EPJ .org

○ EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH   **Open Access**

A reconfigurable entanglement distribution network suitable for connecting multiple ground nodes with a satellite

Stéphane Vinet[1*], Ramy Tannous[1,2] and Thomas Jennewein[1,3]

[*]Correspondence:
svinet@uwaterloo.ca
[1]Institute for Quantum Computing
and Department of Physics &
Astronomy, University of Waterloo,
200 University Ave W, Waterloo, N2L
3G1, Ontario, Canada
Full list of author information is
available at the end of the article

Abstract

Satellite-based quantum communication channels are important for ultra-long distances. Given the short duration of a satellite pass, it can be challenging to efficiently connect multiple users of a city-wide network while the satellite is passing over that area. We propose a network with dual-functionality: during a brief satellite pass, the ground network is configured as a multipoint-to-point topology where all ground nodes establish entanglement with a satellite receiver. During times when this satellite is not available, the satellite up-link is rerouted via a single optical switch to the ground nodes, and the network is configured as a pair-wise ground network. We numerically simulate a pulsed hyper-entangled photon source and study the performance of the proposed network configurations for quantum key distribution. We find favourable scaling in the case that the satellite receiver exploits time-multiplexing whereas the ground nodes utilize frequency-multiplexing. The scalability, simple reconfigurability, and easy integration with fibre networks make this architecture a promising candidate for quantum communication of many ground nodes and a satellite, an important step towards interconnection of ground nodes at a global scale.

Keywords: Quantum networks; Quantum communication; Quantum key distribution; Satellite-based quantum information
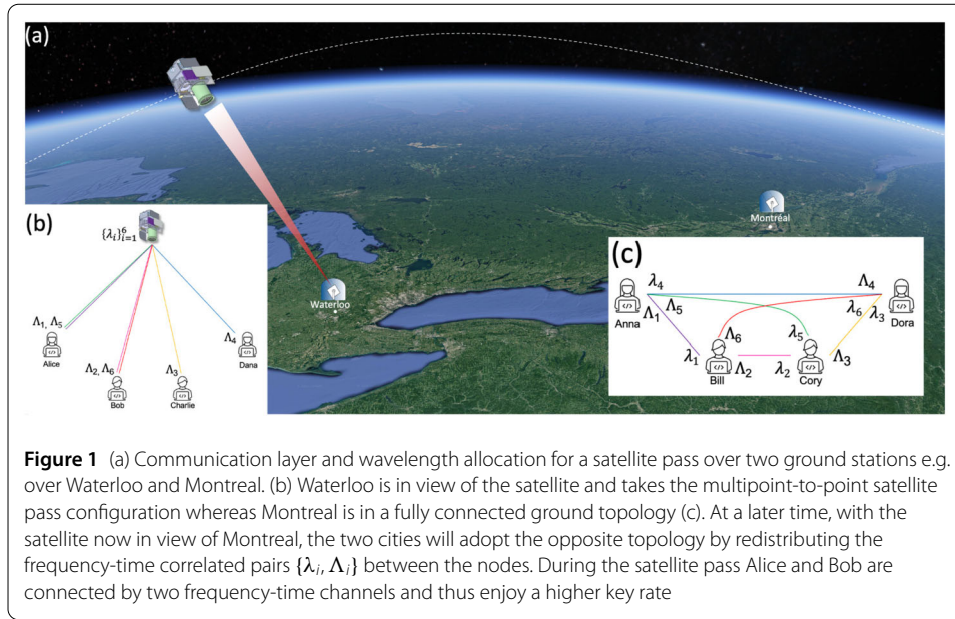
1 Introduction

A primary objective of quantum communication is the distribution of entanglement between distant parties [1]. This serves as the foundation for creating the quantum internet: a quantum network that enables revolutionary applications, including quantum key distribution (QKD) [2, 3], clock synchronization [4, 5], distributed quantum computing [6, 7], and long-baseline interferometry [8]. In recent years, significant research efforts have been done in expanding the scalability of quantum networks beyond two communicating parties. To this extent, multiple network architectures have been proposed, notably trusted-node networks which consist of a mesh of point-to-point links, where each node acts as a trusted relay to establish a complete two-party communication set-up [9–13]. While such a scheme is compatible with heterogeneous quantum links and can be used to increase

Springer

the communication distance arbitrarily, it comes with a significant security cost as one must ensure the privacy of every relay site. Alternatively, active switch quantum networks [14–18] allow for dynamically reconfigurable networks, yet are vulnerable to device failure. Furthermore, the distribution rate is limited by the switch's operating speed. Hence, an all-passive solution is preferred where all users can be connected simultaneously.

Two main approaches have previously been considered to create fully connected quantum networks relying either on high-dimensional entanglement or bi-partite entanglement and multiplexing [9, 19–24]. In the multipartite method, each user pair shares a different subspace of the overall network Hilbert space, which is used to generate their keys. However, adding or subtracting users from the network requires changing the dimensionality of the state produced by the source making this approach unscalable. On the other hand, multiplexing exploits the inherent hyper-correlations produced by the entangled photon source to deterministically separate correlated photon pairs to different users. This architecture eliminates the need to trust the service provider and is easily scalable as the number of users in the network can be modified without any change to the photon source. Nevertheless for an n-node network to be fully connected, $\mathcal{O}(n^2)$ multiplexed channels are required. Consequently, there remains an important hardware requirement as each channel requires a decoder and detector module to be fully distinguishable. Otherwise an increase in accidental counts will deteriorate the performance of the network as was shown in [9, 22]. Recently, [25–28] utilized beamsplitters in addition to multiplexing to increase the scalability of their network, but at the expense of the key generation rate. An interesting solution proposed by [9], is to use a pulsed source to recover the channel distinguishability despite limited detector resources. This implementation requires an additional gating signal to be sent to each user, and results in noise reduction by a factor equal to the gating duty cycle. However, this scheme is unsuitable for mobile nodes as the delays to every other node would need to be continuously compensated by each user thus restricting the reach of these quantum networks to metropolitan areas. Continued extensive research is being conducted on fibre-based quantum repeaters [29–31] and satellite-based quantum links [32–35] to enable the establishment of a global-scale network. While fibre-based links are limited in distance by exponential losses, the use of a free-space link to an orbiting satellite reduces the loss scaling from exponential to quadratic, consequently extending the reach of individual quantum links [36].
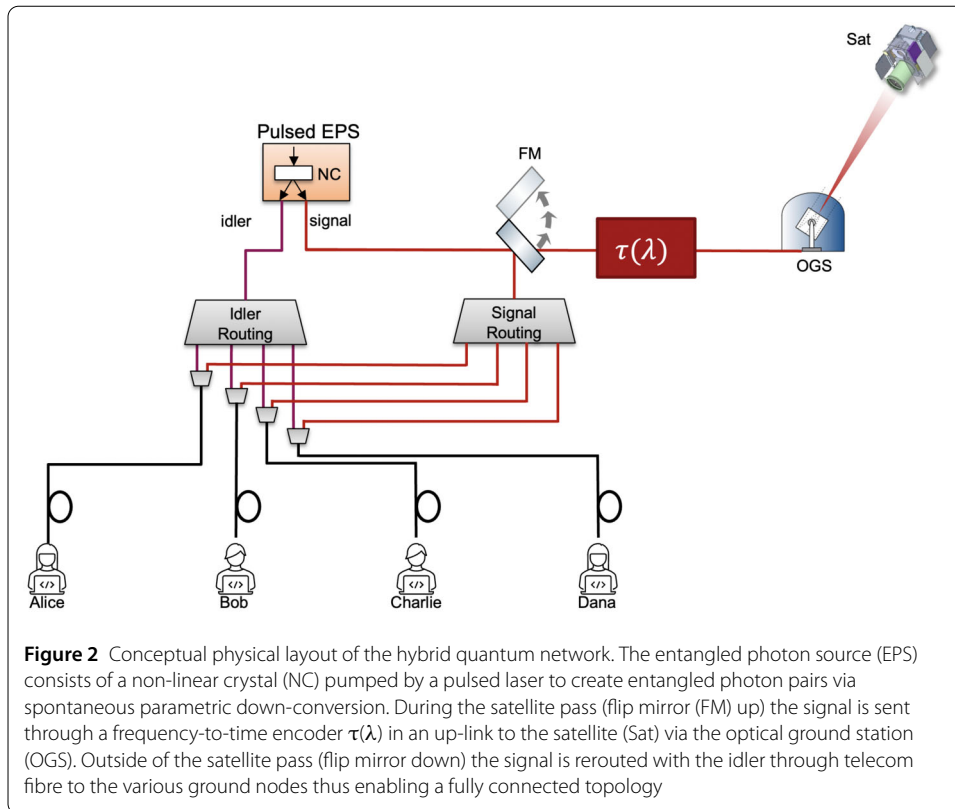
In this paper we present a scalable quantum network architecture that includes a mobile satellite node with minimal hardware requirements. To interface the fibre-optical network with the satellite link, we consider a pulsed non-degenerate entangled photon source in conjunction with a frequency-to-time mapping [37, 38]. Using a medium with a high group delay dispersion (GDD), one can carefully map the frequency distribution of pulsed light onto temporal modes such that each frequency channel obtains a distinct time delay within the resolution of the detector. The satellite node is then able to unambiguously separate the channels while using a single detector module. The rest of the paper is organized as follows. In Sect. 2, we introduce the reconfigurable quantum network architecture. In Sect. 3 we analyze the performance of the proposed network configuration and benchmark its potential by studying its use case for the Canadian QEYSSat quantum satellite mission [39]. A summary of our results and various extensions are given in Sect. 4.

