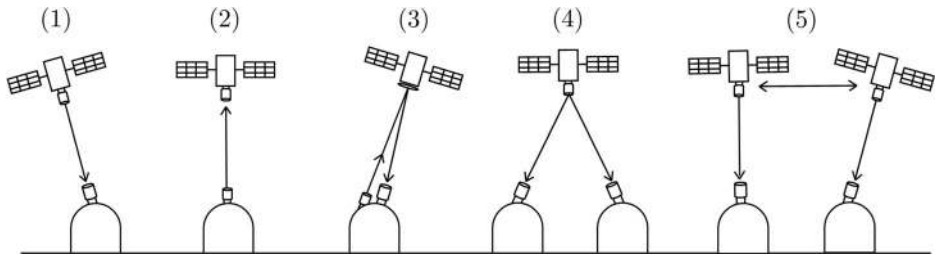

Fig. 2 Illustration of different platforms for performing satellite QKD. Scenarios (1) and (2) depict a downlink and an uplink, respectively, while in scenario (3) a downlink is simulated by using a retro-reflector on board the satellite. In (4) pairs of entangled photons are being transmitted to Earth so that two ground stations can share entangled states. Finally, scenario (5) illustrates how inter-satellite links can allow more complex satellite QKD networks

It should be noted that GEO orbits place the satellites above the equator, so the satellite is closer to the horizon for locations that approach the poles, disappearing below the horizon at 81° latitude. In these cases, the optical link must traverse a much larger amount of atmosphere and will suffer additional loss. Satellite QKD for such locations might adopt less conventional orbit choices, such as the Molniya highly elliptical orbits[54] used to provide polar regions with near-constant satellite coverage.

TECHNICAL REALIZATION

Satellite QKD proposals typically employ polarization encoding of individual photons, as this is well suited to free-space communication. When using polarization encoding, the photons are obtained either from a weak coherent pulse (WCP) source or from polarization-entangled photon-pair sources. A minority of proposals investigate options for time-bin entanglement,[55] or QKD with orbital angular momenta of photons,[56] but these approaches are less mature. Their appeal lies in the possibility of generating hyper-entangled states, where multiple quantum states can be encoded into a single photon.

Development towards the realization of polarization encoded, satellite-based QKD can be traced to the early demonstrations of free-space QKD using both weak coherent pulses and entangled photons. By 1998, Buttler et al. had produced 1 km outdoor QKD links for night-time operations,[57] later extending that to 1.6 km with daytime operations.[58] Other research groups went on to achieve longer links, from 10 km[59] to 23.4 km[60] to 144 km.[17] In 2016 the Micius satellite began performing QKD between space and ground which, at its maximum, is spanning a distance of 1200 km.[42]

Space-based instruments represent serious design challenges, as size, weight, and power are limited on spacecraft. Robustness is also important as the satellite launch process is not gentle, yet precise optical alignments must be maintained. Finally, the space environment requires special considerations to allow for the satellite to survive the vacuum, microgravity, radiation, and thermal environments it experiences in orbit.[61]

In the subsections below we review some technical details and challenges that have been published in this field, from the photon sources, to the optical links, to the quantum receivers and communications overheads.

Photon sources

Significant progress has been made in the design of weak coherent pulse sources used to generate photons in most BB84 schemes[62, 63] (Fig. 3a). One of the bottlenecks towards high-speed BB84 schemes was the need for active polarization manipulation, which is both power-intensive and slow. This limitation was overcome in a design which used four laser diodes inside a single transmitter.[62] By utilizing the high degree of polarization intrinsic to the diodes, this enabled each diode to be identified with a unique polarization state. A drawback of this approach is that the spectra of the diodes are not always identical and provide a possible side-channel for eavesdroppers.[64] This side-channel was closed in a recent development where a single laser diode was coupled to four (direct-write) waveguides, each of which was capable of a fixed amount of polarization rotation.[65] The waveguides were then recombined to result in a single-mode output with four possible polarization states. An added advantage of this design is its small form-factor, enabling it to be considered as a transmitter for both ground or satellite segments.

The Micius satellite performs space-to-ground BB84 QKD using 850 nm photons from eight fibre-based laser diodes–four for signal and four for decoy states–pulsed at 100 MHz.[42] An alternative design could use variable strength lasers, which might additionally be able to function as a laser beacon (see Section Pointing, acquisition and tracking).[53]

Retroreflector schemes use ground-based light sources, which can be quite powerful–not themselves WCP–because it is only the reflected pulses from the retroreflector that need be in the weak coherent state. For synchronization purposes, such QKD photons could be combined with the pulse train from a satellite laser ranging system.[46] To use these setups to perform BB84 QKD the photons leaving the source would all have the same polarization, which would be modified by the satellite upon reflection by a polarization-modulating retroreflector. Significant development work is likely to be necessary to produce a retroreflector that could be modulated at sufficiently high rates with sufficiently high contrast ratios. There would also need to be various compensation devices to overcome the effects of the satellite motion, and as with many QKD systems, irradiance measurements would need to be taken to look out for eavesdroppers,[37] i.e., to check that no eavesdropper laser was also interrogating the retroreflector.[66]

The QKD schemes that utilize entanglement almost all rely on polarization entangled photon-pair sources based on bulk-crystal, collinear, spontaneous parametric downconversion (SPDC), either periodically-poled potassium titanyl phospate (PPKTP) or single-domain crystals such as beta barium oxide (BBO).[47, 67–71]

A PPKTP-based design[70] was identified by the European Space Agency for the original Space-QUEST proposal[41] and for the double-downlink demonstrations the Micius satellite uses a PPKTP source in a Sagnac interferometer arrangement, shown if Fig. 3b.[47] Sagnac-loop arrangements are auto-compensating allowing the spectral characteristics of the source to be tuned without requiring specifically modified birefringent walk-off compensation crystals.[72] The Micius source generates entangled photon pairs of ~810 nm at a rate of ~5.9 million per second under a pump power of ~30 mW. It uses a thick titanium alloy baseplate and Invar mounts for thermal and mechanical stability. It also has piezo

