Deployment Strategies for the Global Coverage of Quantum Key Distribution Network

» **Jing Wang**
CableLabs

Bernardo A. Huberman
CableLabs

Abstract

We present a comprehensive literature review and comparative study on the deployment strategies of quantum key distribution (QKD) networks for global coverage. The state-of-the-art deployment strategies, including terrestrial QKD via optical fibers, free-space QKD via ground-based fixed links and ground-to-air dynamic links, as well as satellite QKD, are reviewed and compared in terms of channel loss, interference, distance limit, connection topology, and deployment cost. Selection criteria and deployment strategies are developed to enable a global coverage of QKD networks from intercontinental, long-haul to metro, and access networks.

KEYWORDS: QUANTUM KEY DISTRIBUTION NETWORKS, QKD, DEPLOYMENT STRATEGY.

Introduction

On the other hand, symmetric cryptographic algorithms, such as AES and SNOW 3G, are considered to be resistant against quantum computers. Although Grover's algorithm does speed up the attacks against symmetric ciphers, increasing the key length can effectively block these attacks [1, 5]. In modern communication, symmetric cryptography is only used for encryption and decryption. All other functions, such as signature, authentication, and key exchange, are carried out by asymmetric cryptography. Once sufficiently powerful quantum computers exist, classical cryptography will no longer be safe.

To address the challenges of quantum computing, two technological strategies were developed, post-quantum cryptography (PQC) and quantum key distribution (QKD). PQC, also known as quantum-safe or quantum-proof cryptography, focuses on increasing the computational complexity by inventing new intractable problems [5]. Thanks to its software implementation and full compatibility with existing systems, PQC is considered a good candidate for post-quantum eras, and three rounds of submissions have been organized by the National Institute of Standards

Recibido: enero 2022 Aceptado: Mayo 2022 Publicado: Junio 2022

and Technology (NIST) [6-8]. It is worth noting that, like their classical counterparts, PQC algorithms also rely on the assumptions of the computational power of attackers, i.e. they are only safe against quantum computers with a certain number of qubits, but may lead to long-term issues due to the ever-growing computational power of quantum computers.

QKD, also known as quantum cryptography, relies on quantum mechanics instead of mathematical assumptions to guarantee the security of keys [9-12]. Instead of computational security, it offers information-theoretic security, i.e., the keys are deemed secure even if the adversary has unlimited computing power. From the original idea of QKD [13] to the first demonstration [14], various protocols [10] and network topologies [11, 12] have been reported. It was found later, however, that the absolute security of QKD is only guaranteed for ideal single-photon sources and detectors [15]. The lack of perfect single-photon sources and low detection efficiency create security loopholes, which may be exploited by side-channel attacks.

In a real system, expensive single-photon sources are replaced by weak coherent pulses (WCP), whose photon number follows the Poisson distribution, so there are always pulses containing multiple photons. These multi-photon pulses could become the target of photon-number-split (PNS) attacks. For example, Alice sends qubits to Bob via single-photon pulses. She does not have an ideal single-photon source and uses weak coherent pulses. The eavesdropper, Eve, can develop a strategy to block all single-photon pulses from Alice and divide all multi-photon pulses, keeping half for herself and sending the rest to Bob. In this way, Eve always gets the same information as Bob. To eliminate this loophole, decoy-state protocols were invented to vary the photon number per pulse [16] so that the blocking strategy of the eavesdropper will be revealed.

On the detector side, measurement-device-independent (MDI) protocols were proposed to close all detection loopholes and are immune to side-channel attacks on imperfect detectors [17, 18]. In conventional prepare-and-measure protocols, Alice prepares qubits and sends them to Bob, and Bob makes measurements on the received qubits. In MDI protocol, both Alice and Bob prepare random qubits independently, and send them to a third party, Charlie, for Bell-state measurement (BSM). Charlie announces successful BSM results, but he has no access to the qubits sent by Alice and Bob. So Charlie serves as an untrusted relay and can even be controlled by an eavesdropper. The post-selection of successful BSM events entangles the qubits from Alice and Bob, that is why MDI-QKD is equivalent to a time-reversed entangled-photon-pair (EPR) protocol. Therefore, MDI-QKD with the decoy-state method can negate the threats of both imperfect single-photon sources and detection losses.

Deployment Strategies of QKD Networks

QKD technologies have grown out of the laboratory and become ready to reach the market [19, 20]. Various demonstrations and field trials have been reported in recent years, including terrestrial QKD via optical fibers, free-space QKD on the ground, and free-space QKD to and from aircraft and satellites. Optical fiber-based terrestrial QKD networks include the DARPA quantum network in Boston [21, 22], the SwissQuantum network in Geneva [23, 24], the SECOQC network in Vienna [25-28], metropolitan QKD networks in Tokyo [29], and Cambridge [30], and Beijing-Shanghai QKD backbone network in China [31]. It should be pointed out that fiber-based terrestrial QKD is limited by short transmission distances, usually less than 600 km in the lab

and ~100 km in the field. This is because the key rate scales linearly with channel transmittance, which in optical fibers decays exponentially with distance due to photon absorption.

There are several strategies to extend the QKD distance, including quantum repeaters, trusted relays, and untrusted relays. Despite recent advances, a quantum repeater remains infeasible because it requires high-quality quantum memory and complicated local entanglement distillation. Trusted relays can infinitely extend the QKD distance but with the penalty of key leakage since the key information ceases to be quantum at each intermediate node. Untrusted relays, on the other hand, eliminate the possibility of key exposure and seem to be a promising candidate to extend QKD distance. Extensive research effort has been spent on MDI-QKD [32-38] and twin-filed QKD (TF-QKD) [39-46], where Alice and Bob independently prepare random qubits and both send them to the relay node for measurement. Several demonstrations and field trials of time-bin phase-coding MDI-QKD have been reported in China [32-35], featuring a metropolitan scale of less than 200 km between Alice and Bob and a key rate of only several bits per second [33]. A field trial demonstrated fiber distances of 15-30 km from users to the relay node with key rates of 16-38.8 bit/s [35]. More sophisticated three-intensity [36] and asymmetric four-intensity [37, 38] decoy-state protocols were proposed to further extend the distance and increase the key rate. The asymmetric four-intensity decoy-state protocol exploits three intensities (vacuum, weak, and signal states) in the X basis, and one intensity in the Z basis, and archives a distance record of 404 km using ultra-low loss optical fibers (0.16 dB/km) with a key rate of only 1.16 bit/s per hour [38].

Both conventional prepare-and-measure and MDI-QKD protocols have their key rate scaling linearly with the channel transmittance η, which decays exponentially with fiber distance. This linear bound severely limits the achievable key rate [39]. TF-QKD, on the other hand, overcomes the linear key-rate constraint by matching the phases of two coherent states and encoding key information into the common phase. It has the key rate scaling with the square root of the channel transmittance while keeping the same untrusted relay merit as MDI-QKD [39-46]. Using a practical sending-or-not-sending (SNS) protocol [39], several milestone experiments have been demonstrated to set new distance records for fiber-based terrestrial QKD, e.g. 509 km over ultra-low loss fiber in the lab [43], long-haul field trials over 511 km [44] and 428 km [45], and dual-band stabilization technique to reduce Rayleigh scattering noise and achieve up to 605 km distance [46].

The point-to-point (P2P) nature of quantum channels and its requirement of dedicated fiber also hamper the wide deployment of terrestrial QKD networks. To enable the coexistence of quantum and classical channels in existing fiber infrastructures, wavelength division multiplexing (WDM) of quantum and classical channels has been investigated [47, 48]. Many reported works focus on the interference caused by spontaneous Raman scattering (SRS) from classical channels [49-52]. So far, the coexistence of quantum and classical channels has been demonstrated in backbone [53, 54], metro [55-58], and access [59-65] networks.