Figure 1 (a) Communication layer and wavelength allocation for a satellite pass over two ground stations e.g. over Waterloo and Montreal. (b) Waterloo is in view of the satellite and takes the multipoint-to-point satellite pass configuration whereas Montreal is in a fully connected ground topology (c). At a later time, with the satellite now in view of Montreal, the two cities will adopt the opposite topology by redistributing the frequency-time correlated pairs $\{\lambda_i, \Lambda_i\}$ between the nodes. During the satellite pass Alice and Bob are connected by two frequency-time channels and thus enjoy a higher key rate

2 Method

The proposed network architecture is depicted in Fig. 1. It allows two reconfigurable quantum metropolitan-area networks (QMAN), for example in Waterloo and Montreal, Canada, to be connected by ground-to-satellite quantum links. As the satellite passes over Waterloo in Fig. 1b, the network adopts a multipoint-to-point topology from the N ground nodes to the satellite. Consequently allowing for a substantive increase of the key generation during the satellite pass via multiplexing. Meanwhile, the Montreal network in Fig. 1c is arranged into a pair-wise configuration where every user is connected to each other. As the satellite travels out of reach of Waterloo and within reach of Montreal, each network reconfigures itself into the opposite topology to optimize its functionality throughout the day. This rearrangement is enabled by the hybrid quantum network design in Fig. 2. For a satellite up-link, the idler is kept on the ground and distributed to the network users. During the satellite pass, the signal is sent through a frequency-to-time encoder $\tau(\lambda)$ to assign a time delay to each wavelength channel. This mapping can be accomplished by wavelength-dependent group delay dispersion e.g. in a chirped fibre Bragg grating [37, 40, 41] (CFBG) or by using a fibre Bragg grating (FBG) array with suitable spacing between each FBG to obtain the desired time delay [38]. Outside of the satellite pass, the flip mirror redirects the signal to the ground nodes.

The minimal duration of the channel time separation for the frequency-to-time mapping is determined by the timing jitter of the satellite single-photon detector and readout electronics which is typically on the order of ~ 130 ps full-width at half-maximum for Si-APDs [42–45]. Thus for a 80 MHz pump repetition rate, the satellite network configuration is limited to a maximum of ~ 95 frequency-time channels within the 12.5 ns pulse train. To ensure the channel distinguishability, the GDD must then be greater than ~ 325 ps/nm. Additionally, guard bands can be utilized to minimize cross-talk between the channels but at the expense of the achievable channel density [46]. For a given device length, the GDD and the CFBG's reflection bandwidth are inversely proportional: a larger dispersion requires higher reflectivities resulting in a narrower resonance and bandwidth

Figure 2 Conceptual physical layout of the hybrid quantum network. The entangled photon source (EPS) consists of a non-linear crystal (NC) pumped by a pulsed laser to create entangled photon pairs via spontaneous parametric down-conversion. During the satellite pass (flip mirror (FM) up) the signal is sent through a frequency-to-time encoder $\tau(\lambda)$ in an up-link to the satellite (Sat) via the optical ground station (OGS). Outside of the satellite pass (flip mirror down) the signal is rerouted with the idler through telecom fibre to the various ground nodes thus enabling a fully connected topology

[47, 48]. However, this limitation can be circumvented by using longer CFBGs or by using a CFBG array i.e. inscribing or splicing multiple CFBGs with adjacent reflection windows in succession [37].

While the number of channels depends on the entangled photon source's brightness and bandwidth, for simplicity we assume four nodes in each QMAN in Fig. 1. To create a fully connected N-user communication network, $\binom{N}{2}$ links are needed. Consequently, in the satellite configuration shown in Fig. 1b the six channels are distributed to the users such that Alice and Bob each receive two frequency-time channels and therefore attain an increased secure key rate. For the pair-wise fully connected topology in Fig. 1c, each node receives 3 wavelength channels to allow communication with every other node. The network connectivity and the wavelength allocation for the two different configurations: satellite (flip mirror up) and ground (flip-mirror down) are summarized in Table 1.