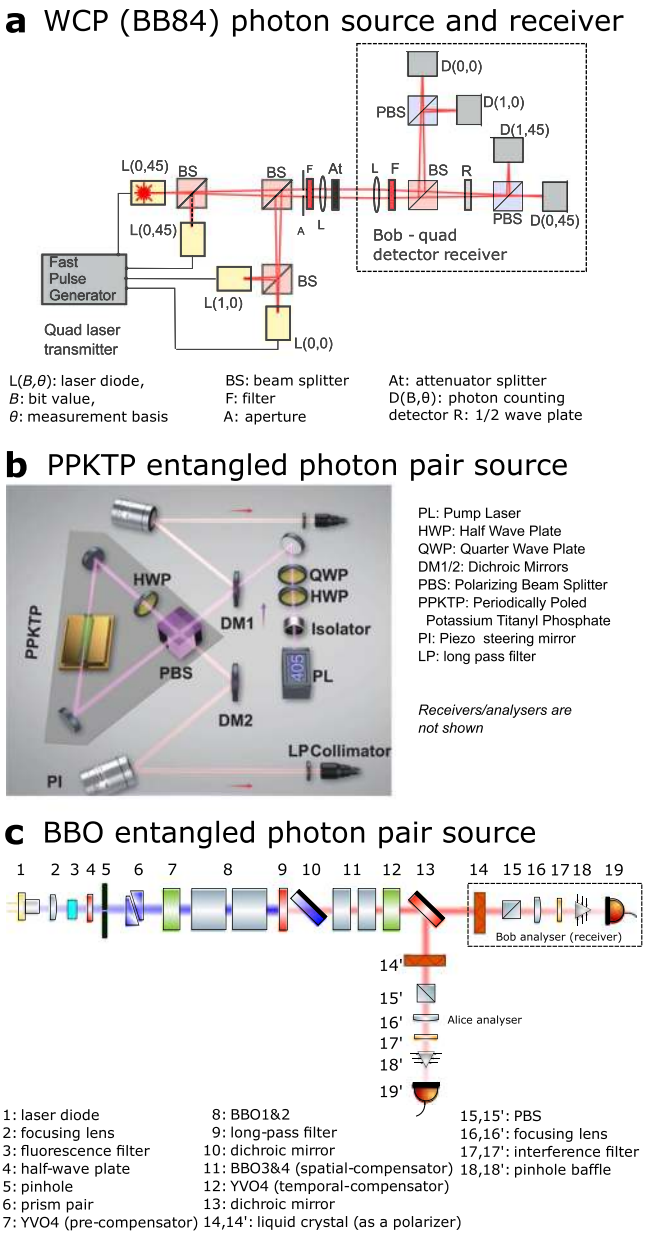

Fig. 3 Examples of optical layouts for sources used in polarization encoded DV-QKD designed for satellite QKD. **a** A weak coherent pulse source for BB84 QKD (adapted from ref. 120). **b** A polarization-entangled photon-pair source using PPKTP in a Sagnac loop arrangement (adapted from ref. 47) **c** A polarization-entangled photon-pair source based on BBO with Bell's violation analysers (adapted from ref. 67), for BBM92 QKD these analysers would most likely be replaced with quad detector receivers as per **a**

adjustable steering mirrors and an on-satellite BB84 receiver to allow it to be realigned in orbit.[47]

Although BBO has a smaller $\chi^{(2)}$ non-linearity compared to PPKTP, its optical properties are much more temperature tolerant. Furthermore, single-domain crystals are available in very large apertures (typically several millimetres), simplifying optical alignment, whereas periodically poled materials are restricted to a small aperture not exceeding 2 mm due to the difficulty in maintaining regular poling across the crystal. Altogether, this makes BBO and other similar single-domain crystals very attractive raw material for the design of sources of entangled photon pairs.[73–75]

Polarization-correlated, photon-pair sources based on BBO have been demonstrated in orbit on board the 2U Galassia nanosatellite.[19] The source design is also extremely robust, having survived a dramatic launch vehicle explosion.[76] The correlated source design is being extended and enhanced to generate polarization-entangled photon pairs[67, 71] for demonstration in future nanosatellite missions[77] (Fig. 3c).

The pump light from laser diodes for SPDC sources can easily reach 40 mW, when stabilized with external cavities[78] and even exceed 100 mW when operated in free-running mode. For QKD links using SPDC sources the limiting factor is therefore not the photon generation, but the ability of the single photon detectors to distinguish between the photons arriving with small timing separations, as will be discussed in Section Detectors.

Optical links

The optical links use telescope-like optics at the photon source transmitter and at the receiver to beam the photons between satellite and ground station in the same manner as classical laser communications links. The links are where the largest losses occur and thus have the biggest impact on the quantum bit error rate (QBER), which is the relevant signal-to-noise ratio in QKD and which will be discussed in more detail in Section Quantum Bit Error Rate. Simulated losses for example optical link scenarios are shown in Table 1 which is adapted from ref. 39 and does not include detector losses.

In the downlink configuration, optical loss is essentially dominated by diffraction, i.e., broadening of the beam, which increases as the square of the link length. In the uplink configuration, atmospheric turbulence, which is most significant in the 20 km immediately above the surface of the Earth, has a much larger effect, adding over 20 dB of loss for the example in Table 1. This extra loss in uplink may mitigate many of the perceived conveniences gained from locating the quantum light source on the ground. However, since this atmospheric turbulence is fluctuating, the use of signal-to-noise ratio filters to discard data when noise levels are highest, can lead to lower QBER and thus longer private keys.[79, 80] This is because if the full data set were used, the QBER value would be higher and many more of the photons would be required for error correction and privacy amplification. Similar schemes have also been discussed for CV-QKD.[81]

The following subsections discuss the origins of these optical losses and the fundamental engineering challenges to address when establishing optical links. These are principally: coping with the losses/depolarizing effects in the optical path, and ensuring the telescopes are pointing precisely at each other.

Optics considerations. Diffraction losses are dependent on the telescope design and beam spatial mode and increase as the inverse square of the wavelength (λ). Conversely, atmospheric absorption losses tend to decrease with increasing wavelength, though there are also large spectral bands in which the atmosphere is almost entirely opaque. Losses due to atmospheric turbulence also decrease slightly as wavelengths increase. Favourable spectral bands, where relevant laser systems also exist, can be seen in Fig. 4 and include 665–685 nm, 775–785 nm, 1000–1070 nm, and 1540–1680 nm.[48]

Of the methods discussed in section Concepts for Satellite QKD, a single downlink is the most practical, and in these cases entanglement-based QKD has been shown to be more tolerant to loss than prepare-and-measure schemes due to the intrinsic timing correlation between photon-pairs generated in the SPDC process.[82]

Table 1. Simulated link attenuation for 800 nm photons in various link scenarios[39]

	1 m ground receiver	30 cm LEO receiver	30 cm GEO receiver
1 m ground transmitter		27.4 dB (500 km)	64.5 dB (36,000 km)
30 cm LEO transmitter	6.4 dB (500 km)	28.5 dB (2000km)	52.9 dB (35,000 km)
30 cm GEO transmitter	43.6 dB (36,000 km)	52.9 dB (35,000 km)	53.9 dB (40,000 km)

A trade-off when designing the telescope optics is the choice of either transmissive or reflective telescopes. Reflective mirrors can be larger, although for polarization-based QKD care must be taken to prevent large depolarization effects. Secondary mirrors of reflector telescopes are often placed within the path of the beam so that it blocks part of the primary mirror and affects the diffraction spreading, although the loss is <1 dB for a secondary mirror diameter up to 25% the ratio of the primary mirror diameter (D).[48] Beam divergence scales with λ/D, so larger apertures produce smaller beam divergences with lower free-space losses, although because of atmospheric turbulence, increasing the diameter of ground-based transmitters above a few tens of centimetres makes little improvement on the losses. Indicative examples of ground-based transmitting telescopes in studies start from 25 cm in diameter, LEO-based transmitting telescopes from 9 cm and GEO-based from 13.5 cm.[48, 53, 81] The Micius quantum satellite uses transmitters of 18 and 30 cm.[47]

The success of the Micius satellite has confirmed the scientific consensus[83, 84] that the atmosphere does not degrade polarization states. Additional studies have also suggested this to be true for the time-bin degree of freedom.[55]

The Micius satellite collects its entangled photons into single mode fibres. These are sensitive to vibrations and after launch introduced random polarization rotations which needed to be compensated using motorized waveplates during in-orbit commissioning and every few weeks thereafter. The satellite's transmitter also has additional polarization correcting elements to compensate for the spacecraft attitude drift. Other polarization corrections are usually performed at the receiver and are discussed in the receiver Section Optical receivers below. Time-bin entanglement-based QKD would require additional Doppler corrections.[85]

Pointing, acquisition and tracking. Establishing the optical link is usually performed in several stages. Satellite orbit determination data such as radar tracking, GPS and star tracker measurements can be exchanged between satellite and ground via radio frequency links to provide a coarse level of mechanical pointing towards each other. Laser beacons on the ground and on the satellite can then be used as a target to enable a finer level of mechanical pointing. The finest level of pointing can then be achieved through optical beam-steering systems, which are essentially correcting for atmospheric turbulence.

Full deformable mirror adaptive optics systems could be implemented, but they are typically not designed to preserve polarization, and since the beam is small, higher order wavefront perturbations would not make a large impact.[53] For larger spacecraft, coarse level pointing is usually achieved by mounting the telescopes on two-axis gimbal or turntable stages, whereas for nanosatellites coarse control is usually achieved by reorienting the entire satellite. Such stages are used together with piezo fast steering mirrors on the Micius satellite to achieve a final pointing of around 0.6 µrad in space.[47] CubeSat Quantum Communications Mission (CQuCom) proposes a 3 µrad pointing capability,[53] which would push the boundaries of current CubeSat capabilities.