Due to the low channel loss in space and negligible interference from classical channels, satellite QKD drew significant research interest and has been considered as a promising candidate to provide global coverage of QKD networks [66, 67]. The feasibility studies of satellite QKD started back in 2002 [68-70]. The first step toward satellite QKD is a ground-based free-space quantum link realized in 1996 [71] with a 150-m indoor path or a 75-m outdoor path. After that, several ground-based free-space QKD links were reported extending the link distance from 75 m to 144

km [72-76]. Then the road toward satellite QKD was paved by the demonstration of dynamic free-space QKD links, including flying transmitters placed on an airborne platform [77, 78] and moving quantum receivers placed on a truck [79] or aircraft [80, 81]. Most free-space QKD links were investigated as a preliminary study for satellite QKD, but they are not quite practical from the deployment perspective. They require line-of-sight (LoS) connections and are subject to geographical constraints (e.g. landscape and buildings) and environmental influences, such as vibration, adverse weather, and atmospheric turbulence. In real applications, free-space QKD links are used in the last segment of access networks.

Thanks to the low channel loss in space, satellite QKD has achieved distances of more than 1000 km [82-92]. Most reported works focused on low-earth-orbit (LEO) satellites, where a precise acquisition, pointing, and tracking system is required to follow the fast-moving satellite with high angular speed [82, 83]. The Micius satellite at ~500 km altitude realized downlink QKD from the satellite to ground over 1200 km [84]. As a trusted relay, it also enables intercontinental quantum-secured communication over 7600 km between China and Austria [85, 86]. Although downlink QKD from a satellite to the ground has the potential for higher detection efficiency and higher key rates, it requires more payload on the satellite and is not as flexible as an uplink configuration, where a simple payload of a quantum receiver is placed on a spacecraft. Micius uses a downlink for QKD and entanglement distribution, and it is also compatible with uplink for quantum teleportation [83]. Canada's satellite plan (QEYSSat) employs an uplink scheme [87], and many works have been done to verify the feasibility of high channel loss [88-90], optical terminal design [91], and noise of single-photon detectors (SPDs) in the space [92]. To further simplify the payload on satellite, a corner cube retroreflector with a modulator for polarization encoding is proposed [93]. Besides LEO, medium earth orbit (MEO) satellites [94] and geostationary orbit (GEO) [95, 96] provide longer flyover time window and larger coverage area, but with the penalty of higher channel loss and lower key rate. Their feasibility is also under investigation. Miniaturization and standardization of satellites are also trends of satellite QKD [97-101].

All the aforementioned satellite QKD schemes utilize the satellite as a trusted relay. To eliminate the key leakage at the satellite, satellite-to-ground entanglement distribution has been demonstrated [102-105] with a distance record of 1200 km [104]. Before that, free-space entanglement distribution on the ground was studied [106-109] over a distance of more than 100 km in the atmosphere [107, 109]. Moreover, free-space MDI-QKD was also demonstrated as an alternative to entanglement distribution [110].

So far, many deployment strategies for QKD have been developed, including terrestrial QKD based on optical fibers, QKD via ground-based free-space links and air-to-ground links, and satellite QKD. Since each method has its strengths and limitations, none of them can achieve global coverage alone. So far as we know, there is no investigation to compare the pros and cons of different deployment technologies. In this paper, we present a literature overview and comparative study of existing deployment strategies of QKD and compare their pros and cons in terms of channel loss, interference, distance limit, connection topology, deployment cost, and use scenarios. Selection criteria and deployment requirements for different network segments are developed to enable a global coverage of QKD networks, from intercontinental, long-haul, to metro and access networks.

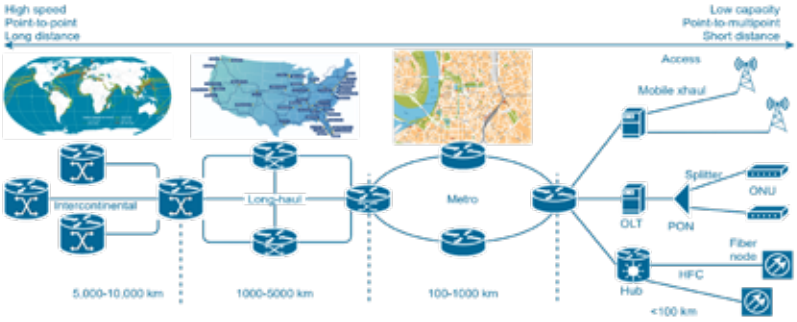

Figure 1 - Global coverage of telecommunication networks, from the intercontinental, long-haul to metro and access networks

Fig. 1 shows a global telecommunication network, which can be divided into four segments according to the coverage area, intercontinental (>5000 km), long-haul (1000-5000 km), metro (100-1000 km), and access (<100 km). Each segment features different connectivity topologies. Intercontinental and long-haul networks feature P2P topology; metro networks utilize ring and mesh topologies; access networks have tree or star topologies.

Terrestrial QKD via Optical Fibers

Fig. 2(a) shows the architecture of a terrestrial QKD link via optical fibers. To avoid the interference caused by SRS noise from classical channels, the quantum channel is ideally deployed in a dedicated dark fiber. In case of fiber deficiency, it can also be deployed in the same fiber with the classical channel using time/wavelength-division multiplexing (TDM/WDM) techniques. There are several techniques to reduce the interference from classical channels, such as spectral filtering before the quantum receiver, temporal filtering (i.e., gated single-photon detectors), and power control of classical data traffic.

Figure 2 - Terrestrial QKD via optical fibers. (a) To avoid interference from classical channels, the quantum channel is deployed in a dedicated fiber. (b) The setup of a prepare-and-measure QKD link.

Fig. 2(b) shows the setup of a prepare-and-measure QKD link. So far, several fiber-based terrestrial QKD networks have been demonstrated, including the DARPA quantum network in Boston [21, 22], SwissQuantum network in Geneva [23, 24], SECOQC network in Vienna [25-28], metropolitan QKD networks in Tokyo [29] and Cambridge [30], and Beijing-Shanghai QKD backbone network in China [31]. Most of them are based on the prepare-and-measure protocol with limited distances to hundreds of km. The usable distance will be further reduced to ~100 km in real deployments. This is because the achievable key rate scales linearly with channel transmittance, whereas in optical fibers the channel transmittance decays exponentially with distance due to the photon absorption, making fiber-based terrestrial QKD impractical for long-haul applications. For example, with a loss of 0.2 dB/km, a 1000 km fiber introduces a

channel loss of 200 dB, which is so high that only 0.3 photons arrive at the receiver per century even if a 10-GHz single-photon source was used at the transmitter.

Figure 3 - Trusted relay for terrestrial QKD networks. (a) The operation principles of a trusted relay. (b) A trusted relay node offers compatibility with point-to-multipoint networks

Relay technologies are essential to increase the distance and enhance the coverage area of terrestrial QKD networks. There are two categories of relay technologies, trusted and untrusted, depending on whether the relay node has access to the keys. The operation principles of a trusted relay node are shown in Fig. 3(a). It connects two neighboring nodes that are too far away from each other to establish a direct QKD link. The trusted relay node, Charlie, performs QKD with Alice and Bob respectively and obtains keys of KA and KB. He then makes a parity announcement of KC=KA⊕KB, which is a bitwise parity-check of KA and KB. Since the original keys are independent bit strings, their bitwise parity is a uniformly random bit string, which does not reveal any information about the keys. With the help of KC, both Alice and Bob can then infer the key of each other using the fact that KA⊕(KA⊕KB)=KB and KB⊕(KA⊕KB)=KA. Trusted relays can unlimitedly extend the distance of secure communication, but with the penalty of key exposure at each relay node. An interesting synergy is that classical fiber cables have repeaters every 100 km for the reamplification, reshaping, and retiming of classical pulses. Trusted relay nodes can be deployed at the same locations as classical repeaters. Since classical repeaters have fixed and public locations, relay nodes collocated with repeaters will be subject to constant surveillance and probing. For example, the Beijing-Shanghai backbone link in China uses 32 trusted relay nodes to divide the overall distance of more than 2000 km into many small segments, each less than 100 km. Moreover, a trusted relay node offers compatibility to the point-to-multipoint (P2MP) network topology, as shown in Fig. 3(b).