3 Performance estimation

We simulated the key rate for various quantum key distribution scenarios using the approaches introduced by Ma et al. [49] and Holloway et al. [50]. Our entangled state is constructed from the following spontaneous parametric down-conversion (SPDC) Hamiltonian:

$$H = i\chi(a_H^\dagger b_V^\dagger - a_V^\dagger b_H^\dagger) + \text{H.c.,} \tag{1}$$

where the subscripts H and V denote the horizontal and vertical polarizations, H.c. the Hermitian conjugate and χ is the squeezing parameter, a coupling constant proportional

Table 1 Proposed network connectivity and wavelength allocation. Wavelength correlated pairs are denoted as $\{\lambda_i, \Lambda_i\}$ for signal and idler respectively. The specific wavelengths considered in Figs. 5-6 are provided in parentheses with their associated ITU channel number

Network connection	Satellite configuration		Ground configuration	
	Signal	Idler	Signal	Idler
Alice-Satellite	λ_1, λ_5	Λ_1, Λ_5	–	–
Bob-Satellite	λ_2, λ_6	Λ_2, Λ_6	–	–
Charlie-Satellite	λ_3	Λ_3	–	–
Dana-Satellite	λ_4	Λ_4	–	–
Alice-Bob	–	–	λ_1 (786.75 nm)	Λ_1 (Ch40 = 1545.32 nm)
Bob-Charlie	–	–	λ_2 (787.03 nm)	Λ_2 (Ch41 = 1544.53 nm)
Charlie-Dana	–	–	λ_3 (787.32 nm)	Λ_3 (Ch42 = 1543.73 nm)
Alice-Dana	–	–	λ_4 (787.63 nm)	Λ_4 (Ch43 = 1542.14 nm)
Alice-Charlie	–	–	λ_5 (787.93 nm)	Λ_5 (Ch44 = 1542.14 nm)
Bob-Dana	–	–	λ_6 (788.24 nm)	Λ_6 (Ch45 = 1541.35 nm)

to the crystal nonlinearity and the amplitude of the pump beam [51]. Expectation values for the detector operators applied to the SPDC state are used in a squashing model to determine the two-fold coincidence rates and quantum bit error rate (QBER) [52, 53]. We analyze the performance of both bucket and photon-number resolving (PNR) detectors whose positive operator-valued measure (POVM) are respectively given by [54]:

$$\hat{E}^{(\text{click})} = \sum_{m=0}^{\infty}[1 - D(0)(1 - \eta)^m]|m\rangle\langle m|. \tag{2}$$

and

$$\hat{E}^{(n)} = \sum_{m=0}^{\infty}\sum_{k=0}^{n}D(k)\binom{n - k + m}{m}\eta^{n-k}(1 - \eta)^m|n + m - k\rangle\langle n + m - k|, \tag{3}$$

where η is the detector efficiency and $D(k)$ the dark count distribution. For the satellite pass configuration, we assume the satellite detector to be a Si-APD [55] with a detector dead time of 1 μs whereas we assume the ground detector to be an SNSPD with a dead time of 10 ns [56, 57].

Due to the dead time, the photon count rate is no longer linearly proportional to the impinging photon flux but is given by:

$$N_{count} = \frac{N_{ideal}}{1 + N_{ideal}T_D/T_{INT}}, \tag{4}$$

where T_D corresponds to the dead time, T_{INT} to the integration time, N_{ideal} to the number of photons impinging on the detector and N_{count} the number of resolved photons [58]. The secure key-rate (*SKR*) is then obtained via
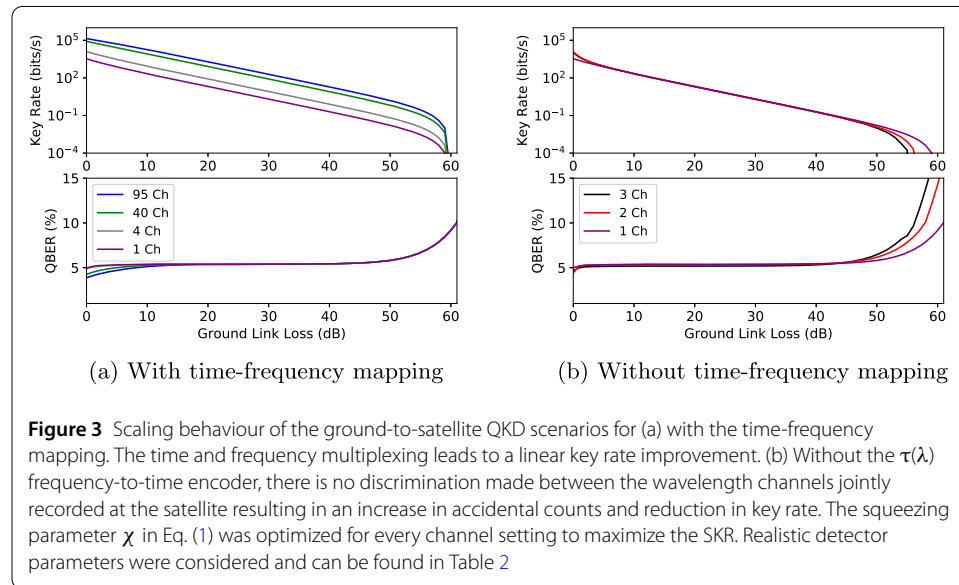
$$SKR = q\{Q_\lambda[1 - f(\delta_b)H_2(\delta_b) - H_2(\delta_p)]\} \tag{5}$$

where q is the basis reconciliation factor, the subscript λ denotes for one-half of the expected photon number μ, Q_λ is the overall gain, δ_b (δ_p) is the bit (phase) error rate, $f(x)$ is the bidirection error correction efficiency and $H_2(x)$ is the binary entropy function,

$$H_2(x) = -x\log_2(x) - (1 - x)\log_2(1 - x). \tag{6}$$

Table 2 Experimental assumptions for QKD modeling

Sat-APD dark count rate	1000 cps
Ground detector dark count rate	100 cps
Sat-APD timing jitter	130 ps
Sat-APD dead time	1 μs
Ground detector dead time	10 ns
coincidence time window	1 ns
Error correction factor	1.17
Satellite link loss	40 dB

(a) With time-frequency mapping   (b) Without time-frequency mapping

Figure 3 Scaling behaviour of the ground-to-satellite QKD scenarios for (a) with the time-frequency mapping. The time and frequency multiplexing leads to a linear key rate improvement. (b) Without the $\tau(\lambda)$ frequency-to-time encoder, there is no discrimination made between the wavelength channels jointly recorded at the satellite resulting in an increase in accidental counts and reduction in key rate. The squeezing parameter χ in Eq. (1) was optimized for every channel setting to maximize the SKR. Realistic detector parameters were considered and can be found in Table 2

A summary of the experimental parameters assumed throughout the simulation can be found in Table 2. At low ground link loss (< 10 dB) in Fig. 3a, detector saturation at the satellite node partially limits the scaling performance. However, in the higher loss regime one obtains a linear key rate increase whilst maintaining the same QBER. This scaling stems from the deterministic separation of the multiplexed channels resulting in independent communication channels with the same signal-to-noise ratio (see Appendix B) [9]. To achieve this deterministic scenario, the frequency-to-time mapping $\tau(\lambda)$ plays a crucial role. This is particularly apparent, in Fig. 3b where we only consider wavelength multiplexing. In other words, the idler photons are demultiplexed on the ground but the signal photons are recorded at the satellite detector without any channel discrimination. Surprisingly, demultiplexing solely the idler at the ground stations provides little advantage and in fact results in a maximal tolerable loss decrease compared to a single channel. This is due to an increase in accidental coincidences resulting in a loss of fidelity caused by detecting several channels on the single satellite detector [22]. Therefore, the signal-to-noise ratio decreases proportionally to the number of users added. Note that for every channel link setting, the squeezing parameter (χ) was numerically optimized to maximize the SKR. To compensate for the increase in accidental counts at higher loss, the photon pair production was decreased proportionally to the number of channels considered. At low loss, this one-sided multiplexing approach yields a slight key rate increase due to detector load management bypassing the dead time of the detector. Nonetheless, for realistic loss scenarios detector saturation has negligible significance. We investigate