Relative to the incoming laser beacons, outgoing optical signals must be pointed at an angle to compensate for the time delay and chromatic dispersion. For typical ground-to-LEO QKD uplink proposals, atmospheric turbulence means the transmitter pointing accuracy has less of a consequence than for LEO-to-ground downlinks. A 2 µrad rms error in the pointing of a 20 cm downlink transmitter would introduce 4 dB of loss compared with <1 dB for a 20 cm uplink transmitter.[48] Jitter and imperfections in the tracking systems should be minimized so their contributions to beam broadening are much less than those caused by diffraction and atmospheric turbulence. The receiver system need only point to an accuracy within its field of view, e.g., 50 µrad.[48]

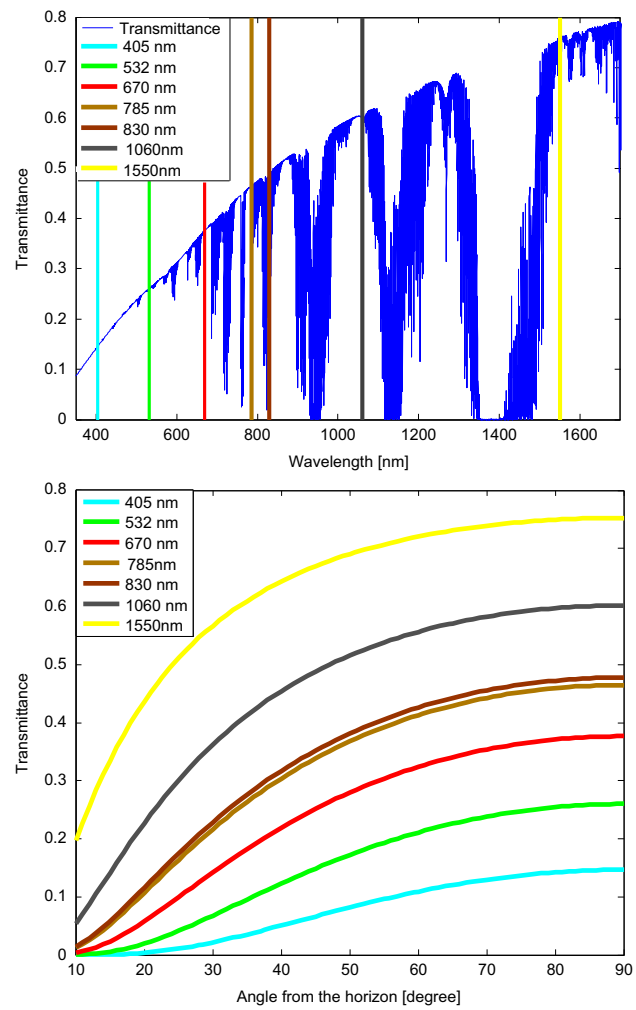

Fig. 4 Simulated transmittance of the atmosphere (adapted from ref. 48). *Top*–at zenith in a typical rural location with overlaid coloured lines showing the wavelengths of commercially available laser systems. *Bottom*–as a function of the pointing angle above the horizon for the various lasers

Optical receivers. Optically, the receiver telescope can be identical to the transmitter telescope, discussed in Section Optics

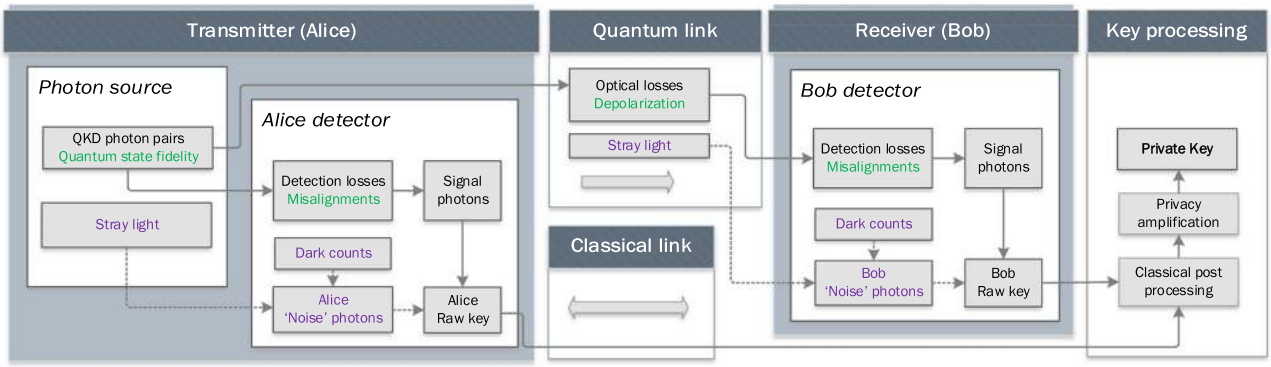

Fig. 5 Noise contributions to entanglement-based QKD between Alice (transmitter) and Bob (receiver) in a scenario such as Fig. 1 frame **a**. Effects determining the fidelity of the quantum states (visibility) are shown in green. Sources of unwanted photons are shown in purple with dotted connector lines. A WCP BB84 configuration would look similar, except Alice would have a random number generator selecting the polarization bases for her photon source and would not have a detector

considerations. For uplink configurations, the final key rate is strongly driven by the diameter of the space-based receiver telescope,[48] but flying large telescopes in space is complex and costly. For uplink QKD experiments to the International Space Station, a 14.3 cm camera lens mounted on an ESA NightPod tracking stage has been proposed as a QKD receiver.[86] The Canadian NanoQEY uplink nanosatellite proposal uses a similar-sized 15 cm receiver while their larger (microsatellite) uplink proposal, QEYSSAT, opts for a 40 cm one. The QEYSAT receiver would be similar to the quad detector receiver shown in Fig. 3a, so it can potentially be made capable of performing both BB84 and BBM92 protocols, to allow for a variety of QKD sources to be demonstrated with it.[43]

Ground-based receivers can be made larger more easily than their space-based counterparts and have a large impact on key rates for downlink configurations.[48] In retroreflector experiments, the 1.5 m Matera Laser Ranging Observatory (MLRO) was used to receive the qubits reflected from satellites from 1000 to 7000 km.[46, 55] MLRO was also baselined as the receiver for the CQuCom mission,[53] while the Micius satellite has so far been using ground-based receivers of 1, 1.2, and 1.8 m.[42, 47] For commercial usage though, smaller diameters are considered more attractive (e.g., 25–50 cm), in part because they can be made more mobile, except for GEO communications where receivers can have fixed pointing and thus are easier to make larger (e.g., 2 m).[81] While free space QKD demonstrations are sometimes performed at high altitude sites to reduce atmospheric turbulence, these locations are unlikely to be attractive for useful QKD networks. For commercial usage though, smaller diameters are considered more attractive (e.g., 25–50 cm), in part because they can be made more mobile, except for GEO communications where receivers can have fixed pointing and thus are easier to make larger (e.g., 2 m).[81] While free space QKD demonstrations are sometimes performed at high altitude sites to reduce atmospheric turbulence, these locations are unlikely to be attractive for useful QKD networks.

For polarization-based QKD schemes, the receiver telescope is typically coupled to an analyser like that in Fig. 3a or, in the case of the Micius entanglement distribution demonstration, a Pockels cell connected to a random number generator.[47] For the analysers to be effective, systems must be in place to allow dynamic polarization variations–most particularly the relative roll orientation of the satellite and ground station–to be understood and compensated, so that the reference frame of the polarization bases is preserved. This is a complex task for non-GEO orbits as the satellites are moving across the sky throughout the operation, but it can be achieved without the requirement for a feedback loop between space and ground.[87–90] In all tests, atmospheric depolarization has been found to be minimal.