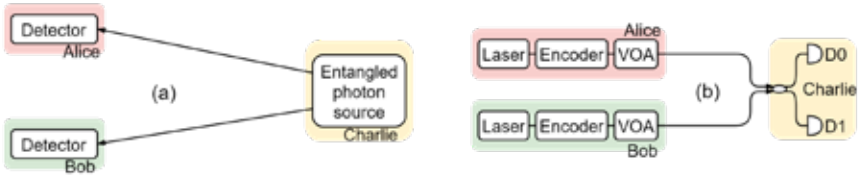

Figure 4 - Untrusted relay for terrestrial QKD networks. (a) Distribution of entangled photon pairs. (b) Measurement-device-independent (MDI) QKD

On the other hand, an untrusted relay eliminates the key leakage at the relay node. It can be implemented by the distribution of entangled photon pairs or MDI-QKD. In either case, the relay node has no information on the keys and could even be an eavesdropper itself. Fig. 4(a) shows

Revista Abierta de Informática Aplicada/ (): 9-30
ISSN 2591-5320

an entanglement distribution setup, where an entangled photon source at the relay node generates entangled photon pairs (EPR) using a nonlinear crystal or nonlinear fibers. The entangled photons are distributed to two users, who make independent measurements and get correlated results. The relay node is considered secure since the entangled photon source has no access to the exact states of two photons, but the measurement results of two users are always correlated. Fig. 4(b) shows an MDI-QKD setup. Two users prepare random qubits independently and send them to the relay node for Bell state measurements (BSM). Although the BSM cannot tell the exact states of two incoming photons, it can tell whether or not the two photons have entangled states. By post-selecting entangled photons from the two users, MDI-QKD is equivalent to a time-reversed EPR protocol. So far, the distance record for MDI-QKD is 404 km using asymmetric four-intensity decoy-state protocol in ultra-low loss optical fibers [38]. The key rate, however, is only 1.16 bit/s per hour, which is orders of magnitude lower than practical requirements.

The key rate of conventional QKD, including prepare-and-measure protocols, entanglement distribution, and MDI-QKD, has linear dependency on the channel transmittance η. Since the channel transmittance decays exponentially with distance in optical fibers, this linear bound severely limits the achievable key rate and distance of terrestrial QKD networks. Recently, a new QKD protocol, twin-field (TF) QKD, was proposed to overcome the linear key-rate constraint. Its setup is almost identical to a phase-encoding MDI-QKD and maintains the same merit of an untrusted relay, where pairs of phase-randomized optical fields are generated at two distant locations and combined at a central measuring station. Fields imparted with the same random phase are 'twins' and can be used to distill a key. By matching the phases of two coherent states and encoding key information into the common phase, TF-QKD exhibits the same dependence on distance as quantum repeaters, i.e. its key rate scales with the square root of the channel transmittance. Several milestone experiments have been demonstrated to set new distance records of fiber-based terrestrial QKD links [43-46]. It should be noted that in MDI-QKD, the two photons from two users interfere at the relay station. Charlie's receiver has two-photon interference and records coincidence detections. In TF-QKD, however, two optical fields are sent from both users and Charlie's receiver has a single-photon interference followed by a single-photon detection event. TF-QKD retains the characteristics of MDI-QKD, whereas gaining extra distance thanks to the square-root dependence of key rate on the channel transmittance.

Free-Space QKD

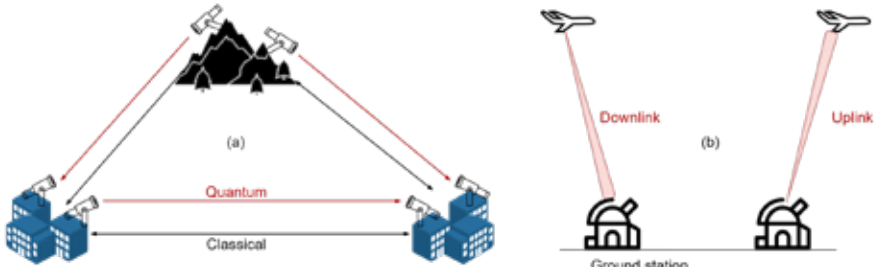

Figure 5 - Free-space QKD. (a) Ground-based free-space QKD links. (b) Free-space QKD links to/from an aircraft

Fig. 5 shows the architectures of free-space QKD. Fig. 5(a) shows ground-based free-space QKD links. Different from optical fibers, free-space QKD requires LoS connections, and the transmitters and receivers are usually deployed on top of buildings or mountains to avoid obstruction in the path. The associated classical channels could exploit wireless links, e.g. cellular, microwave, or rely on free-space optics as well. Since no fiber trenching is required, free-space QKD features low deployment cost, easy and fast installation, and is an important reinforcement for fiber-based QKD networks owing to its configurational flexibility. The distance record for ground-based free-space QKD is 144 km [76]. Dynamic free-space QKD links to/from an aircraft were investigated as a preliminary step toward satellite QKD and the feasibility of both downlink and uplink configurations have been verified, shown in Fig. 5(b). A downlink scheme includes a flying transmitter on an airborne platform and a receiver on the ground [77, 78]; an uplink configuration uses a ground-based transmitter and places a quantum receiver on aircraft [80, 81]. The downlink scheme has higher detection efficiency, whereas the uplink scheme has a smaller payload on aircraft.

Since the quantum channel is not confined in the waveguide of optical fibers, free-space QKD is subject to environmental influence, such as vibration, adverse weather (fog, rain, cloud), and atmospheric turbulence. Although the atmosphere has lower absorption than optical fibers, only 0.07 dB/km at 2400 m, the channel loss of free-space QKD is not dominated by absorption. Instead, it is determined by diffraction, weather, turbulence, and misalignment. Moreover, free-space quantum channels are subject to decoherence more than those in optical fibers, which further limits the link distance. On the other hand, there is no interference from classical channels in free-space and the coexistence of quantum and classical channels is no longer an issue. Free-space QKD can easily support P2MP topologies, making it a promising candidate for inter-building secure communication in the last few miles of access networks.

Satellite as a Trusted Relay

Thanks to the low channel loss in space, negligible interference from classical channels, and reduced environmental influences, satellite QKD can achieve distances more than 1000 km. It is not limited by terrestrial conditions and can provide coverage for rural areas. Most reported work focused on LEO satellites with altitudes of less than 900 km, where a precise acquisition, pointing, and tracking system is required to follow the fast-moving satellite. The feasibility of MEO and GEO satellites is also under investigation. Miniaturization and standardization of satellites are also trends of satellite QKD. Fig. 6 shows the operation principles of satellite QKD where the satellite is used as a trusted relay. An LEO satellite performs downlink QKD with two ground stations, Alice and Bob, respectively. It then makes a parity announcement, so that Alice and Bob can infer each other's keys. The satellite needs LoS connections with Alice and Bob, but not necessarily at the same time. It can exchange keys with several ground stations one after another as it flies over them. As a trusted relay, any access to the satellite leaks the complete information about keys. The associated classical channels for satellite QKD can rely on terrestrial fibers, microwave, or free-space laser communication in space. For example, most Starlink satellites are currently operating in Ku and Ka bands and can be upgraded to laser communication in the future.

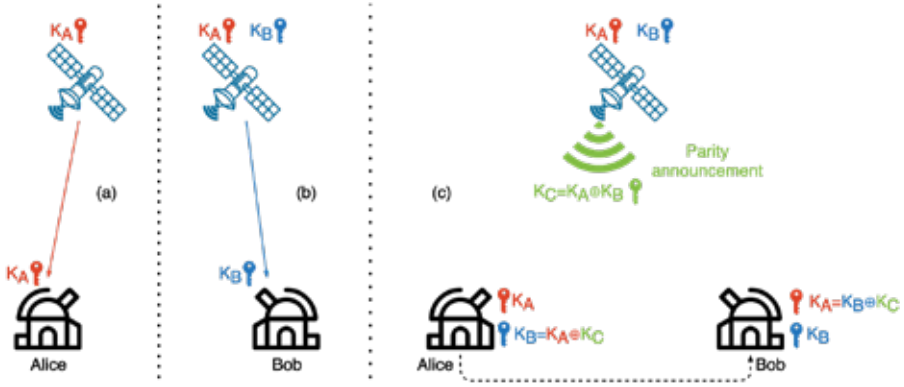

Figure 6 - Satellite as a trusted relay. The satellite first exchanges keys with ground stations, Alice (a) and Bob (b), respectively, then makes a parity announcement (c) so that Alice and Bob can infer each other's keys.