Figure 4 Secure key rate performance comparison between PNR and Bucket detectors for the ground user nodes. The simulation parameters considered can be found in Table 2
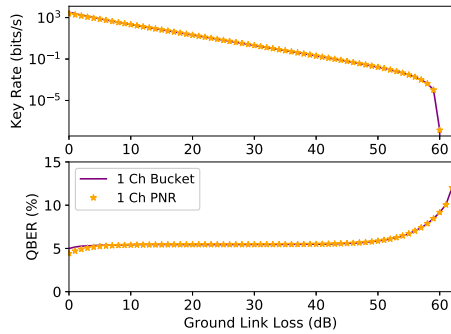
Table 3 Entangled photon source assumptions

Repetition rate	80 MHz
Pump central wavelength	521.4 nm
Pump bandwidth	2 nm
Signal central wavelength	787.5 nm
Signal bandwidth	15 nm
Idler central wavelength	1543.2 nm
Idler bandwidth	39 nm

in Fig. 4 the use of PNR detectors at the ground user nodes. Interestingly, we find that PNR detectors offer no significant key rate advantage compared to bucket detectors. This can be readily seen in the high loss regime from considering the series expansion of $\hat{E}^{(1)}$ for $D(1) \ll 1, \eta \to 0$ at which point one finds that $\hat{E}^{(1)} \to \hat{E}^{\text{(click)}}$. A detailed analysis of this phenomenon is in preparation [59].

3.1 QEYSSat mission

To further benchmark the potential of our network proposal, we analyze its performance for the QEYSSat mission use case. For this purpose, we assume the entangled photon source consists of a 15 mm long PPMgOLN waveguide pumped by a mode-locked pulsed laser centered at 521.4 nm with a bandwidth of 2 nm and a repetition rate of 80 MHz which produces polarization entangled photon pairs at 787.5 nm (signal) and 1543.2 nm (idler) via spontaneous parametric downconversion with respectively 15 nm and 39 nm of bandwidth. These assumptions on the entangled photon source are summarized in Table 3. The required wavelength channels for a hypothetical 4-node ground network and QEYSSat are illustrated in Fig. 5. The color coding is done in accordance with the channel allocation depicted in Fig. 1. The idler wavelength channels were chosen for compatibility with the standard International Telecommunication Union (ITU) 100 GHz grid. The corresponding correlated signal channel around 787.5 nm was selected for low-loss transmission through the atmosphere and compability with mature high-efficiency Si-APDs [36, 60]. Outside of the satellite pass, the 787.5 nm signal is rerouted to the ground users through standard telecom infrastructure. Whilst the telecom fibre is slightly multimode for the 787.5 nm light, Meyers-Scott et al. have shown that there is minimal crosstalk between the spatial modes over several kilometers resulting in a well-preserved polarization state and timing signature [61]. In spite of the greater fibre losses for the 787.5 nm light (~ 3 dB/km), the 32 km range shown in Fig. 6 is large enough to span a metropolitan area network. Furthermore, the range for the ground configuration could be expanded with a
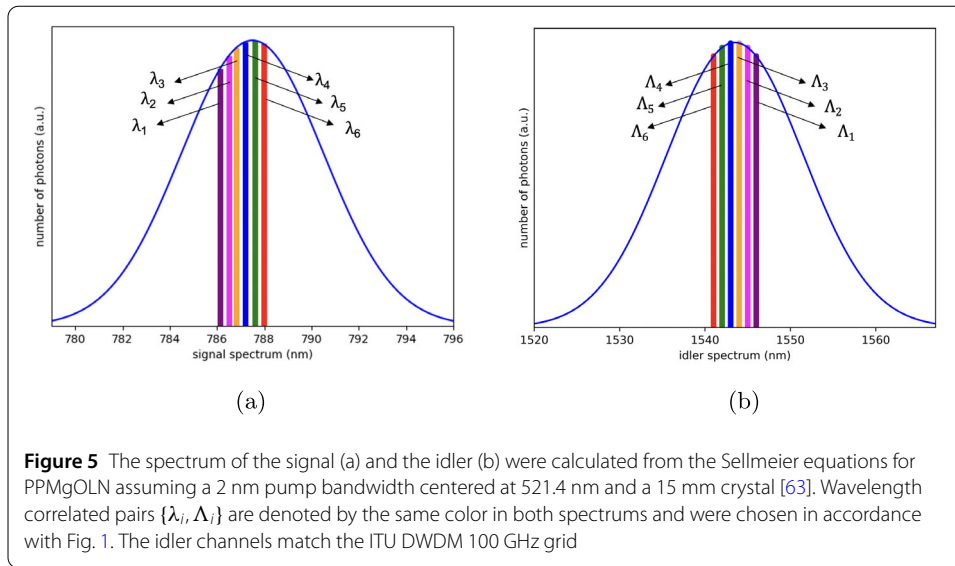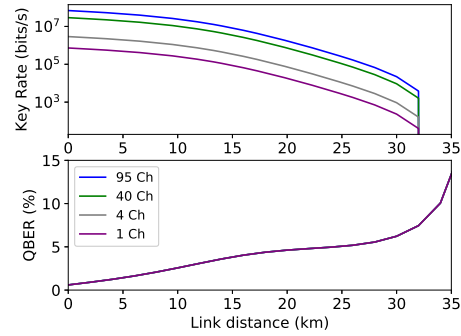
Figure 5 The spectrum of the signal (a) and the idler (b) were calculated from the Sellmeier equations for PPMgOLN assuming a 2 nm pump bandwidth centered at 521.4 nm and a 15 mm crystal [63]. Wavelength correlated pairs $\{\lambda_i, \Lambda_i\}$ are denoted by the same color in both spectrums and were chosen in accordance with Fig. 1. The idler channels match the ITU DWDM 100 GHz grid

Table 4 Generated key rate over a one-month period for both network configurations

User-to-user ground distance	16 km
Number of ground users in the network	14
User to OGS distance	16 km
Average number of passes	10
Average satellite pass duration	100 s
Average satellite link loss	40 dB
Total key generated per ground user pair	1.9×10^{11} **bits**
Total key generated between a ground node and satellite	4.1×10^{7} **bits**

telecom-band degenerate entangled photon source [25] or via quantum frequency conversion of the signal to telecom [62]. As the ground user nodes are not resource-limited, we can circumvent the detector timing limitation via frequency demultiplexing to extend the linear performance increase to the low-loss regime. Table 4 shows the estimated key produced per month between ground users (ground configuration), and between a satellite and ground users (satellite configuration). Assuming that over a one-month period, one would typically have around 10 satellite passes with a typical 100 seconds quantum link duration, we estimate the total key generated monthly in both configurations by a user located 16 kilometres equidistant from all other users in the network and the OGS. In the ground configuration, the 95 channels can connect up to 14 users with two preferred connections. The average key generated by a given user pair is then $\sim 1.9 \times 10^{11}$ bits. For the satellite configuration, the link loss will vary throughout the pass. Based off of the link loss data from [36], we compute a conservative estimate by assuming an upper quartile pass with 45 dB average link loss, which corresponds to a generated key of $\sim 4.1 \times 10^{7}$ bits. The proposed design presents a considerable scaling potential as the entire SPDC spectrum can be utilized. Assuming detector time resolutions as low as 35 ps [64], a 80 MHz repetition rate and an ultra-dense WDM (UDWDM) with 12.5 GHz spacing, one could employ up to ~ 350 channels. The number of available frequency-time channels could be further increased by reducing the pulse repetition rate but at the expense of the single channel key rate.