Detection and key generation

The optical signal arriving at the receiving detectors is composed of both QKD photons and stray light. The detector output is also mixed with technical noise (e.g., 'dark-counts' from GM-APDs) and is considered as a raw key that must be processed to produce a private encryption key (see Fig. 5).

Detectors. In DV-QKD schemes, the individual photons are registered by photo multiplier tubes (PMTs) or increasingly by GM-APDs–also known as single-photon avalanche diodes (SPADs)–which are advantageous due to their smaller power requirement and physical footprint.

As has been mentioned in Section Photon sources, the detector time resolution capability is typically the system performance bottleneck rather than the source brightness. Silicon-based GM-APDs have a typical timing jitter of 0.5 ns; a reduced timing jitter can be achieved by sacrificing the avalanche volume of the photodiode, which means that the detection efficiency is also reduced.

Detectors also have a recovery time (dead time) between detections, for APDs this can be, e.g., 26 ns.[91] CMOS arrays of GM-APDs offer the potential to reduce this to several tens of picoseconds.[53]

Space-based GM-APDs must be appropriately shielded from radiation damage if several years of operation are required. The detection efficiency of GM-APDs is typically on the order of 50% for silicon-based devices, which can detect visible or near-infrared light. GM-APDs for IR telecom wavelengths also exist, although they are much noisier and have a lower detection efficiency–around 20%–due to the different materials needed to detect long-wavelength photons.

The GM-APDs have noise from dark-counts which have an exponential dependence on temperature as demonstrated in Fig. 6 (*left*), and which can be a significant contributor to QBER in the satellite environment. Figure 6 (*right*) shows that a simulated QKD link can tolerate an additional 0.5 dB of loss for every degree drop in temperature, making it highly attractive to provide cooling to the detectors.

In addition to PMTs and GM-APDs, ground-based receivers equipped with cryostats do have the option of operating state-of-the-art single-photon detectors which use superconducting technologies and can have detection efficiencies over 90%. These detectors can have extremely low technical noise, but must be appropriately shielded from thermal blackbody emission. While superconducting detectors need to be cooled to 4 K or less, for optimal performance GM-APDs need only to be cooled to about 250 K. Unless the ultra-low temperature requirements are

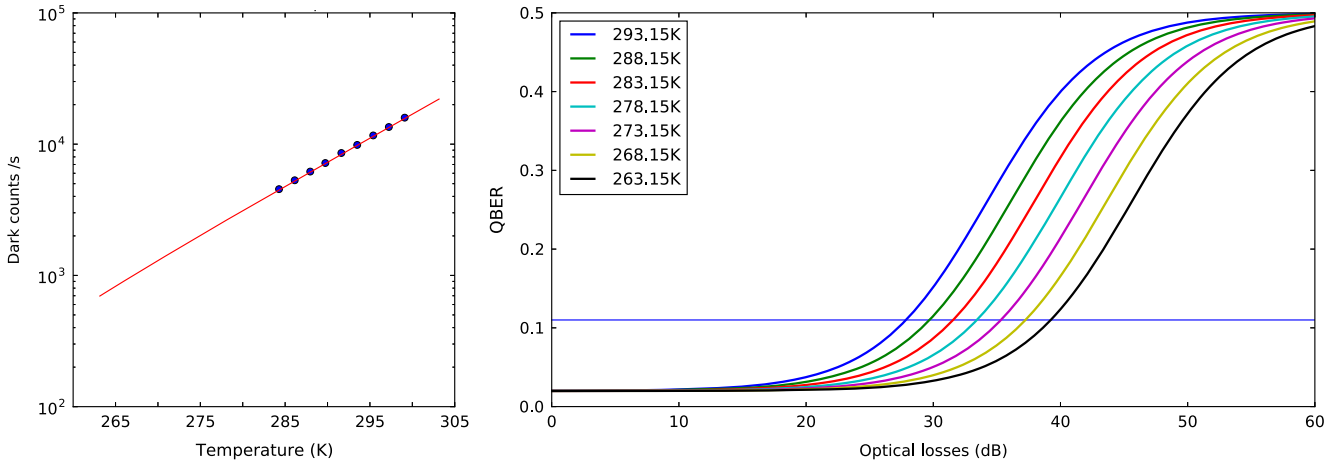

Fig. 6 Impact of noise and losses on an example BBM92 system. *Left*–dark counts measured in a typical SAP500 GM-APD as a function of temperature. *Blue dots* are measurements, *red line* is fitted exponential, $ae^{(x-273.15)b}+c$ where $a=1790$, $b=0.08$, $c=-81$. *Right*–QBER as a function of optical losses (e.g., diffraction, atmosphere, etc.) and technical noise in the SAP500 detector at different temperatures. Secure QKD is only possible when QBER is below 11% (*dotted line*)

overcome, superconducting detectors are unlikely to be an attractive option for use in space.[92]

Thermal management of any space-based device can be challenging. In-orbit temperatures can vary by tens of degrees, electrical power is limited, and, for the most part, heat can only be lost radiatively. One approach for the APDs may be to cool them by connecting them passively to radiators on the satellite, and while excursions in temperature may occur, stable operation can still be achieved by monitoring the pulse height of the detector output to actively control the GM-APD bias voltage.[93] Technical noise in the detectors steadily increases as ionizing space radiation damages the silicon with extended time in orbit.[61] Efforts are underway to investigate effective shielding techniques, as well as in-orbit annealing methods to attempt to reverse this effect.[94–96]

Quantum bit error rate. Quantum bit error rate (QBER) is the percentage of the sifted raw keys that is erroneous, i.e., that does not match between Alice and Bob. As the rate of the true signal falls, the accidental coincidences from stray light and other technical noise in the detection and measurement apparatus make a larger contribution to the raw keys and the QBER rises. Once QBER exceeds 11%, the QKD protocols based on BB84–which are the ones considered by the vast majority of satellite projects–will not be able to generate any private key.

For DV-QKD protocols, noise appears as accidental correlations between the detectors of Alice and Bob. Accidental correlations are well-approximated by the expression: $S_1 \times S_2 \times \tau$, where S_1 and S_2 are the rate of events at the individual detectors, and τ is the coincidence-time window. In systems where either detector can fire first, an additional factor of 2 is needed.[97] This expression only works when the detectors are in the linear regime. In scenarios where the detectors are saturated, e.g. by stray light, the recovery behaviour of the detectors must be taken into account.[98]

The effect of link loss on QBER for a model BBM92 system is shown in Fig. 6 (*right*) where the QBER is plotted against link loss for a range of GM-APD temperatures, with the corresponding dark counts shown in Fig. 6 (*left*). In this simulated system, the intrinsic QBER is assumed to be 1.5% at full transmission, the source produces photon pairs at 1 Mcps and the coincidence window is 2 ns.

Although it is not specifically included in the simulation in Fig. 6, another significant noise source is stray light: background photons being detected. In general, stray light can be minimized in optical systems with extensive baffling and optical blacking, however even after extensive filtering,[59, 99] DV-QKD is likely to be a night-time activity for the near future.[100, 101] A possible, but challenging, solution to this is to perform DV-QKD at other wavelengths with alternative detectors,[50] or–if suitable light sources can be found–at the wavelengths of the Fraunhofer lines, the narrow absorption lines in the output spectra of the Sun.[102] In this respect, CV-QKD has the advantage because the optical systems used have a sufficiently small spectral bandwidth that allows much of the background to be filtered, enabling daytime operations.[103]

Establishing keys. For QKD to be carried out, a number of communication tasks need to be performed between the key sharing parties, such as basis reconciliation, clock synchronization and time tagging of photons, the latter being the most significant in data bandwidth.