Since the effective thickness of the atmosphere is only ~10 km, the propagation of a quantum channel takes place mostly in vacuum space with negligible absorption and turbulence. Instead of absorption, the channel loss of satellite QKD is determined by beam diffraction and scales quadratically with distance. In comparison, the channel loss of terrestrial QKD is dominated by fiber absorption and scales exponentially with distance. Channels in space also have smaller decoherence than those in the atmosphere or optical fibers. For example, a 600-km optical fiber has a channel loss of 120 dB, whereas a link of the same length in space from satellite to the ground has a loss of only 50 dB given a reasonable aperture size is used at the receiver telescope. This is why satellite QKD can reach much longer distances. Inter-satellite channels have even lower losses due to the absence of atmosphere.

Channel loss in space comes from two sources, beam diffraction and beam spreading beyond the effects of diffraction. Diffraction loss depends on the divergence of the transmitter telescope and the aperture size of the receiver telescope. Further beam spreading arises from wavefront aberrations caused by refractive index inhomogeneities due to atmospheric turbulence. There are two categories of turbulence. Small turbulence induces beam spreading, whereas large turbulent eddies with sizes larger than the beam spot cause beam wandering. A long-term beam spot is a superposition of moving short-term beam spots. The short-term beam size is determined by spreading and the instantaneous beam displacement from the unperturbed position caused by beam wandering. In real applications, the channel loss from a satellite to a ground station is dominated by diffraction, followed by beam spreading. Beam wandering and absorption have negligible contributions to the channel loss.

Satellite QKD has three different schemes, downlink, uplink, and retroreflection. In Fig. 7(a), the downlink scheme has the quantum transmitter on a satellite and receiver on the ground. Since the effective thickness of the atmosphere is only ~10 km, the optical beam first propagates through vacuum space where the only channel loss is diffraction, then passes through the atmosphere in the final stage of the path. Due to the diffraction effect, when the beam arrives at the atmosphere, its size has been larger than most turbulent eddies. There is no beam wandering and the beam size is spread slightly by wavefront aberrations caused by turbulence. For the downlink configuration, atmospheric turbulence has a limited impact on the channel loss and beam spreading. For

example, the beam size after 1200 km downlink propagation expands to 12 m with diffraction loss of ~22 dB depending on the receiver telescope size [84]. Atmospheric turbulence introduces additional 3-8 dB attenuation, with an overall channel loss of less than 30 dB [84].

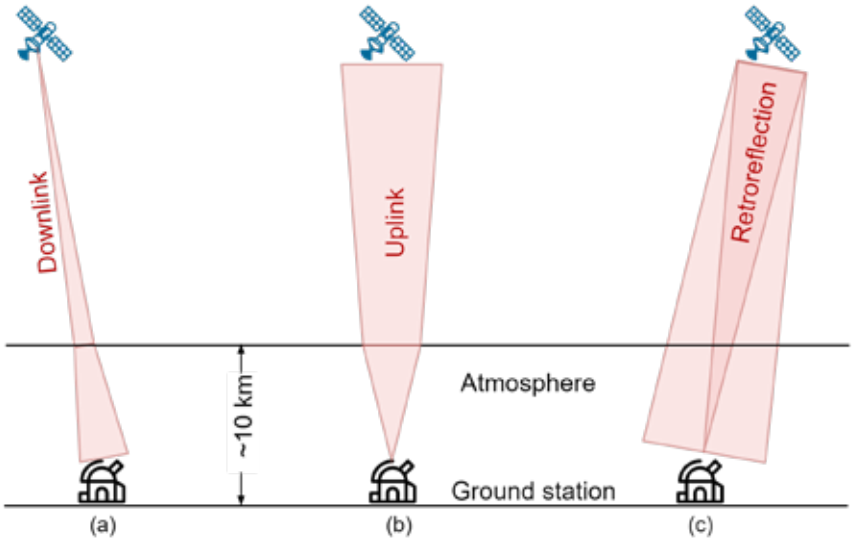

Figure 7 - Downlink (a) and uplink (b) configurations of satellite QKD

In Fig. 7(b), an uplink channel first propagates through the atmosphere, where the wavefront aberration induced by turbulence causes significant beam spreading. At 500 km altitude, the beam size of an uplink channel can reach up to 50 m, much larger than any available spaceborne telescope aperture. Downlink channels can exploit large aperture receiver telescopes on the ground, but uplink channels have limited aperture size for receiver telescopes due to the weight and size limit on satellites. Thanks to the strong wavefront aberration, large beam spot, and small aperture size, uplink channels have higher channel loss than downlink ones. For example, a 500-km uplink channel has a loss up to 50 dB; whereas a downlink channel of the same length would have a loss less than 20 dB [88]. Most uplink channels cannot work without the help of the decoy-state technique [88].

Although the downlink scheme has higher detection efficiency and higher key rates, the transmitter setup requires more payload on the satellite and needs more adjustment during operation, which makes the downlink scheme not as flexible as an uplink configuration. The uplink scheme, on the other hand, only needs a simple payload of quantum receivers on the satellite, enabling an easier operation on the satellite. The downlink scheme leaves expensive and delicate SPDs on the ground for better protection, cooling, and maintenance; whereas the uplink scheme has to launch the sensitive SPDs into space, which have to go through launch vibration, shock in the flight, extreme temperature, and work under adverse conditions in space. Due to the sunlight, the satellite temperature varies by up to tens of degrees in one orbit, and there is limited electrical power on the satellite for cooling. The only way to dissipate heat is by radiation. To make things worse, most SPDs are avalanche photon detectors (APD), which are sensitive to dark counts caused by ionizing radiation in space. The feasibility of low-noise SPDs on a satellite is under investigation [92]. So far, downlink and uplink schemes are both considered important for future

satellite QKD. For example, Micius uses downlink QKD and entanglement distribution, and it is also compatible with uplink for quantum teleportation [83]. Canada's satellite plan (QEYSSat) employs an uplink scheme [87], and many works have been done to verify the feasibility of high channel loss [88-90], optical terminal design [91], and noise of SPDs in space [92].

In a quantum channel, the qubits are carried by single photons and no amplification is allowed. The only way to increase the signal-to-noise ratio (SNR) is to reduce channel loss and background noise. Thanks to the low loss, downlink channels have larger SNR than uplink ones. In the daytime, the background noise from sunlight makes it difficult to establish a QKD link. One way to improve SNR in the daytime is to use the wavelengths at Fraunhofer lines, i.e. Sun absorption lines. At night, background noise is dominated by moonlight and scattered light from human activities, which depends on the location of the ground stations. SNR at night is orders of magnitude higher than that in the daytime, which is why most satellite QKD works were demonstrated at clear night by downlink channels. There are several techniques to improve the SNR of a free-space quantum link, e.g., reducing the beam size, reducing the field-of-view of the receiver telescope, narrowband spectral filtering before the receiver, and temporal filtering (gating window) of SPDs.

To further simplify the payload on satellites, a third configuration, retroreflection, was proposed [93, 94], as shown in Fig. 7(c). It uses an orbiting corner cube retroreflector on a satellite with a modulator to encode polarizations. The single-photon transmitter is realized by corner cube retroreflectors mounted on a satellite. Only the reflected beam from the satellite to the ground is a quantum channel; the laser beam from the ground station to the satellite is a classical channel with strong pulse intensity. This configuration features a compact and low-cost payload on satellite and can be used on not only LEO but also MEO and GEO satellites. The feasibility of single-photon exchange from an MEO satellite using a retroreflection scheme has been verified [94].

Satellite as an Untrusted Relay

When a satellite is used as a trusted relay, it has access to all the keys of all ground stations. To avoid the key leakage at the satellite, untrusted relaying is preferred since the eavesdropper gets no information even if it takes full control of the satellite. Fig. 8 shows the architecture of satellite QKD with the satellite as an untrusted relay. Fig. 8(a) shows entanglement distribution, where an entangled photon source on a satellite sends entangled photons down to two ground stations, Alice and Bob, respectively. Alice and Bob make independent measurements on the incoming photons and get correlated results. Since the entangled photon source has no control over the exact qubits carried by each photon, the satellite has no information of the key. For entanglement distribution, the loss of two downlink channels has to be combined since only photon pairs that both arrive at ground stations can be used for keys.