Figure 6 Scaling behaviour of the ground configuration (Fig. 1c) for the QEYSSat compatible scenario considered in Table 3 with the detector parameters given in Table 2

4 Conclusion

We proposed and analyzed an architecture suitable for serving both metropolitan networks or ground-satellite links, reconfigurable with minimal modifications. Our approach is uniquely designed to optimize the efficiency of satellite up-link scenarios such as QEYSSat, where the satellite receiver is only available for a few minutes every 24 hours. During the satellite pass, the secure key rate is improved through time and frequency multiplexing with no additional hardware requirements on the satellite. Additionally, the network's utility outside of the satellite pass is optimized by rerouting the signal to form a ground-based metropolitan network. The satellite can be exploited as a trusted node station to interconnect two metropolitan areas and extend the reach of quantum networks to a global scale. The scalability and simplicity render our network architecture a good candidate for commercial quantum communication networks.

Appendix A: Quantum key distribution simulation

The simulation code was written using the QuTIP toolbox in Python [50, 65]. We assume the protocol is symmetric with respect to the X and Z bases thus we find that $\delta_b = \delta_p$ and calculate the detection probabilities for the Z basis according to the squashing model below with the following parameters:

χ : squeezing parameter

loss_a: Efficiency of the ground quantum channel

loss_b: Efficiency of the satellite quantum channel

n_factor_a: Dark count rate in ground detectors

n_factor_b: Dark count rate in satellite detectors

dim: Fock space dimension

N: number of multiplexed channels

τ: Detector dead time

f_ec: error correction factor.

A.1 Squashing model

```
def measure_2folds_4modes_squashing_optimized(dim,chi,proj,proj2,
tau):
    vacc = basis(dim,0)
    det_exp = zeros((2,2,2,2))
    H_sq = 1j*\chi*(tensor(create(dim),create(dim))
    +tensor(destroy(dim),destroy(dim)))
```

```
    U_sq= H_sq.expm()
    spdc =U_sq*tensor(vacc,vacc)
    psi_i = tensor(spdc,spdc)
    out_i = reshape(transpose(reshape(psi_i.full(), (dim,dim,dim,-
1)),(0,3,2,1)),
    (dim*dim*dim*dim,-1))
    psi_i = Qobj(out_i,dims = [[dim, dim, dim, dim],
    [1, 1, 1, 1]])}
    for i in range(2):
        for j in range(2):
            for k in range(2):
                for l in range(2):
                    det_exp[i][j][k][l]} =
                    abs(expect(tensor(proj[i],proj[j],proj2[k],
                    proj2[l]),psi_i))
    HH=(det_exp[0][1][0][1]+0.5*(det_exp[0][0][0][1]
    +det_exp[0][1][0][0])
    +0.25*det_exp[0][0][0][0])/(1+ tau*(det_exp[0][1][0][1]
    +0.5*(det_exp[0][0][0][1]+det_exp[0][1][0][0])
    +0.25*det_exp[0][0][0][0]))
    VV=(det_exp[1][0][1][0]+0.5*(det\_exp[0][0][1][0]
    +det_exp[1][0][0][0])
    +0.25*det_exp[0][0][0][0])/(1+\tau*(det_exp[1][0][1][0]
    +0.5*(det_exp[0][0][1][0]+det_exp[1][0][0][0])
    +0.25*det_exp[0][0][0][0]))
    HV=(det_exp[0][1][1][0]+0.5*(det_exp[0][0][1][0]
    +det_exp[0][1][0][0])
    +0.25*det_exp[0][0][0][0])/( 1+\tau*(det_exp[0][1][1][0]
    +0.5*(det_exp[0][0][1][0]+det_exp[0][1][0][0])
    +0.25*det_exp[0][0][0][0]))
    VH=(det_exp[1][0][0][1]+0.5*(det_exp[0][0][0][1]
    +det_exp[1][0][0][0])
    +0.25*det_exp[0][0][0][0])/(1+ \tau*(det_exp[1][0][0][1]
    +0.5*(det_exp[0][0][0][1]+det_exp[1][0][0][0])
    +0.25*det_exp[0][0][0][0]))
return [HH,HV,VH,VV]
```

A.2 Secure key rate calculation

```
simqkdentanglement(chi,loss_a,loss_b,n_factor_a,n_factor_b,dim,N}):
    vacc= basis(N,0)
    qber_list=[]
    twofolds_list=[]
    for i in range(N):
        BucketDetector_realistic_detector(N,loss_a,n_factor_a)}
        b_det = BucketDetector_realistic_detector(N,loss_b,
        n_factor_b)}
        probs2f_i= measure_2folds_4modes_squashing_optimized(N,
        chi,a_det,b_det,tau)}
        twofolds_i=probs2f_i[0]+probs2f_i[1]+probs2f_i[2]
        +probs2f_i[3]
        twofolds_list.append(twofolds_i)}
        qber_i=(probs2f_i[0]+probs2f_i[3])
        qber_list.append(qber_i)}
        twofolds=sum(twofolds_list)}
```

```
        qber=sum(qber_list)/sum(twofolds_list)}
        if qber>0:
            H2=-qber*log2(qber) - (1-qber)*log2(1-qber)}
        else:
            H2 = 0
    f_e = f_ec + qber
    skr=-1.0*real(twofolds*0.5*(1-(1+f_e)*H2))
return [skr,qber,twofolds]
```

Appendix B: Hyper-entangled state

As shown in Pseiner et al. [22], due to energy conservation in the SPDC process, the frequency domain is also entangled. Consequently the output state is hyper-entangled:

$$|\Psi^-\rangle \approx \int \alpha(\omega_s, \omega_i)|\omega_s, \omega_i\rangle \otimes \frac{1}{\sqrt{2}}\bigg(|HV\rangle - |VH\rangle\bigg)d\omega_s d\omega_i,$$

where $\omega_s + \omega_i = \omega_p$ and $\alpha(\omega_s, \omega_i)$ is a continuous function characterizing the spectrum of the SPDC source. As the spontaneous parametric down-conversion produces well-defined correlations in discrete spectral regions, with proper filtering we can express the resulting state as

$$|\Psi^-\rangle_{MUX} \approx \Pi_{k=1}^N \otimes \frac{1}{\sqrt{2}}\bigg(|H_{\omega_k^s} V_{\omega_k^i}\rangle - |V_{\omega_k^s} H_{\omega_k^i}\rangle\bigg),$$

where N is the total number of frequency pairs contributing independently to the overall output.

Declarations

Author details
[1]Institute for Quantum Computing and Department of Physics & Astronomy, University of Waterloo, 200 University Ave W, Waterloo, N2L 3G1, Ontario, Canada. [2]Currently with the National Research Council of Canada, 100 Sussex Drive, Ottawa, K1A 0R6, Ontario, Canada. [3]Department of Physics, Simon Fraser University, 8888 University Dr W, Burnaby, V5A 1S6, British Columbia, Canada.