For QKD based on SPDC sources the intrinsic timing correlation of entangled photon pairs[104] is in the femtosecond regime,[105] and can be exploited to perform asynchronous pair detection over long-range.[106] Prepare-and-measure schemes require alternative approaches[107, 108]; the Micius satellite achieves this through 10 kHz pulses in its 532 nm, downward-pointing tracking beacon.[42] Laser ranging to passive retroreflectors on the satellite can also be used to provide centimetre level distance knowledge.[53]

For continuous key production in the simulated BBM92 system used for Fig. 6, with a detector temperature of 288.15 K, the classical communications link requires a baseline bit rate of a few Mbps which would increase to a few tens of Mbps as the QBER decreases allowing for a few 100 s kbps of private key to be established, as shown in Fig. 7. For the specific example of the losses in the LEO-to-ground configuration in Table 1 this would correspond to about 55 kbps of private key requiring about 7.5 Mbps classical bit rate for steady state operations. For space-based QKD this authenticated classical link could be established over radio links, or since an optical link is already established it could be implemented using classical laser communications. The Micius satellite opts for radio with 1 Mbps uplink and 4 Mbps downlink.[42]

However, for QKD there is no requirement that the classical communications happen at the same time as the quantum communications, i.e., for non-steady state key production, the classical communications could be stored and transmitted at a later time and the time stamps synchronized, bases matched and

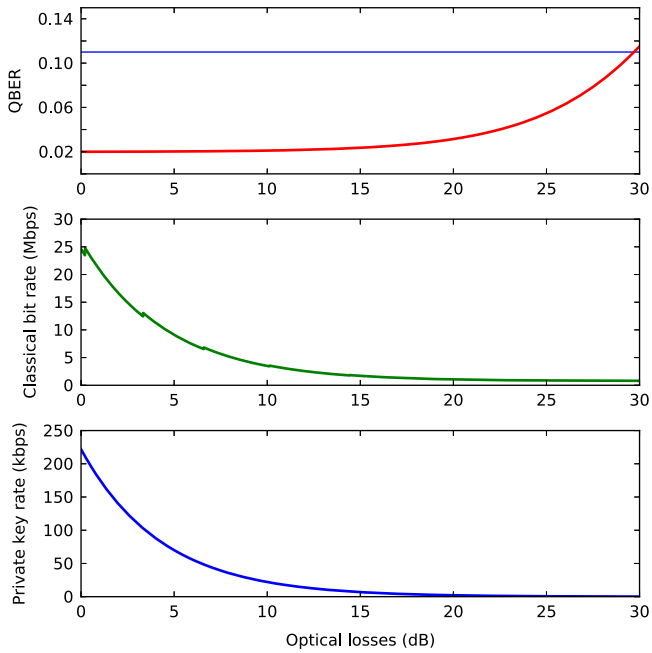

Fig. 7 Private key rate achievable as a function of optical losses, and the corresponding classical communication overhead that would be required for continuous steady state key production, for the simulated BBM92 link in the previous figure (288.15 K). The highest QBER with which QKD can be performed securely here is 0.11 (*horizontal blue line*)

keys generated in post processing. For example, after passing over an optical ground station and transmitting or receiving qubits, a LEO satellite could then perform the classical comms at a slower rate, e.g., via a GEO communications relay during the remainder of the orbit.

The proposed NanoQEY uplink QKD nanosatellite is projected to create 10 kbit of secure key per month with its 15 cm receiver, paired with a 50 cm telescope on the ground.[109] The microsatellite QEYSSAT uplink proposal however, suggests that a 40 cm receiver can achieve ~100 kbit of secure key per pass.[43] In contrast, the Micius downlink satellite, with a 30 cm transmitter in space and a 1 m receiver on ground, is achieving >300 kbit of secure key per pass. For future QKD service satellites it has been estimated that with a 13.5 cm transmitter at LEO, the monetary costs of QKD for 50 and 25 cm receivers could be €77 per Mbit and €312 per Mbit respectively while a service from GEO to a 2 m receiver would be 615 per Mbit.[81]

To operate as a trusted node within a QKD network additional elements such as key management, and control and accounting subsystems are required.[81] As with all practical implementations of QKD, special considerations must be paid to the side-channel attacks that might be possible with real-world systems.[110]

CONCLUSIONS

Satellite QKD has overcome the range limit of ground-based links and, is being used to enable global coverage.[42] The technical challenges to achieving a global network remain daunting, but progress is being made in overcoming them.

Table 2 shows a summary of notable satellite QKD initiatives that have been reported in recent years.

The top eleven rows show completed or ongoing experiments and missions. Besides photon sources and tracking systems,[19, 65, 67] much important work has been made to confirm that quantum states encoded with polarization[46, 89] and time-bin[55] experience negligible decoherence in space-ground optical links. These are showing that the standard QKD protocols, already proven in ground tests, also work from space, possibly even from geostationary orbits.[103] The most notable experiment thus far is QUESS (the Micius satellite) by the Chinese Academy of Sciences.[20]

Work in developing light sources for DV-QKD is ongoing at various groups. For protocols relying on weak coherent pulses, there are now very compact designs using laser diodes and waveguide-based polarization rotators.[65] Space capable polarization-entangled photon-pair sources to enable BBM92 or E91 protocols are also at various stages of development.[67, 72]

The performance of single photon detectors is an important consideration for DV-QKD. Currently, the limitation on QKD rates (in space or on the ground) is not given by the brightness of the photon sources, but by the detection efficiency and timing jitter of the single photon detectors. At the moment the only fast detectors with near-unit detection efficiency are based on superconducting technology and have requirements that make them costly to operate on satellites. This is motivating research into GM-APDs to understand how to operate them more efficiently, and to prolong their lifetime in a space environment.[93, 96]

Table 2 also lists the sizes of the satellites used. In recent years research on satellite QKD has become more attractive with the emergence of nanosatellite platforms, particularly the CubeSat. The standardized satellite buses provided by CubeSats allow for the rapid development of cost-effective space missions. In the first instance, these missions aim to be technological pathfinders aimed at raising the technology readiness level of sub-systems. As the technology matures, we can expect that full QKD missions with nanosatellites, such as the NanoQEY[109] and CQuComm[53] proposals, will be realized.

The placement of quantum optics technologies on satellites also enables various fundamental physics experiments,[21] such as placing experimental bounds on the effect of gravity on quantum systems as they traverse a changing gravitational potential.[111, 112]

A technology related to QKD is the quantum random number generator[113] used in the production of random bits that are not pre-existing. This technology already has applications in a number of cryptographic scenarios, relevant in both ground and space environments. The distribution of entanglement as part of a quantum internet[114, 115] is another possibility—the capability to perform this is an important building block in a global network of distributed quantum computers.

A quantum internet would not be a purely optical technology like QKD, but will require an interface to material systems that can act as quantum memory or processing units. Furthermore, in contrast to QKD, Doppler effects cannot be neglected in any attempted satellite information transfer because candidates for quantum storage can only interact with light fields with very narrow linewidths (in the kHz or MHz regime).

Another potential area for growth is the placement of quantum sensors on satellites to aid in gravimetry or mineral exploration. First steps in operating quantum matter systems in space are being carried out by fundamental physics experiments on the International Space Station,[116, 117] on sounding rockets,[118] as well as with nanosatellites.[119]

In summary, quantum satellite communications is paving the way for the deployment of other quantum technologies in space. The current pace of development suggests that world-wide communications privacy can be maintained in the era of powerful quantum computers, and at the same time it is bringing the concept of a global quantum internet closer to fruition.

Data availability

The code for the QBER simulation can be found here: https://github.com/CQT-Alex/s2qkd-sim.