As an alternative, Fig. 8(b) shows satellite MDI-QKD, where two ground stations independently prepare random qubits and send them via uplink channels to a satellite for BSM. Satellite MDI-QKD is equivalent to a time-reversed entanglement distribution protocol. The BSM can only tell whether or not the two photons are entangled, but it cannot tell the exact states of two incoming photons. The loss of two uplink channels has to be combined since only photon pairs that both arrive at the satellite can be used for keys. Due to the high loss of uplink channels, there is no demonstration of satellite MDI-QKD so far. But the feasibility study of free-space MDI-QKD

has been reported on the ground over 19.2 km [110], well beyond the effective thickness of the atmosphere (~10 km).

Unlike trusted relaying, untrusted relaying requires simultaneous LoS connections from the satellite to both ground stations, which limits the separation distance between ground stations. For a given altitude of the satellite, wider separation between ground stations makes lower slant angles and longer propagation in the atmosphere, which leads to higher channel loss. The current distance record for entanglement distribution is ~1200 km, achieved by an LEO satellite Micius of China [104].

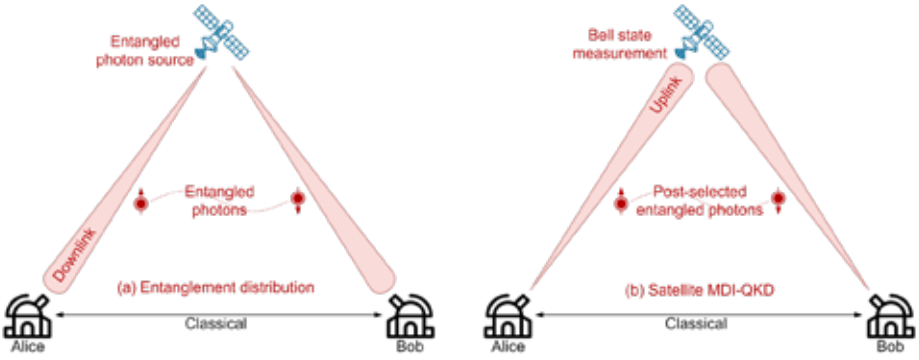

Figure 8 - Satellite QKD with the satellite as an untrusted relay. (a) Entanglement distribution from a satellite. (b) Free-space MDI-QKD to a satellite

Deployment Strategies for Global Coverage

Table 1 lists the pros and cons of different deployment strategies of QKD networks, including fiber-based terrestrial QKD, free-space QKD including ground-based and ground-to-air schemes, satellite QKD with the satellite used as a trusted or untrusted relay. Terrestrial QKD via optical fibers suffers from high channel loss and short distance but offers compatibility with existing fiber infrastructure and P2MP topologies. Since the quantum channels are confined in fiber waveguides, terrestrial QKD networks can operate all day in adverse environments, such as background light, weather, and vibration. Without relays, a single span of fiber-based QKD can reach ~100 km in the field, only suitable for metro and access networks. Trusted relaying can extend the distance of fiber-based QKD unlimitedly with the penalty of key leakage at each relay node. An interesting synergy is that classical fiber cables also have repeaters every 100 km. Trusted relay nodes can be deployed at the same locations as classical repeaters. Since classical repeaters have fixed and public locations, relay nodes collocated with repeaters will be subject to constant surveillance and probing. In contrast, satellite QKD using a satellite as a trusted relay is more secure because the satellite and quantum links are moving fast, making side-channel attacks difficult.

Table 1 - Pros and cons of fiber-based terrestrial QKD, free-space QKD, and satellite QKD

Deployment strategies	Fiber-based terrestrial QKD	Ground-based Free-space QKD	Ground-to-air free-space QKD	Satellite QKD (trusted relay)	Satellite QKD (untrusted relay)
Attenuation	Fiber absorption	Diffraction Turbulence Weather Absorption	Same as ground-based QKD plus	Diffraction Turbulence Weather	Diffraction Turbulence Weather
Interferences from classical channels	Spontaneous Raman scattering noise	No	No	No	No
Channel loss	High, scale exponentially with fiber length	High, scale exponentially with distance		Low Scale quadratically with distance	
Distance	~100 km in fields without relay unlimited distance with trusted relay MDI-QKD: 404 km in the lab [38] 200 km in fields [33] TF-QKD: >500 km in lab [43, 44, 46] 428 km in fields [45]	144 km in	96 km in experiments [78]	Satellite to the ground distance over 1200 km [84] Unlimited distance between ground stations	1200 km between ground stations for a 500-km altitude LEO satellite longer for MEO/ GEO
Compatibility to P2MP topology	P2MP	P2MP	P2P at a time	P2P at a time	satellite to two ground stations
Line-of-sight	No	Yes	Yes	Yes	Simultaneous LoS with both ground stations
Time window	whole day	Only night need special care for daytime operation		Short window in the clear night	
Deployment	Low cost Dedicated fiber or reuse existing ones	Low cost Simple and fast installation No fiber trenching		Expensive and slow Synergy with satellite laser communication in space	
Application scenarios	Metro, access	last few miles of access networks		Long-haul	

Ground-based free-space QKD requires LoS connections, and the transmitters and receivers are usually deployed on top of buildings or mountains to avoid obstruction in the path. It supports P2MP topology and can handle the coexistence of quantum and classical channels without interference. These features make it suitable for the last few miles of access networks among buildings. Although the atmosphere has lower absorption, the channel loss of free-space QKD is dominated by diffraction, adverse weather, and atmospheric turbulence. The distance record of ground-based free-space QKD is 144 km [76], but in real deployments, the usable distance will be less than 10 km for practical key rates. Since no fiber trenching is required, ground-based free-space QKD features low deployment cost, fast and easy installation, and serves as an important reinforcement for fiber-based QKD networks. The ground-to-air free-space QKD shares the same pros and cons of ground-based counterparts plus the additional channel loss caused by misalignment and vibration due to the movement of the aircraft. We do not include the applications of airborne free-space QKD here, since it was mainly investigated as a preliminary step towards satellite QKD.

Compared with terrestrial and free-space QKD, satellite QKD features low channel loss and long distances. The downlink scheme from satellite to the ground has higher detection efficiency and higher key rates thanks to the lower loss and less turbulence-induced wavefront abbreviation. But it requires more payload on the satellite and needs more adjustment during operation. The uplink channels are more flexible, since it only needs a simple payload of quantum receivers on the satellite, enabling an easier operation on the satellite. On the other hand, the downlink scheme leaves expensive and delicate SPDs on the ground for easiest maintenance; whereas the uplink scheme launches the sensitive SPDs into space, which have to go through the launch vibration, shock in the flight, extreme temperature, and work under adverse conditions in space.

Satellite QKD requires LoS connections between the satellite and ground stations and only works at night due to the background noise from sunlight during the daytime. To reduce the channel loss, LEO satellites are preferred, but low altitude leads to the fast movement of the satellite, a small coverage area, and a short flyover time window for each ground station. MEO satellites at higher orbit provide wider coverage and longer flyover time, but with the penalty of higher channel loss and lower key rate [94]. To choose an appropriate altitude, a trade-off must be made between the coverage area and time window versus channel loss and key rate. An extreme example is a GEO satellite, which has an operational time window of the whole night but with a long path length of 35,786 km [95, 96].

There is a strong synergy between satellite QKD and classical satellite communication. For example, space communication also exploits LEO satellites at an altitude of 300-1000 km. Starlink plans to launch thousands of satellites at altitudes of 350-580 km. Although these satellites are using microwave communication in Ku and Ka bands, most of them are equipped with optical transceivers for future upgrades to laser communication. By adding quantum transmitters onboard, these satellites can be used as a trusted relay for QKD in space. Since quantum transmitters for most prepare-and-measure protocols only consist of commercial off-the-shelf devices, this upgrade will not significantly increase the satellite cost. The beam acquisition, tracking, and pointing systems designed for laser communication in space can also be reused by quantum channels. Satellite QKD covers long-haul networks, and by using the satellites as a trusted relay, its secure distance can be extended unlimitedly.