References

1. Wehner S, Elkouss D, Hanson R. Quantum Internet: a vision for the road ahead. Science. 2018;362(6412):9288. https://doi.org/10.1126/science.aam9288.
2. Bennett CH, Brassard G. Proceedings of the IEEE international conference on computers, systems and signal processing. Bangalore: IEEE; 1984.
3. Ekert AK. Quantum cryptography based on bell's theorem. Phys Rev Lett. 1991;67:661–3. https://doi.org/10.1103/PhysRevLett.67.661.
4. Kómár P, Kessler EM, Bishof M, Jiang L, Sørensen AS, Ye J, Lukin MD. A quantum network of clocks. Nat Phys. 2014;10(8):582–7. https://doi.org/10.1038/nphys3000.
5. Ilo-Okeke EO, Tessler L, Dowling JP, Byrnes T. Remote quantum clock synchronization without synchronized clocks. npj Quantum Inf. 2018;4(1):40. https://doi.org/10.1038/s41534-018-0090-2.
6. Broadbent A, Fitzsimons J, Kashefi E. Universal blind quantum computation. In: 2009 50th annual IEEE symposium on foundations of computer science. 2009. p. 517–26. https://doi.org/10.1109/FOCS.2009.36.
7. Nickerson NH, Fitzsimons JF, Benjamin SC. Freely scalable quantum technologies using cells of 5-to-50 qubits with very lossy and noisy photonic links. Phys Rev X. 2014;4:041041. https://doi.org/10.1103/PhysRevX.4.041041.
8. Gottesman D, Jennewein T, Croke S. Longer-baseline telescopes using quantum repeaters. Phys Rev Lett. 2012;109:070503. https://doi.org/10.1103/PhysRevLett.109.070503.
9. Wengerowsky S, Joshi SK, Steinlechner F, Hübel H, Ursin R. An entanglement-based wavelength-multiplexed quantum communication network. Nature. 2018;564(7735):225–8. https://doi.org/10.1038/s41586-018-0766-y.
10. Stucki D, Legré M, Buntschu F, Clausen B, Felber N, Gisin N, Henzen L, Junod P, Litzistorf G, Monbaron P, Monat L, Page J-B, Perroud D, Ribordy G, Rochas A, Robyr S, Tavares J, Thew R, Trinkler P, Ventura S, Voirol R, Walenta N, Zbinden H. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. New J Phys. 2011;13(12):123001. https://doi.org/10.1088/1367-2630/13/12/123001. arXiv:1203.4940 [quant-ph].
11. Sasaki M, Fujiwara M, Ishizuka H, Klaus W, Wakui K, Takeoka M, Miki S, Yamashita T, Wang Z, Tanaka A, Yoshino K, Nambu Y, Takahashi S, Tajima A, Tomita A, Domeki T, Hasegawa T, Sakai Y, Kobayashi H, Asai T, Shimizu K, Tokura T, Tsurumaru T, Matsui M, Honjo T, Tamaki K, Takesue H, Tokura Y, Dynes JF, Dixon AR, Sharpe AW, Yuan ZL, Shields AJ, Uchikoga S, Legré M, Robyr S, Trinkler P, Monat L, Page J-B, Ribordy G, Poppe A, Allacher A, Maurhart O, Länger T, Peev M, Zeilinger A. Field test of quantum key distribution in the Tokyo QKD network. Opt Express. 2011;19:10387. https://doi.org/10.1364/OE.19.010387. arXiv:1103.3566 [quant-ph].
12. Peev M, Pacher C, Alléaume R, Barreiro C, Bouda J, Boxleitner W, Debuisschert T, Diamanti E, Dianati M, Dynes JF, Fasel S, Fossier S, Fürst M, Gautier J-D, Gay O, Gisin N, Grangier P, Happe A, Hasani Y, Hentschel M, Hübel H, Humer G, Länger T, Legré M, Lieger R, Lodewyck J, Lorünser T, Lütkenhaus N, Marhold A, Matyus T, Maurhart O, Monat L, Nauerth S, Page J-B, Poppe A, Querasser E, Ribordy G, Robyr S, Salvail L, Sharpe AW, Shields AJ, Stucki D, Suda M, Tamas C, Themel T, Thew RT, Thoma Y, Treiber A, Trinkler P, Tualle-Brouri R, Vannel F, Walenta N, Weier H, Weinfurter H, Wimberger I, Yuan ZL, Zbinden H, Zeilinger A. The SECOQC quantum key distribution network in Vienna. New J Phys. 2009;11(7):075001. https://doi.org/10.1088/1367-2630/11/7/075001.
13. Xu F, Chen W, Wang S, Yin Z, Zhang Y, Liu Y, Zhou Z, Zhao Y, Li H, Liu D, Han Z, Guo G. Field experiment on a robust hierarchical metropolitan quantum cryptography network. Chin Sci Bull. 2009;54(17):2991–7. https://doi.org/10.1007/s11434-009-0526-3.
14. Toliver P, Runser RJ, Chapuran TE, Jackel JL, Banwell TC, Goodman MS, Hughes RJ, Peterson CG, Derkacs D, Nordholt JE, Mercer L, McNown S, Goldman A, Blake J. Experimental investigation of quantum key distribution through transparent optical switch elements. IEEE Photonics Technol Lett. 2003;15(11):1669–71. https://doi.org/10.1109/LPT.2003.818687.
15. Tang X, Ma L, Mink A, Nakassis A, Xu H, Hershman B, Bienfang J, Su D, Boisvert RF, Clark C, Williams C. Demonstration of an active quantum key distribution network. In: Meyers RE, Shih Y, Deacon KS, editors. Quantum communications and quantum imaging IV. International society for optics and photonics. vol. 6305. Bellingham: SPIE; 2006. p. 630506. https://doi.org/10.1117/12.679589.
16. Elliott C, Colvin A, Pearson D, Pikalo O, Schlafer J, Yeh H. Current status of the DARPA quantum network. In: Donkor EJ, Pirich AR, Brandt HE, editors. Quantum information and computation III. International society for optics and photonics. vol. 5815. Bellingham: SPIE; 2005. p. 138–49. https://doi.org/10.1117/12.606489.
17. Chen T-Y, Wang J, Liang H, Liu W-Y, Liu Y, Jiang X, Wang Y, Wan X, Cai W-Q, Ju L, Chen L-K, Wang L-J, Gao Y, Chen K, Peng C-Z, Chen Z-B, Pan J-W. Metropolitan all-pass and inter-city quantum communication network. Opt Express. 2010;18(26):27217–25. https://doi.org/10.1364/OE.18.027217.
18. Chen Y-A, Zhang Q, Chen T-Y, Cai W-Q, Liao S-K, Zhang J, Chen K, Yin J, Ren J-G, Chen Z, Han S-L, Yu Q, Liang K, Zhou F, Yuan X, Zhao M-S, Wang T-Y, Jiang X, Zhang L, Liu W-Y, Li Y, Shen Q, Cao Y, Lu C-Y, Shu R, Wang J-Y, Li L, Liu N-L, Xu F, Wang X-B, Peng C-Z, Pan J-W. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature. 2021;589(7841):214–9. https://doi.org/10.1038/s41586-020-03093-8.
19. Törmä P, Gheri KM. Establishing multi-party entanglement with entangled photons. In: Mysteries, puzzles, and paradoxes in quantum mechanics. American institute of physics conference series. vol. 461. 1999. p. 220–8. https://doi.org/10.1063/1.57855.
20. Aktas D, Fedrici B, Kaiser F, Lunghi T, Labonté L, Tanzilli S. Entanglement distribution over 150 km in wavelength division multiplexed channels for quantum cryptography. Laser Photonics Rev. 2016;10(3):451–7. https://doi.org/10.1002/lpor.201500258. arXiv:1601.02402 [quant-ph].
21. Lim HC, Yoshizawa A, Tsuchida H, Kikuchi K. Broadband source of telecom-band polarization-entangled photon-pairs for wavelength-multiplexed entanglement distribution. Opt Express. 2008;16(20):16052. https://doi.org/10.1364/OE.16.016052.
22. Pseiner J, Achatz L, Bulla L, Bohmann M, Ursin R. Experimental wavelength-multiplexed entanglement-based quantum cryptography. Quantum Sci Technol. 2021;6(3):035013. https://doi.org/10.1088/2058-9565/ac0519.
23. Ecker S, Pseiner J, Piris J, Bohmann M. Advances in entanglement-based QKD for space applications. In: Minoglou K, Karafolas N, Cugny B, editors. International conference on space optics - ICSO 2022. International society for optics and photonics. vol. 12777. Bellingham: SPIE; 2023. p. 1277727. https://doi.org/10.1117/12.2689972.