Table 2. A summary of satellite QKD enabling initiatives

Initiative	Goal	Vehicle	Status/Results
QUESS[20]	LEO-to-ground trusted-node satellite QKD, uplink quantum teleportation and double-downlink entanglement distribution.	Micius 631 kg satellite.	Entanglement distribution of 1203 km[47], teleportation up to 1400 km[43] and BB84 QKD up to 1200 km with QBER ~1% and sifted key 14 kbps.[42]
Toyoshima et al.[121]	LEO-to-ground polarization measurement.	OICETS 570 kg satellite.	Polarization preserved within system rms error of 28 mrad.
Takenaka et al.[90, 122]	LEO-to ground polarization measurements from a small optical transponder (SOTA).	SOCRATES 48 kg satellite.	Effectively no depolarization was observed (100% Degree-of-polarization) and QBER of < 5%.
Günthner et al.[103]	GEO-to-ground test of quantum state used in coherent communication.	Alphasat I-XL 6649 kg satellite.	Quantum-limited states arrive on the ground after transmission from satellite.
Vallone et al.[46]	Test of polarization state for weak coherent pulses using retro-reflectors on LEO satellites.	Jason-2 510 kg, Larets 21 kg and Starlette/Stella 48 kg satellites.	Average QBER of 6.5% achieved.
Yin et al.[122]	Test of polarization state for weak coherent pulses using retro-reflectors in a LEO satellite.	CHAMP 500 kg satellite.	Signal to noise ratio of 16:1 observed for polarization measurements.
Dequal et al.[124]	Test of weak coherent pulse transmission from retro-reflectors on a MEO satellite.	LAGEOS-2 411 kg satellite.	Peak signal-to-noise ratio of 1.5 with 3 counts per second.
Tang et al.[19]	In-orbit observation of polarization correlations from a photon-pair source on a nano-satellite.	Galassia 2 kg 2U CubeSat.	97% contrast in polarization correlation measurements. Pathfinder for SpooQySats (below).
Nauerth et al.[125]	QKD between the ground and a aircraft moving at similar angular velocities to a LEO satellite.	Dornier 228 utility aircraft.	Sifted key rate of 145 bps, QBER of 4.8% from range of 20 km at angular speed of 4mrad per second.
Bourgoin et al.[18]	QKD with a moving receiver similar to the angular speed of satellite at 600 km altitude.	Pick-up truck.	Key rate of 40 bps with QBER of 6.5 to 8% with receiver at a range of 650 m moving at angular speed of 13 mrad per second.
Wang et al.[126]	Verification of pointing, acquisition and tracking.	Hot-air balloon.	Key rate of 48 bps and QBER of ~4% over a range of 96 km.
SpooQySats[127]	Demonstrate polarization-entangled photon-pair sources in space.	3U CubeSats.	Funded mission. Launches planned from 2018.
QEYSSat[43]	Trusted-node receiver for uplink QKD.	Microsatellite.	Funded mission.
CAPSat[94]	Laser annealing of radiation-damaged APDs.	3U CubeSat.	Funded mission.
NanoBob[128]	Trusted-node receiver for uplink QKD.	CubeSat.	Proposal.
SpaceQUEST (2008)[41]	Double LEO-to-ground downlinks QKD using polarization-entangled photon-pairs.	International Space Station.	Proposal (since updated as a mission exclusively investigating decoherence due to gravity[111]).
Scheidl et al.[86]	Entanglement-based QKD and Bell tests, ground-to-LEO.	International Space Station.	Proposal.
NanoQEY[109]	QKD and Bell tests ground-to-LEO with a trusted-node satellite.	Based on NEMO nanosatellite bus, 16 kg.	Proposal.
Zeitler et al.[85]	Superdense teleportation, LEO-to-ground.	International Space Station.	Proposal.
QuCHAP-IDQuantique	Establish QKD networks based on high altitude platforms.	High-altitude platform.	Proposal.
CQuCom[53]	LEO-to-ground QKD downlinks.	6U CubeSat.	Proposal.

ACKNOWLEDGEMENTS

We thank Tanvirul Islam and Christian Kurtsiefer for feedback and Tanvirul Islam for the QBER simulation and plots. 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).

AUTHOR CONTRIBUTIONS

All authors contributed to the paper equally. R.B. led Section Technical Realization, J.M.A. led the preceding introductory sections, A.L. led Section Conclusions. All authors then reviewed and contributed to each others sections substantially.

ADDITIONAL INFORMATION

Competing Interests: The authors declare that they have no competing financial interests.

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

REFERENCES

1. Bennett, C. H. Quantum cryptography: public key distribution and coin tossing. *Int. Conf. Comput. Syst. Signal Process. IEEE* **1984**, 175–179 (1984).
2. Dixon, A. et al. High speed prototype quantum key distribution system and long term field trial. *Opt. Express* **23**, 7583–7592 (2015).
3. Choi, I. et al. Field trial of a quantum secured 10 gb/s dwdm transmission system over a single installed fiber. *Opt. Express* **22**, 23121–23128 (2014).
4. Fröhlich, B. et al. Quantum secured gigabit optical access networks. *Sci. Rep.* **5**, 18121 (2015).
5. Pirandola, S., García-Patrón, R., Braunstein, S. L. & Lloyd, S. Direct and Reverse Secret-Key Capacities of a Quantum Channel. *Phys. Rev. Lett.* **102** (2009).
6. Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **5**, 5235 (2014).
7. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
8. Corning Incorporated. Corning SMF-28 ultra optical fibre datasheet URL https://www.corning.com/media/worldwide/coc/documents/Fiber/SMF-28 (2014).
9. Tamura, Y. et al. Lowest-ever 0.1419-db/km loss optical fiber. *Optical Fiber Communication Conference Postdeadline Papers*, Th5D.1 (Optical Society of America, 2017).
10. Yin, H.-L. et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* **117**, 190501 (2016).
11. Sangouard, N., Simon, C., De Riedmatten, H. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **83**, 33 (2011).
12. Duan, L.-M., Lukin, M., Cirac, J. I. & Zoller, P. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414**, 413–418 (2001).
13. Fowler, A. G. et al. Surface code quantum communication. *Phys. Rev. Lett.* **104**, 180503 (2010).
14. Jiang, L. et al. Quantum repeater with encoding. *Phys. Rev. A.* **79**, 032325 (2009).
15. Muralidharan, S., Kim, J., Lütkenhaus, N., Lukin, M. D. & Jiang, L. Ultrafast and fault-tolerant quantum communication across long distances. *Phys. Rev. Lett.* **112**, 250501 (2014).
16. Munro, W. J., Stephens, A. M., Devitt, S. J., Harrison, K. A. & Nemoto, K. Quantum communication without the necessity of quantum memories. *Nat. Photonics* **6**, 777–781 (2012).
17. Schmitt-Manderbach, T. et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.* **98**, 010504 (2007).
18. Bourgoin, J.-P. et al. Free-space quantum key distribution to a moving receiver. *Opt. Express* **23**, 33437–33447 (2015).
19. Tang, Z. et al. Generation and analysis of correlated pairs of photons aboard a nanosatellite. *Phys. Rev. Appl.* **5**, 054022 (2016).
20. Pan, J.-w Quantum science satellite. *Chin. J. Sp. Sci.* **34**, 547–549 (2014).
21. Rideout, D. et al. Fundamental quantum optics experiments conceivable with satellites—reaching relativistic distances and velocities. *Class. Quantum Gravity* **29**, 224011 (2012).
22. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).
23. Diamanti, E., Lo, H.-k, Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. *Quantum Inf.* **2**, 16025 (2016).
24. Grosshans, F. et al. Quantum key distribution using gaussian-modulated coherent states. *Nature* **421**, 238–241 (2003).
25. Diamanti, E. & Leverrier, A. Distributing secret keys with quantum continuous variables: principle, security and implementations. *Entropy* **17**, 6072–6092 (2015).
26. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **7**, 378–381 (2013).
27. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121 (1992).
28. Scarani, V., Acin, A., Ribordy, G. & Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **92**, 057901 (2004).
29. Marcikic, I., Lamas-Linares, A. & Kurtsiefer, C. Free-space quantum key distribution with entangled photons. *Appl. Phys. Lett.* **89**, 8–10 (2006).
30. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
31. Hwang, W.-Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **91**, 57901 (2003).
32. Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.* **68**, 557 (1992).
33. Ekert, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* **67**, 661 (1991).
34. Acín, A. et al. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
35. Ling, A. et al. Experimental quantum key distribution based on a Bell test. *Phys. Rev. A.* **78**, 020301 (2008).
36. IEEE Spectrum. China's 2,000-km quantum link is almost complete URL http://spectrum.ieee.org/telecom/security/chinas-2000km-quantum-link-is-almost-complete (2016).
37. Gerhardt, I. et al. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* **2**, 349 (2011).
38. Nordholt, J. E., Hughes, R. J., Morgan, G. L., Peterson, C. G. & Wipf, C. C. Present and future free-space quantum key distribution. in *High-Power Lasers and Applications*, 116–126 (International Society for Optics and Photonics, 2002).
39. Aspelmeyer, M., Jennewein, T., Pfennigbauer, M., Leeb, W. R. & Zeilinger, A. Long-distance quantum communication with entangled photons using satellites. *IEEE J. Sel. Top. Quantum Electron.* **9**, 1541–1551 (2003).
40. Rarity, J. G., Gorman, P. M., Knight, P., Weinfurter, H. & Kurtsiefer, C. Quantum communications in space. *Optical Science and Technology, SPIE's 48th Annual Meeting*, 240–251 (International Society for Optics and Photonics, 2004).
41. Perdigues Armengol, J. M. et al. Quantum communications at ESA: Towards a space experiment on the ISS. *Acta Astronaut.* **63**, 165–178 (2008).
42. Sheng-Kai, L. et al. Satellite-to-ground quantum key distribution *ArXiV preprint* 1707.00542v1 (2017).
43. Jennewein, T. et al. QEYSSAT: A mission proposal for a quantum receiver in space. *Proc. SPIE* **8997**, 89970A (2014).
44. Liao, S.-K. et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nat. Photon.* **11**, 509–513 (2017).
45. Makarov, V. et al. Creation of backdoors in quantum communications via laser damage. *Phys. Rev. A* **94**, 030302 (2016).
46. Vallone, G. et al. Experimental satellite quantum communications. *Phys. Rev. Lett.* **115**, 1–5 (2015).
47. Yin, J. et al. Satellite-based entanglement distribution over 1200 kilometers. *Science* **356**, 1140–1144 (2017).
48. Bourgoin, J.-P. et al. A comprehensive design and performance analysis of low Earth orbit satellite quantum communication. *New. J. Phys.* **15**, 023006 (2013).
49. Boone, K. et al. Entanglement over global distances via quantum repeaters with satellite links. *Phys. Rev. A* **91**, 052325 (2015).
50. Sheng-Kai, L. et al. Ground test of satellite constellation based quantum communication *ArXiV preprint* 1611.09982v1 (2016).
51. Pfennigbauer, M., Leeb, W. & Aspelmeyer, M. Free-space optical quantum key distribution using intersatellite links. in *Proceedings of the CNES-intersatellite link workshop* 1–9 (2003).
52. Wertz, J. & Larson, W. *Space Mission Analysis and Design*. Space technology library (Kluwer Academic, 1991).
53. Oi, D. K. et al. CubeSat quantum communications mission. *EPJ Quantum Technol.* **4**, 6 (2017).
54. Kidder, S. Q. & Vonder Haar, T. H. On the use of satellites in molniya orbits for meteorological observation of middle and high latitudes. *J. Atmos. Ocean. Technol.* **7**, 517–522 (1990).
55. Vallone, G. et al. Interference at the single photon level along satellite-ground channels. *Phys. Rev. Lett.* **116**, 253601 (2016).
56. Mafu, M. et al. Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Phys. Rev. A.* **88**, 032305 (2013).