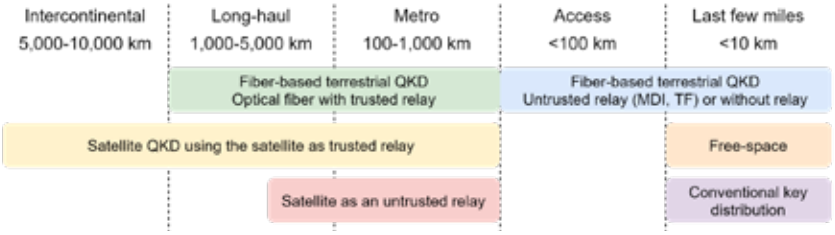

Figure 9 - Deployment strategies for global coverage of QKD networks

The scheme with a satellite as an untrusted relay shares the same pros and cons with trusted relays but eliminates the key leakage at satellites. It requires simultaneous LoS connections from the satellite to both ground stations, which limits the separation between two ground stations. The distance record of entanglement distribution from a satellite is 1200 km, which can be employed for long-haul networks, but not long enough for intercontinental connections. Fig. 9 shows the

deployment strategies for global coverage of QKD networks, from the intercontinental, long-haul, metro to access networks.

It should be noted that not all user devices are equipped with optical terminals for fiber or free-space optics connections. Radio access has been and will continue to be used extensively in the last few miles of access networks. In these cases, keys have to be distributed wirelessly in a classical way to user devices. Fig. 10 shows a hierarchical key delivery architecture. Several secure sites, e.g. bank buildings, business campuses, government offices, are connected by satellite, fiber-based or free-space QKD links, so the keys are delivered in an absolute secure way among these secure sites. Within each secure site, however, the keys are distributed wirelessly to mobile users using PQC algorithms. This involves a trade-off between security and mobility because it is not feasible to connect all devices with optical fibers or free-space optics. We thus have to leverage the ubiquity and flexibility of radio access technologies in the last few miles.

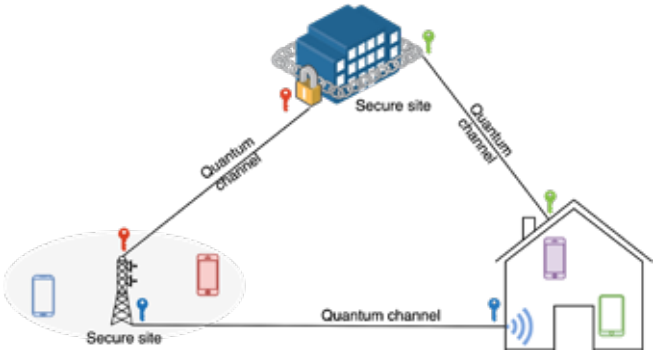

Figure 10 - Hierarchical key delivery over the last few miles in access networks

In this hierarchical architecture, two different levels of security-as-a-service (SaaS) are provided, i.e. absolute security over long-distance among secure sites, and computational classical security over a short distance within each site. Once the mobile users get the keys, they can use these keys to encrypt their wireless communication. They can even roam away from the secure site and continue the secure communication as soon as they still possess the keys. Once they consume all the keys, they have to return to a secure site to fetch new keys. It should be noted that PQC and QKD do not necessarily compete with each other. Instead, they should work in an orchestrated way to complement each other. For example, PQC could exploit the keys delivered by QKD to enhance its security, while QKD can employ PQC for authentication, which cannot be handled by QKD itself.

Conclusions

To date, many deployment strategies of QKD networks have been demonstrated, but none of them provides global coverage of QKD networks. A comparative study on the pros and cons of various deployment strategies is still missing. In this paper, the state-of-the-art deployment technologies of QKD networks, including fiber-based terrestrial QKD, free-space QKD, and satellite QKD, are compared in terms of channel loss, interference, distance limit, connection

topology, deployment cost, and application scenarios. Instead of competing with each other, these different deployment strategies will work in an orchestrated way to complement each other and enable a global coverage of QKD networks, from intercontinental, long-haul, to metro and access networks.

Given its compatibility with P2MP topology and ~100-km distance limit without relay, fiber-based terrestrial QKD is suitable for metro and access networks. With the help of a trusted relay, the QKD distance can be extended unlimitedly to cover long-haul networks, where the relay nodes are collocated with classical fiber repeaters. Ground-based free-space QKD is limited to 10 km due to diffraction, weather, and atmosphere turbulence, and is suitable for the last few miles among buildings in access networks. Satellite QKD features low channel loss, high key rates, and long distances more than 1000 km. By utilizing satellites as trusted relays, the QKD distance can be extended infinitely and can be used for intercontinental, long-haul, and metro networks. Furthermore, satellite QKD is not restricted by terrain conditions and can reach rural underserved areas without difficulty. On the other hand, using an LEO satellite as an untrusted relay requires simultaneous LoS connections from the satellite to both ground stations, where the separation between the ground stations is limited by the altitude of the satellite. MEO and GEO satellites feature longer time windows and larger coverage areas, but with the penalty of higher channel loss and lower key rate.

Abbreviations

APD	avalanche photon detector
BSM	Bell-state measurement
ECC	elliptic curve cryptography
EPR	entangled photon pair
GEO	geostationary orbit
LEO	low-earth-orbit
LoS	line-of-sight
MEO	medium-earth-orbit
MDI	measurement-device-independent
NIST	National Institute of Standards and Technology
P2P	point-to-point
P2MP	point-to-multipoint
PNS	photon-number-split
PQC	post-quantum cryptography
QKD	quantum key distribution
SaaS	security-as-a-service
SNR	signal-to-noise ratio
SNS	sending-or-not-sending
SPD	single-photon detector
SRS	spontaneous Raman scattering
TDM	time-division multiplexing
TF-QKD	twin-filed QKD
WCP	weak coherent pulses
WDM	wavelength division multiplexing

References

» P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Journal on Computing, vol. 26, no. 5, pp. 1484-1509, 1997.

» E. Grumbling, M. Horowitz, (eds.), "Quantum Computing: Progress and Prospects," The National Academies Press, Washington, DC, https://doi.org/10.17226/25196.

» F. Arute, K. Arya, R. Babbush, "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, pp. 505-510, October 2019.

» IBM Research Blog, "On 'Quantum Supremacy'" 22 October 2019.

» D. J. Bernstein, "Introduction to post-quantum cryptography," In: D. J. Bernstein, J. Buchmann, E. Dahmen (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg, 2009.

» L. Chen, S. Jordan, Y.-K. Liu, et. al., "Report on Post-Quantum Cryptography," NISTIR 8105, 04/28/2016.

» G. Alagic, J. Alperin-Sheriff, D. Apon, et. al., "Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process," NISTIR 8240, 01/31/2019.

» G. Alagic, J. Alperin-Sheriff, D. Apon, et. al., "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process," NISTIR 8309, 07/22/2020.

» C. H. Bennett, "Quantum Cryptography: Uncertainty in the Service of Privacy," Science, vol. 257, no. 5071, pp. 752-753, 1992.

» N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Reviews of Modern Physics, vol. 74, no. 1, pp. 145-195, Mar 2002.

» V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, et al., "The security of practical quantum key distribution," Reviews of Modern Physics, vol. 81, no. 3, pp. 1301-1350, Sep 2009.

» H. K. Lo, M. Curty, K. Tamaki, "Secure quantum key distribution," Nature Photonics, vol. 8, pp. 595-604, 2014.

» C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 10-12 December 1984, pp. 175-179.

» C. H. Bennett, F. Bessette, G. Brassard, et al., "Experimental quantum cryptography," Journal of Cryptology, vol. 5, pp. 3-28, 1992.

» D. Gottesman, Hoi-Kwong Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quantum Information & Computation, vol. 4, no. 5, pp. 325-360, Sep 2004.

» H.-K. Lo, X. Ma, K. Chen, "Decoy State Quantum Key Distribution," Physical Review Letters, vol. 94, no. 23, pp. 230504, Jun 2005.

» H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Physical Review Letters, vol. 108, 130503, Mar 2012.

» Z. Tang, Z. Liao, F. Xu, et al., "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution," Physical Review Letters, vol. 112, 190503, May 2014.

» J. Qiu, "Quantum communications leap out of the lab," Nature, vol. 508, pp. 441-442, April 2014.

» M. Peev, "Why do I believe that Quantum Key Distribution (QKD) is Finally About to Reach Telecom Markets and Grow Out of Its Present Exotic Standing?," Optical Fiber Communications Conference (OFC) 2019, paper W4D.3.

» C. Elliott, "Building the quantum network," New Journal of Physics, vol. 4, 46.1-46.12, Jan 2002.