24. Kržič A, Sharma S, Spiess C, Chandrashekara U, Töpfer S, Sauer G, Campo LJ, Kopf T, Petscharnig S, Grafenauer T, Lieger R, Ömer B, Pacher C, Berlich R, Peschel T, Damm C, Risse S, Goy M, Rieländer D, Tünnermann A, Steinlechner F. Towards metropolitan free-space quantum networks. npj Quantum Inf. 2023;9(1):95. https://doi.org/10.1038/s41534-023-00754-0.

25. Joshi SK, Aktas D, Wengerowsky S, Lončarić M, Neumann SP, Liu B, Scheidl T, Lorenzo GC, Samec KL, Qiu A, Razavi M, Stipčević M, Rarity JG, Ursin R. A trusted node-free eight-user metropolitan quantum communication network. Sci Adv. 2020;6(36):0959. https://doi.org/10.1126/sciadv.aba0959.

26. Qi Z, Li Y, Huang Y, Feng J, Zheng Y, Chen X. A 15-user quantum secure direct communication network. Light: Sci Appl. 2021;10(1):183. https://doi.org/10.1038/s41377-021-00634-2.

27. Liu X, Liu J, Xue R, Wang H, Li H, Feng X, Liu F, Cui K, Wang Z, You L, Huang Y, Zhang W. 40-user fully connected entanglement-based quantum key distribution network without trusted node. PhotoniX. 2022;3(1):2. https://doi.org/10.1186/s43074-022-00048-2.

28. Liu D, Liu J, Ren X, Feng X, Liu F, Cui K, Huang Y, Zhang W. Photonic-reconfigurable entanglement distribution network based on silicon quantum photonics. Photon Res. 2023;11(7):1314–25. https://doi.org/10.1364/PRJ.489139.

29. Li Z-D, Zhang R, Yin X-F, Liu L-Z, Hu Y, Fang Y-Q, Fei Y-Y, Jiang X, Zhang J, Li L, Liu N-L, Xu F, Chen Y-A, Pan J-W. Experimental quantum repeater without quantum memory. Nat Photonics. 2019;13(9):644–8. https://doi.org/10.1038/s41566-019-0468-5. arXiv:1908.05351 [quant-ph].

30. Pu Y-F, Zhang S, Wu Y-K, Jiang N, Chang W, Li C, Duan L-M. Experimental demonstration of memory-enhanced scaling for entanglement connection of quantum repeater segments. Nat Photonics. 2021;15(5):374–8. https://doi.org/10.1038/s41566-021-00764-4. arXiv:2101.08541 [quant-ph].

31. Langenfeld S, Thomas P, Morin O, Rempe G. Quantum repeater node demonstrating unconditionally secure key distribution. Phys Rev Lett. 2021;126:230506. https://doi.org/10.1103/PhysRevLett.126.230506.

32. Liao S-K, Cai W-Q, Liu W-Y, Zhang L, Li Y, Ren J-G, Yin J, Shen Q, Cao Y, Li Z-P, Li F-Z, Chen X-W, Sun L-H, Jia J-J, Wu J-C, Jiang X-J, Wang J-F, Huang Y-M, Wang Q, Zhou Y-L, Deng L, Xi T, Ma L, Hu T, Zhang Q, Chen Y-A, Liu N-L, Wang X-B, Zhu Z-C, Lu C-Y, Shu R, Peng C-Z, Wang J-Y, Pan J-W. Satellite-to-ground quantum key distribution. Nature. 2017;549(7670):43–7. https://doi.org/10.1038/nature23655. arXiv:1707.00542 [quant-ph].

33. Yin J, Cao Y, Li Y-H, Ren J-G, Liao S-K, Zhang L, Cai W-Q, Liu W-Y, Li B, Dai H, Li M, Huang Y-M, Deng L, Li L, Zhang Q, Liu N-L, Chen Y-A, Lu C-Y, Shu R, Peng C-Z, Wang J-Y, Pan J-W. Satellite-to-ground entanglement-based quantum key distribution. Phys Rev Lett. 2017;119:200501. https://doi.org/10.1103/PhysRevLett.119.200501.

34. Liao S-K, Cai W-Q, Handsteiner J, Liu B, Yin J, Zhang L, Rauch D, Fink M, Ren J-G, Liu W-Y, Li Y, Shen Q, Cao Y, Li F-Z, Wang J-F, Huang Y-M, Deng L, Xi T, Ma L, Hu T, Li L, Liu N-L, Koidl F, Wang P, Chen Y-A, Wang X-B, Steindorfer M, Kirchner G, Lu C-Y, Shu R, Ursin R, Scheidl T, Peng C-Z, Wang J-Y, Zeilinger A, Pan J-W. Satellite-relayed intercontinental quantum network. Phys Rev Lett. 2018;120:030501. https://doi.org/10.1103/PhysRevLett.120.030501.

35. Yin J, Li Y-H, Liao S-K, Yang M, Cao Y, Zhang L, Ren J-G, Cai W-Q, Liu W-Y, Li S-L, Shu R, Huang Y-M, Deng L, Li L, Zhang Q, Liu N-L, Chen Y-A, Lu C-Y, Wang X-B, Xu F, Wang J-Y, Peng C-Z, Ekert AK, Pan J-W. Entanglement-based secure quantum cryptography over 1,120 kilometres. Nature. 2020;582(7813):501–5. https://doi.org/10.1038/s41586-020-2401-y.

36. Bourgoin J-P, Meyer-Scott E, Higgins BL, Helou B, Erven C, Hübel H, Kumar B, Hudson D, D'Souza I, Girard R, Laflamme R, Jennewein T. A comprehensive design and performance analysis of low Earth orbit satellite quantum communication. New J Phys. 2013;15(2):023006. https://doi.org/10.1088/1367-2630/15/2/023006.