57. Buttler, W. T. et al. Practical free-space quantum key distribution over 1 km. *Phys. Rev. Lett.* **81**, 3283–3286 (1998).
58. Buttler, W. T. et al. Daylight quantum key distribution over 1.6 km. *Phys. Rev. Lett.* **84**, 5652–5655 (2000).
59. Hughes, R. J., Nordholt, J. E., Derkacs, D. & Peterson, C. G. Practical free-space quantum key distribution over 10 km in daylight and at night. *New. J. Phys.* **4**, 43 (2002).
60. Kurtsiefer, C. et al. Quantum cryptography: A step towards global key distribution. *Nature* **419**, 450–450 (2002).
61. TanY. C., ChandrasekaraR., ChengC. & LingA. Radiation tolerance of optoelectronic components proposed for space-based quantum key distribution. *J. Mod. Opt.* **62**, 1–4 (2015).
62. Weier, H., Schmitt-Manderbach, T., Regner, N., Kurtsiefer, C. & Weinfurter, H. Free space quantum key distribution: towards a real life application. *Fortschr. Phys.* **54**, 840–845 (2006).
63. Jofre, M. et al. Fast optical source for quantum key distribution based on semiconductor optical amplifiers. *Opt. Express* **19**, 3825 (2011).
64. Nauerth, S., Fürst, M., Schmitt-Manderbach, T., Weier, H. & Weinfurter, H. Information leakage via side channels in freespace BB84 quantum cryptography. *New J. Phys.* **11**, 065001 (2009).
65. Vest, G. et al. Design and evaluation of a handheld quantum key distribution sender module. *IEEE J. Sel. Top. Quantum Electron.* **21**, 131–137 (2015).
66. Gisin, N., Fasel, S., Kraus, B., Zbinden, H. & Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A.* **73**, 022320 (2006).
67. Durak, K. et al. The next iteration of the small photon entangling quantum system (SPEQS-2.0). *Adv. Photonics Quantum Comput. Mem. Commun. IX*, 976209 (SPIE, 2016).
68. Steinlechner, F. O. et al. Ultra-bright source of polarization-entangled photons in a linear double-pass configuration. *Conf. Lasers Electro-Opt. Eur. Int. Quantum Electron. Conf.* **21**, 11943–11951 (2013).
69. Steinlechner, F. et al. Efficient heralding of polarization-entangled photons from type-0 and type-II spontaneous parametric downconversion in periodically poled KTiOPO4. *J. Opt. Soc. Am. B* **31**, 2068–2076 (2014).
70. Steinlechner, F. et al. A high-brightness source of polarization-entangled photons optimized for applications in free space. *Opt. Express* **20**, 9640 (2012).
71. Bedington, R. et al. Small photon entangling quantum systems (speqs) enabling space-based quantum key distribution. in *Proc. Int. Astronaut. Congr.* (Jerusalem, 2015).
72. Steinlechner, F. O. et al. Development of a space-proof polarization-entangled photon source. *Conf. Lasers Electro-Optics*, vol. 13, FTu1C.8 (OSA, 2016).
73. Kwiat, P. G. et al. New high-intensity source of polarization-entangled photon pairs (1995).
74. Kwiat, P. G., Waks, E., White, A. G., Appelbaum, I. & Eberhard, P. H. Ultrabright source of polarization entangled photons. *Phys. Rev. A* **60**, 773–776 (1999).
75. Trojek, P. & Weinfurter, H. Collinear source of polarization-entangled photon pairs at nondegenerate wavelengths. *Appl. Phys. Lett.* **92**, 211103 (2008).
76. Tang, Z. et al. The photon pair source that survived a rocket explosion. *Sci. Rep.* **6**, 25603 (2016).
77. Bedington, R. et al. Deploying quantum light sources on nanosatellites II: Lessons and perspectives on CubeSat spacecraft. *Proc. SPIE* 964811 (2015).
78. ONDAX. ONDAX Surelock wavelength stabilized laser datasheet URL http://www.ondax.com/Downloads/SureLock/405nm_12_25_40mW.pdf (2011).
79. Capraro, I. et al. Impact of turbulence in long range quantum and classical communications. *Phys. Rev. Lett.* **109**, 1–5 (2012).
80. Usenko, V. C. et al. Entanglement of Gaussian states and the applicability to quantum key distribution over fading channels. *New. J. Phys.* **14**, 093048 (2012).
81. Elser, D. et al. Network architectures for space-optical quantum cryptography service. in *Proceedings International Conference on Space Optical Systems and Applications (ICSOS) 2012, Post-1, Ajaccio, Corsica, France, October 9–12,* **12** (2012).
82. Scheidl, T. et al. Feasibility of 300 km quantum key distribution with entangled states. *New. J. Phys.* **11**, 085002 (2009).
83. Toyoshima, M. & Takayama, Y. Free-space laser communications: the Japanese experience. in *35th European Conference on Optical Communication* 1–4 (2009).
84. Vallone, G. et al. Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels. *Phys. Rev. A–At., Mol., Opt. Phys.* **91**, 1–6 (2015).
85. Zeitler, C., Graham, T. M., Chapman, J., Bernstein, H. & Kwiat, P. G. Super-dense teleportation for space applications. *Proc. SPIE* **9739**, 973912 (2016).
86. Scheidl, T., Wille, E. & Ursin, R. Quantum optics experiments using the International Space Station: a proposal. *New. J. Phys.* **15**, 043008 (2013).
87. Bonato, C. et al. Influence of satellite motion on polarization qubits in a Space-Earth quantum communication link. *Opt. Express* **14**, 10050 (2006).
88. Toyoshima, M. et al. Polarization-basis tracking scheme in satellite quantum key distribution. *Int. J. Opt.* **2011**, 8 (2011).
89. Wang, C. et al. Experimental validation of dynamic polarization compensation in ground-satellite quantum key distribution. *Sci. China Phys. Mech. Astron* **57**, 1233–1237 (2014).
90. Carrasco-Casado, A. et al. LEO-to-ground polarization measurements aiming for space QKD using Small Optical TrAnsponder (SOTA). *Opt. Express* **24**, 12254 (2016).
91. Stipcevic, M., Wang, D. & Ursin, R. Characterization of a commercially available large area, high detection efficiency single-photon avalanche diode. *J. Light. Technol.* **31**, 3591–3596 (2013).
92. Miki, S., Yamashita, T., Fujiwara, M., Sasaki, M. & Wang, Z. Multichannel SNSPD system with high detection efficiency at telecommunication wavelength. *Opt. Lett.* **35**, 2133 (2010).
93. Tan, Y. C., Chandrasekara, R., Cheng, C. & Ling, A. Silicon avalanche photodiode operation and lifetime analysis for small satellites. *Opt. Express* **21**, 16946–16954 (2013).
94. University of Illinois at Urbana-Champaign. Illinois wins nasa awards for three cubesat missions. https://aerospace.illinois.edu/news/illinois-wins-nasa-awards-three-cubesat-missions (2016).
95. Anisimova, E. et al. Mitigating radiation damage of single photon detectors for space applications. *EPJ Quantum Technol.* **4**, 10 (2017).
96. Lim, J. G. et al. Laser annealing heals radiation damage in avalanche photodiodes. *EPJ Quantum Technol.* **4**, 11 (2017).
97. Janossy, L. Rate of n-fold accidental coincidences. *Nature* **153**, 165–165 (1944).
98. Grieve, J. A., Chandrasekara, R., Tang, Z., Cheng, C. & Ling, A. Correcting for accidental correlations in saturated avalanche photodiodes. *Opt. Express* **24**, 3592 (2016).
99. PelosoM. P., GerhardtI., HoC., Lamas-LinaresA. & KurtsieferC. Daylight operation of a free space, entanglement-based quantum key distribution system. *New J. Phys.* **11**, 13 (2009).
100. Er-Long, M. et al. Background noise of satellite-to-ground quantum key distribution. *New. J. Phys.* **7**, 215 (2005).
101. Tomaello, A., Bonato, C., Da Deppo, V., Naletto, G. & Villoresi, P. Link budget and background noise for satellite quantum key distribution. *Adv. Space Res.* **47**, 802–810 (2011).
102. Benton, D. M., Gorman, P. M., Tapster, P. R. & Taylor, D. M. A compact free space quantum key distribution system capable of daylight operation. *Opt. Commun.* **283**, 2465–2471 (2010).
103. Günthner, K. et al. Quantum-limited measurements of optical signals from a geostationary satellite. *Optica* **4**, 611 (2017).
104. Burnham, D. C. & Weinberg, D. L. Observation of simultaneity in parametric production of optical photon pairs. *Phys. Rev. Lett.* **25**, 84 (1970).
105. Hong, C. K., Ou, Z. Y. & Mandel, L. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 2044–2046 (1987).
106. Ho, C., Lamas-LinaresA. & KurtsieferC. Clock synchronization by remote detection of correlated photon pairs. *New J. Phys.* **11**, 13 (2009).
107. Bienfang, J. et al. Quantum key distribution with 1.25 Gbps clock synchronization. *Opt. Express* **12**, 2011–2016 (2004).
108. Bourgoin, J. P. et al. Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations. *Phys. Rev. A–At., Mol. Opt. Phys.* **92**, 1–12 (2015).
109. Jennewein, T. et al. The NanoQEY mission: Ground to space quantum key and entanglement distribution using a nanosatellite. *Proc. SPIE* **9254**, 925402 (2014).
110. Scarani, V. & Kurtsiefer, C. The black paper of quantum cryptography: real implementation problems. *Theor. Comput. Sci.* **560**, 27–32 (2014).
111. Joshi, S. K. et al. Space QUEST mission proposal: experimentally testing decoherence due to gravity *ArXiV preprint* 1703.08036.v1 (2017).
112. Ralph, T. C. & Pienaar, J. Entanglement decoherence in a gravitational well according to the event formalism. *New. J. Phys.* **16**, 085008 (2014).
113. Ma, X., Yuan, X., Cao, Z., Qi, B. & Zhang, Z. Quantum random number generation. *Quantum Inf.* **2**, 16021 (2016).
114. Kimble, H. J. The quantum internet. *Nature* **453**, 1023–1030 (2008).
115. Pirandola, S. & Braunstein, S. L. Physics: unite to build a quantum Internet. *Nature* **532**, 169–171 (2016).
116. Soriano, M. et al. Cold atom laboratory mission system design. *IEEE Aerosp. Conf. Proc.* (2014).
117. Williams, J., Chiow, S.-w, Yu, N. & Müller, H. Quantum test of the equivalence principle and space-time aboard the International Space Station. *New. J. Phys.* **18**, 025018 (2016).
118. Schkolnik, V. et al. A compact and robust diode laser system for atom interferometry on a sounding rocket. *Appl. Phys. B* **122**, 217 (2016).
119. Oi, D. K. L. et al. Nanosatellites for quantum science and technology. *Contemp. Phys.* **7514**, 1–28 (2016).