» C. Elliott, A. Colvin, D. Pearson, et al., "Current status of the DARPA quantum network," Proc. SPIE 5815,

Quantum Information and Computation III, May 2005.

» P. Eraerds, N. Walenta, M. Legré, et al., "Quantum key distribution and 1 Gbps data encryption over a single fibre," New Journal of Physics, vol. 12, 063027, June 2010.

» D. Stucki, M. Legré, F. Buntschu, et al., "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," New Journal of Physics, vol. 13, 123001, December 2011.

» A. Poppe, M. Peev and O. Maurhart, "Outline of the SECOQC quantum-key-distribution network," International Journal of Quantum Information, vol. 6, no. 2, pp. 209-218, 2008.

» M. Peev, T. Länger, T. Lorünser, et al., "The SECOQC Quantum-Key-Distribution Network in Vienna," Optical Fiber Communication Conference 2009, paper OThL2.

» M. Peev, A. Poppe, O. Maurhart, et al., "The SECOQC Quantum Key Distribution Network in Vienna," 35th European Conference on Optical Communication, Vienna, Austria, 2009, paper 1.4.1.

» M. Peev, C. Pacher, R. Alléaume, et al., "The SECOQC quantum key distribution network in Vienna," New Journal of Physics, vol. 11, 075001, July 2009.

» M. Sasaki, M. Fujiwara, H. Ishizuka, et al., "Field test of quantum key distribution in the Tokyo QKD Network," Optics Express, vol. 19, no. 11, pp. 10387-10409, 2011.

» J. F. Dynes, A. Wonfor, W. W. -S. Tam, et al., "Cambridge quantum network," Nature Partner Journals (NPJ) Quantum Information, vol. 5, article number 101, 2019.

» Q. Zhang, F. Xu, Y.-A. Chen, et al., "Large scale quantum key distribution: challenges and solutions," Optics Express, vol. 26, no. 18, pp. 24260-24273, 2018.

» Y. Liu, T.-Y. Chen, L.-J. Wang, et al., "Experimental measurement-device-independent quantum key distribution," Physical Review Letters, vol. 111, 130502, Sep 2013.

» Y.-L. Tang, H.-L. Yin, S.-J. Chen, et al., "Measurement-device-independent quantum key distribution over 200 km," Physical Review Letters, vol. 113, 190501, Nov 2014.

» Y.-L. Tang, H.-L. Yin, S.-J. Chen, et al., "Field test of measurement-device-independent quantum key distribution," IEEE Journal of Selected Topics in Quantum Electronics, vol. 21, no. 3, pp. 116-122, May-June 2015, Art no. 6600407.

» Y.-L. Tang, H.-L. Yin, Q. Zhao, et al., "Measurement-device-independent quantum key distribution over untrustful metropolitan network," Physics Review X, vol. 6, 011024, Mar 2016.

» X.-B. Wang, "Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors," Physical Review A, vol. 87, 012320, January 2013.

» Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, "Making the decoy-state measurement-device-independent quantum key distribution practically useful," Physical Review A, vol. 93, 042324, April 2016.

» H.-L. Yin, T.-Y. Chen, Z.-W. Yu, et al., "Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber," Physical Review Letters, vol. 117, 190501, November 2016.

» M. Lucamarini, Z. L. Yuan, J. F. Dynes, et al., "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," Nature, vol. 557, pp. 400-403, 2018.

» X. Ma, P. Zeng, and H. Zhou, "Phase-Matching Quantum Key Distribution," Physical Review X, vol. 8, 031043, 2018.

» X. T. Fang, P. Zeng, H. Liu, et al., "Implementation of quantum key distribution surpassing the linear rate-transmittance bound," Nature Photonics, vol. 14, pp. 422-425, 2020.

» X.-B. Wang, Z.-W. Yu, and X.-L. Hu, "Twin-field quantum key distribution with large misalignment error," Physical Review A, vol. 98, 062323, December 2018.

» J.-P. Chen, C. Zhang, Y. Liu, et al., "Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km," Physical Review Letters, vol. 124, 070501, February 2020.

» J. P. Chen, C. Zhang, Y. Liu, et al., "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," Nature Photonics, vol. 15, pp. 570–575, 2021.

» H. Liu, C. Jiang, H.-T. Zhu, et al., "Field Test of Twin-Field Quantum Key Distribution through Sending-or-Not-Sending over 428 km," Physical Review Letters, vol. 126, 250502, June 2021.

» M. Pittaluga, M. Minder, M. Lucamarini, et al., "600-km repeater-like quantum communications with dual-band stabilization," Nature Photonics, vol. 15, pp. 530-535, 2021.

» P. D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," Electronics Letters, vol. 33, no. 3, pp. 188-190, 1997.

» B. Qi, W. Zhu, L. Qian, and H.-K. Lo, "Feasibility of quantum key distribution through a dense wavelength division multiplexing network," New Journal of Physics, vol. 12, 103042, 2010.

» M. S. Goodman, P. Toliver, R. J. Runser, et al., "Quantum cryptography for optical networks: a systems perspective," The 16th Annual Meeting of the IEEE Lasers and Electro-Optics Society (LEOS) 2003, paper ThEE1, vol. 2, pp. 1040-1041.

» N. A. Peters, P. Toliver, T. E. Chapuran, et al., "Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments," New Journal of Physics, vol. 11, 045012, April 2009.

» T. E. Chapuran, P. Toliver, N. A. Peters, et al., "Optical networking for quantum key distribution and quantum communications," New Journal of Physics, vol. 11, 105001, October 2009.

» N. A. Peters, P. Toliver, T. E. Chapuran, et al., "Quantum communications in reconfigurable optical networks: DWDM QKD through a ROADM," Conference on Optical Fiber Communication (OFC) 2010, paper OTuK1.

» L.-J. Wang, K.-H. Zou, W. Sun, et al., "Long-distance copropagation of quantum key distribution and terabit classical optical data channels," Physics Review A, vol. 95, no. 1, pp. 012301, 2017.

» Y. Mao, B.-X. Wang, C. Zhao, et al., "Integrating quantum key distribution with classical communications in backbone fiber network," Optics Express, vol. 26, no. 5, pp. 6010-6020, 2018.

» W. Chen, Z. Han, T. Zhang, et al., "Field experiment on a "star type" metropolitan quantum key distribution network," in IEEE Photonics Technology Letters, vol. 21, no. 9, pp. 575-577, May 2009.

» S. Wang, W. Chen, Z. Yin, et al., "Field test of wavelength-saving quantum key distribution network," Optics Letters, vol. 35, no. 14, pp. 2454-2456, July 2010.

» S. Wang, W. Chen, Z. Yin, et al., "Field and long-term demonstration of a wide area quantum key distribution network," Optics Express, vol. 22, no. 18, pp. 21739-21756, September 2014.

» T.-Y. Chen, J. Wang, H. Liang, et al., "Metropolitan all-pass and inter-city quantum communication network," Optics Express, vol. 18, no. 26, pp. 27217-27225, 2010.

» K. A. Patel, J. F. Dynes, I. Choi, et al., "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," Physical Review X, vol. 2, no. 4, 041010, November 2012.

» B. Fröhlich, J. F. Dynes, M. Lucamarini, et al., "A quantum access network," Nature, vol. 501, pp. 69-72, 2013.

» K. A. Patel, J. F. Dynes, M. Lucamarini, et al., "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," Applied Physics Letters, vol. 104, no. 5, 051123, 2014.

» I. Choi, Y. Zhou, J. F. Dynes, et al., "Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber," Optics Express, vol. 22, no. 19, pp. 23121-23128, 2014.

» B. Fröhlich, J. F. Dynes, M. Lucamarini, et al., "Quantum secured gigabit optical access networks," Scientific Reports, vol. 5, article number 18121, 2015.

» J. F. Dynes, W. W-S. Tam, A. Plews, et al., "Ultra-high bandwidth quantum secured data transmission,"

Scientific Reports, vol. 6, article number 35149, 2016.

» L.-J. Wang, L.-K. Chen, L. Ju, et al., "Experimental multiplexing of quantum key distribution with classical optical communication," Applied Physics Letters, vol. 106, no. 8, 081108, 2015.

» R. Bedington, J. M. Arrazola, A. Ling, "Progress in satellite quantum key distribution," Nature Partner Journals (NPJ) Quantum Information, vol. 3, article number 30, 2017.