37. Davis AOC, Saulnier PM, Karpiński M, Smith BJ. Pulsed single-photon spectrometer by frequency-to-time mapping using chirped fiber Bragg gratings. Opt Express. 2017;25(11):12804–11. https://doi.org/10.1364/OE.25.012804.

38. Lei M, Zou W, Li X, Chen J. Ultrafast fbg interrogator based on time-stretch method. IEEE Photonics Technol Lett. 2016;28(7):778–81. https://doi.org/10.1109/LPT.2015.2513903.

39. Scott A, Jennewein T, Cain J, D'Souza I, Higgins B, Hudson D, Podmore H, Soh W. The QEYSSAT mission: on-orbit demonstration of secure optical communications network technologies. In: Stein K, Gladysz S, editors. Environmental effects on light propagation and adaptive systems III. International society for optics and photonics. vol. 11532. Bellingham: SPIE; 2020. p. 115320. https://doi.org/10.1117/12.2574154.

40. Karpiński M, Davis AOC, Sośnicki F, Thiel V, Smith BJ. Control and measurement of quantum light pulses for quantum information science and technology. Adv Quantum Technol. 2021;4(9):2000150. https://doi.org/10.1002/qute.202000150.

41. Yang Y, Xiang X, Hou F, Quan R, Li B, Li W, Zhu N, Liu T, Zhang S, Dong R, Li M. Inherent resolution limit on nonlocal wavelength-to-time mapping with entangled photon pairs. Opt Express. 2020;28(5):7488–97. https://doi.org/10.1364/OE.387146.

42. Gulinatti A, Maccagnani P, Rech I, Ghioni M, Cova S. 35 ps time resolution at room temperature with large area single photon avalanche diodes. Electron Lett. 2005;41:272–2742.

43. Gersbach M, Richardson J, Mazaleyrat E, Hardillier S, Niclass C, Henderson R, Grant L, Charbon E. A low-noise single-photon detector implemented in a 130 nm cmos imaging process. Solid-State Electron. 2009;53(7):803–8. https://doi.org/10.1016/j.sse.2009.02.014.

44. Pancheri L, Stoppa D. Low-noise single photon avalanche diodes in 0.15 um cmos technology. In: 2011 proceedings of the European solid-state device research conference (ESSDERC). 2011. p. 179–82. https://doi.org/10.1109/ESSDERC.2011.6044205.

45. Niclass C, Gersbach M, Henderson R, Grant L, Charbon E. A single photon avalanche diode implemented in 130-nm cmos technology. IEEE J Sel Top Quantum Electron. 2007;13(4):863–9. https://doi.org/10.1109/JSTQE.2007.903854.

46. Shaw G, Sridharan S, Ranu S, Shingala F, Mandayam P, Prabhakar A. Time-bin superposition methods for DPS-QKD. IEEE Photonics J. 2022;14(5):1–7. https://doi.org/10.1109/JPHOT.2022.3204920.

47. Azana J, Muriel MA. Real-time optical spectrum analysis based on the time-space duality in chirped fiber gratings. IEEE J Quantum Electron. 2000;36(5):517–26. https://doi.org/10.1109/3.842092.

48. Ouellette F, Cliche J-F, Gagnon S. All-fiber devices for chromatic dispersion compensation based on chirped distributed resonant coupling. J Lightwave Technol. 1994;12(10):1728–38. https://doi.org/10.1109/50.337484.

49. Ma X, Fung C-HF, Lo H-K. Quantum key distribution with entangled photon sources. Phys Rev A. 2007;76:012307. https://doi.org/10.1103/PhysRevA.76.012307.

50. Holloway C, Doucette JA, Erven C, Bourgoin J-P, Jennewein T. Optimal pair-generation rate for entanglement-based quantum key distribution. Phys Rev A. 2013;87:022342. https://doi.org/10.1103/PhysRevA.87.022342.
51. Thomas Jennewein MB, White AG. Single-photon device requirements for operating linear optics quantum computing outside the post-selection basis. J Mod Opt. 2011;58(3–4):276–87. https://doi.org/10.1080/09500340.2010.546894.
52. Lütkenhaus N. Estimates for practical quantum cryptography. Phys Rev A. 1999;59:3301–19. https://doi.org/10.1103/PhysRevA.59.3301.
53. Moroder T, Gühne O, Beaudry N, Piani M, Lütkenhaus N. Entanglement verification with realistic measurement devices via squashing operations. Phys Rev A. 2010;81:052342. https://doi.org/10.1103/PhysRevA.81.052342.
54. Kok P, Lovett BW. Introduction to optical quantum information processing. Cambridge: Cambridge University Press; 2010. https://doi.org/10.1017/CBO9781139193658.
55. Pugh CJ, Kaiser S, Bourgoin J-P, Jin J, Sultana N, Agne S, Anisimova E, Makarov V, Choi E, Higgins BL, Jennewein T. Airborne demonstration of a quantum key distribution receiver payload. Quantum Sci Technol. 2017;2(2):024009. https://doi.org/10.1088/2058-9565/aa701f.
56. Migdall A, Polyakov SV, Fan J, Bienfang JC. Single-photon generation and detection. In: Single-photon generation and detection. Experimental methods in the physical sciences. vol. 45. San Diego: Academic Press; 2013. https://doi.org/10.1016/B978-0-12-387695-9.00017-2.
57. Eisaman MD, Fan J, Migdall A, Polyakov SV. Invited review article: single-photon sources and detectors. Rev Sci Instrum. 2011;82(7):071101. https://doi.org/10.1063/1.3610677.
58. Severini F, Cusini I, Berretta D, Pasquinelli K, Incoronato A, Villa F. Spad pixel with sub-ns dead-time for high-count rate applications. IEEE J Sel Top Quantum Electron. 2022;28:1–8. https://doi.org/10.1109/JSTQE.2021.3124825.
59. Vinet S, Jennewein T. Photon-number resolving detectors for quantum key distribution. In preparation.
60. ID120 Visible Single-Photon Detector. Accessed: 2023-12-01.
61. Meyer-Scott E, Hübel H, Fedrizzi A, Erven C, Weihs G, Jennewein T. Quantum entanglement distribution with 810 nm photons through telecom fibers. Appl Phys Lett. 2010;97(3):031117. https://doi.org/10.1063/1.3460920.
62. Raymer MG, Srinivasan K. Manipulating the color and shape of single photons. Phys Today. 2012;65(11):32–7. https://doi.org/10.1063/PT.3.1786.
63. Gayer O, Sacks Z, Galun E, Arie A. Temperature and wavelength dependent refractive index equations for MgO-doped congruent and stoichiometric LiNbO3. Appl Phys B. 2008;91(2):343–8. https://doi.org/10.1007/s00340-008-2998-2.
64. Gulinatti A, Maccagnani P, Rech I, Ghioni M, Cova S. 35 ps time resolution at room temperature with large area single photon avalanche diodes. Electron Lett. 2005;41:272–4.
65. Johansson JR, Nation PD, Nori F. Qutip: an open-source python framework for the dynamics of open quantum systems. Comput Phys Commun. 2012;183(8):1760–72. https://doi.org/10.1016/j.cpc.2012.02.021.
66. Vinet S, Tannous R, Jennewein T. Quantum key distribution simulation. 2024. https://github.com/stephanevinet-q/HTSN.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.