120. Rarity, J., Tapster, P., Gorman, P. & Knight, P. Ground to satellite secure key exchange using quantum cryptography. *New. J. Phys.* **4**, 82 (2002).
121. Toyoshima, M. et al. Polarization measurements through space-to-ground atmospheric propagation paths by using a highly polarized laser source in space. *Opt. Express* **17**, 22333–22340 (2009).
122. Takenaka, H., Carrasco-Casado, A., Fujiwara, M., Kitamura, M., Sasaki, M. & Toyoshima, M. Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite. *Nat. Photon.* (2017).
123. Yin, J. et al. Experimental quasi-single-photon transmission from satellite to earth. *Opt. Express* **21**, 20032 (2013).
124. Dequal, D. et al. Experimental single-photon exchange along a space link of 7000 km. *Phys. Rev. A* **93**, 010301 (2016).
125. Nauerth, S. et al. Air-to-ground quantum communication. *Nat. Photonics* **7**, 382–386 (2013).
126. Wang, J.-Y. et al. Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nat. Photonics* **7**, 387–393 (2013).
127. Bedington, R. et al. Nanosatellite experiments to enable future space-based QKD missions. *Quantum Technol.* **3**, 12 (2016).
128. Centre Spatial Universitaire de Grenoble. Projet nanobob URL https://www.csug.fr/menu-principal/projets/projet-nanobob/ (2016).

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/.

© The Author(s) 2017