» I. Khan, B. Heim, A. Neuzner and C. Marquardt, "Satellite-Based QKD," Optics and Photonics News, Feb 2018.

» J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," New Journal of Physics, vol. 4, 82.1-82.21, 2002.

» C. Bonato, A. Tomaello, V. D. Deppo, et al., "Feasibility of satellite quantum key distribution," New Journal of Physics, vol. 11, 045017, 2009.

» A. Tomaello, A. Dall'Arche, G. Naletto, and P. Villoresi, "Intersatellite quantum communication feasibility study", Proc. SPIE 8163, Quantum Communications and Quantum Imaging IX, 816309, September 2011.

» B. C. Jacobs and J. D. Franson, "Quantum cryptography in free space," Optics Letters, vol. 21, no. 22, pp. 1854-1856, 1996.

» W. T. Buttler, R. J. Hughes, P. G. Kwiat, et al., "Free-space quantum key distribution," Physical Review A, vol. 57, no. 4, pp. 2379-2382, April 1998.

» W. T. Buttler, R. J. Hughes, P. G. Kwiat, et al., "Practical Free-Space Quantum Key Distribution over 1 km," Physical Review Letters, vol. 81, no. 15, pp. 3283-3286, October 1998.

» R. J. Hughes, J. E. Nordholt, D. Derkacs, et al., "Practical free-space quantum key distribution over 10 km in daylight and at night," New Journal of Physics, vol. 4, 43.1-43.14, 2002.

» C. Kurtsiefer, P. Zarda, M. Halder, et al., "Quantum cryptography: a step towards global key distribution," Nature vol. 419, pp. 450, 2002.

» T. Schmitt-Manderbach, H. Weier, M. Fürst, et al., "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km," Physical Review Letters, vol. 98, 010504, January 2007

» S. Nauerth, F. Moll, M. Rau, et al., "Air-to-ground quantum communication," Nature Photonics, vol. 7, pp. 382-386, 2013.

» J. Y. Wang, B. Yang, S. K. Liao, et al., "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," Nature Photonics, vol. 7, pp. 387-393, 2013.

» J.-P. Bourgoin, B. L. Higgins, N. Gigov, et al., "Free-space quantum key distribution to a moving receiver," Optics Express, vol. 23, no. 26, pp. 33437-33447, 2015.

» C. J. Pugh, S. Kaiser, J.-P. Bourgoin, et al., "Airborne demonstration of a quantum key distribution receiver payload," Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC), 2017.

» C. J. Pugh, S. Kaiser, J.-P. Bourgoin, et al., "Airborne demonstration of a quantum key distribution receiver payload," Quantum Science and Technology, vol. 2, no. 2, 024009, June 2017.

» J. Yin, Y. Cao, S.-B. Liu, et al., "Experimental quasi-single-photon transmission from satellite to earth," Optics Express, vol. 21, no. 17, pp. 20032-20040, 2013.

» J. Pan, "Quantum science satellite," Chinese Journal of Space Science, vol. 34, no. 5, pp. 547-549, 2014.

» S. Liao, W. Cai, W. Liu, et al., "Satellite-to-ground quantum key distribution," Nature, vol. 549, pp. 43-47, 2017.

» S. Liao, W. Cai, J. Handsteiner, et al., "Satellite-Relayed Intercontinental Quantum Network," Physical Review Letters, vol. 120, 030501, 2018.

» T. Scheidl, J. Handsteiner, D. Rauch, R. Ursin, "Space-to-ground quantum key distribution," Proceedings vol. 11180, International Conference on Space Optics (ICSO) 2018, Chania, Greece.

» T. Jennewein, J. P. Bourgoin, B. Higgins, et al., "QEYSSAT: a mission proposal for a quantum receiver in space," Proc. SPIE 8997, Advances in Photonics of Quantum Computing, Memory, and Communication VII, 89970A, February 2014.

» E. Meyer-Scott, Z. Yan, A. MacDonald, et al., "How to implement decoy-state quantum key distribution for a satellite uplink with 50-dB channel loss," Physical Review A, vol. 84, 062326, December 2011.

» J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, et al., "A comprehensive design and performance analysis of low Earth orbit satellite quantum communication," New Journal of Physics, vol. 15, 023006, February 2013.

» J.-P. Bourgoin, N. Gigov, B. L. Higgins, et al., "Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations," Physical Review A, vol. 92, 052339, November 2015.

» H. Podmore, I. D'Souza, D. Hudson, et al., "Optical Terminal for Canada's Quantum Encryption and Science Satellite (QEYSSat)," IEEE International Conference on Space Optical Systems and Applications (ICSOS) 2019.

» M. Yang, F. Xu, J.-G. Ren, et al., "Spaceborne, low-noise, single-photon detection for satellite-based quantum communications," Optics Express, vol. 27, pp. 36114-36128, 2019.

» G. Vallone, D. Bacco, D. Dequal, et al., "Experimental Satellite Quantum Communications," Physical Review Letters, vol. 115, 040502, July 2015.

» D. Dequal, G. Vallone, D. Bacco, et al., "Experimental single-photon exchange along a space link of 7000 km," Physical Review A, vol. 93, 010301, January 2016.

» K. Günthner, I. Khan, D. Elser, et al., "Quantum-limited measurements of optical signals from a geostationary satellite," Optica, vol. 4, pp. 611-616, 2017.

» Y. A. Chen, Q. Zhang, T. Y. Chen, et al., "An integrated space-to-ground quantum communication network over 4,600 kilometres," Nature, vol. 589, pp. 214-219, 2021.

» T. Jennewein, C. Grant, E. Choi, et al., "The NanoQEY mission: ground to space quantum key and entanglement distribution using a nanosatellite," Proc. SPIE 9254, Emerging Technologies in Security and Defence II; and Quantum-Physics-based Information Security III, 925402, October 2014.

» D. K. L. Oi, A. Ling, J. A. Grieve, et al., "Nanosatellites for quantum science and technology," Contemporary Physics, pp. 25-52, 2016.

» R. Bedington, X. Bai, E. Truong-Cao, et al., "Nanosatellite experiments to enable future space-based QKD missions," EPJ Quantum Technology, vol. 3, article 12, 2016.

» D. K. L. Oi, A. Ling, G. Vallone, et al., "CubeSat quantum communications mission," EPJ Quantum Technology, vol. 4, article 6, 2017.

» H. Takenaka, A. Carrasco-Casado, M. Fujiwara, et al., "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite," Nature Photonics, vol. 11, pp. 502-508, 2017.

» K. Boone, J.-P. Bourgoin, E. Meyer-Scott, et al., "Entanglement over global distances via quantum repeaters with satellite links," Physical Review A, vol. 91, 052325, May 2015.

» Z. Tang, R. Chandrasekara, Y. C. Tan, et al., "Generation and Analysis of Correlated Pairs of Photons aboard a Nanosatellite," Physical Review Applied, vol. 5, 054022, May 2016.

» J. Yin, Y. Cao, Y.-H. Li, et al., "Satellite-based entanglement distribution over 1200 kilometers," Science, vol. 356, no. 6343, pp. 1140-1144, 2017.

» A. Villar, A. Lohrmann, X. Bai, et al., "Entanglement demonstration onboard a nano-satellite," Optica, vol. 7, no. 7, pp. 734-737, 2020.

» C.-Z. Peng, T. Yang, X.-H. Bao, et al., "Experimental Free-Space Distribution of Entangled Photon Pairs Over 13 km: Towards Satellite-Based Global Quantum Communication," Physical Review Letters, vol. 94, 150501, April 2005.

» R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, et al., "Entanglement-based quantum communication over 144 km," Nature Physics, vol. 3, pp. 481-486, 2007.

» X.-M. Jin, J.-G. Ren, B. Yang, et al., "Experimental free-space quantum teleportation," Nature Photonics, vol. 4, pp. 376-381, 2010.

» J. Yin, J.-G. Ren, H. Lu, et al., "Quantum teleportation and entanglement distribution over 100-kilometre free-space channels," Nature, vol. 488, pp. 185-188, 2012.

» Y. Cao, Y.-H. Li, K.-X. Yang, et al., "Long-Distance Free-Space Measurement-Device-Independent Quantum Key Distribution," Physical Review Letters, vol. 125, 260503, December 2020.

»