Neumann et al. *EPJ Quantum Technology* (2018) 5:4
https://doi.org/10.1140/epjqt/s40507-018-0068-1

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Q^{3}Sat: quantum communications uplink to a 3U CubeSat—feasibility & design

Sebastian Philipp Neumann[1,2†], Siddarth Koduru Joshi[1,2†], Matthias Fink[1,2], Thomas Scheidl[1,2], Roland Blach[1], Carsten Scharlemann[3], Sameh Abouagaga[3], Daanish Bambery[3], Erik Kerstel[4], Mathieu Barthelemy[4] and Rupert Ursin[1,2*]

*Correspondence:
rupert.ursin@oeaw.ac.at
[1]Institute for Quantum Optics and Quantum Information Vienna, Vienna, Austria
[2]Vienna Center for Quantum Science and Technology, Vienna, Austria
Full list of author information is available at the end of the article
[†]Equal contributors

Abstract

Satellites are the most efficient way to achieve global scale quantum communication (Q.Com) because unavoidable losses restrict fiber based Q.Com to a few hundred kilometers. We demonstrate the feasibility of establishing a Q.Com uplink with a 3U CubeSat, measuring only 10 × 10 × 34 cm^3, using commercial off-the-shelf components, the majority of which have space heritage. We demonstrate how to leverage the latest advancements in nano-satellite body-pointing to show that our 4 kg CubeSat can generate a quantum-secure key, which has so far only been shown by a much larger 600 kg satellite mission. A comprehensive link budget and simulation was performed to calculate the secure key rates. We discuss design choices and trade-offs to maximize the key rate while minimizing the cost and development needed. Our detailed design and feasibility study can be readily used as a template for global scale Q.Com.

Keywords: Quantum communication; CubeSat; Quantum Key Distribution; Feasibility study; Satellite technology; Quantum optics

1 Introduction

The security of quantum communication (Q.Com) is based on fundamental and immutable laws of physics and not on the assumption that a problem is and always will be too difficult for an adversary to solve. Naturally, this unconditionally secure communication technology has a large impact on global communications. Attempts to overcome the limits imposed by losses, such as Ref. [1], and attempts to create a global satellite based network, are underway [2, 3]. The latter are large and complex satellites which can cost upwards of 100 M€ each. Small CubeSats however can be constructed and launched for 0.5 to 10 M€. We present a simple, small, light-weight and low power-consuming satellite system capable of Q.Com. To achieve this, we considered several possible designs and individual components. The CubeSat performance was evaluated in each instance and design choices were made to minimize the Size, Weight and Power consumption (SWaP). This was done iteratively to create a commercially viable satellite system capable of Q.Com. Our CubeSat mission is called Q^{3}Sat (pronounced Q-CubeSat). Previous long distance implementations via optical fiber such as Ref. [4] and free space terrestrial links like Ref. [5] have approached the limits of terrestrial Q.com in terms of distance. The successful 600 kg class

[2] and 50 kg class [6] large satellites have shown that Q.com in space is feasible. By analyzing the results of these proof-of-concept missions and evaluating their performance in both the uplink and the downlink scenario, we find that a downlink scenario offers a larger key rate. In an uplink, only a relatively simple polarization analysis module needs to be on board the satellite and ultra bright state-of-the-art quantum source(s) can be used on ground. Thus, an uplink is more suitable for a low cost CubeSat mission. Additionally, an uplink allows for a larger variety of implementable Q.Com protocols. This is because many different Q.Com protocols (e.g., E91 [7], BB84 [8], decoy state protocol (DSP) [9], BBM [10], B92 [11]) rely on nearly identical detection schemes for the receiver and can thus all be implemented on our CubeSat. Changes would only have to be made to the easily accessible ground module. Previous studies such as Refs. [12–16] have shown that space-based Q.Com is in principle feasible (also with small satellites) and culminated in two successful Q.Com satellites as well as other quantum experiments in space [17]. Recent efforts have evaluated the feasibility of downlinks [18] while others have attempted to solve the technological challenges identified by space-certifying detectors and sources of entanglement [19]. However, no previous works have evaluated the feasibility of Q.Com uplinks to satellites as small as a 3U CubeSat.

The CubeSat design considered here will also be able to perform tasks beyond Q.Com, e.g. measuring light pollution stemming from ground with a narrow field of view (FoV) to establish a global map in unprecedented resolution at single-photon level. This is crucial to finding dark areas near potential Q.Com customers and for other, more general applications. Additionally, the timing resolution of the single photon detectors enables pulse-position-modulation in classical communication from ground to space with exceptionally fast data rates. The extremely sensitive single photon detectors can also be re-purposed for other terrestrial and astronomical observations requiring an exceptional cadence and narrow FoV. In this manuscript we nevertheless focus on Q.Com, since this objective drives the design for the satellite infrastructure.

1.1 Quantum communication protocols

Let us consider the two most common Q.Com protocols—E91 [7] and the decoy state protocol (DSP) [9] which are explained in detail in Refs. [20, 21]. In both, information is encoded in the polarization state of single photons at the ground station (Alice) which then sends these states to the satellite (Bob). Bob measures the polarization of the received photons in a set of randomly chosen bases. The protocol is divided into several individual "trials". In each trial, one state is sent and received. The techniques used to identify each trial depend on experimental implementation and protocol. To ensure that the key is secure, Alice and Bob perform statistical tests (i.e., compute the Quantum Bit Error Rate (QBER E) [22] and/or perform a Bell test) on the data they measured from several trials. Thus, they also need a form of (insecure but authenticated) classical communication. To obtain the key, Alice and Bob need various post-processing (PP) steps (detailed in [23]) that vary between protocols.[a] Importantly, the larger the measured QBER, the more information an eavesdropper (Eve) could, in principle, obtain about the raw key. This means that privacy amplification must use up more raw key bits to reach the same level of security, reducing the total number of secure key bits. Thus, the amount of key that can be exchanged per second strongly depends on the QBER.[b]

The key difference between the two protocols is that E91 exploits quantum entanglement of photons to obtain mutually shared randomness (the key) between the two parties.

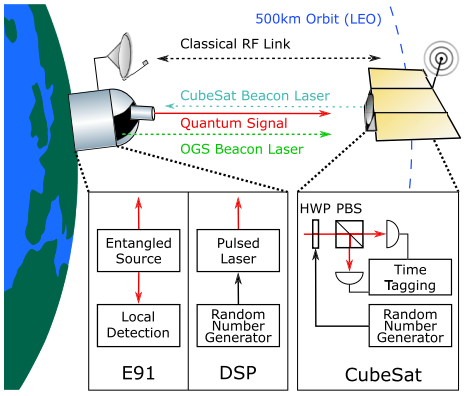

Figure 1 The optical ground station (OGS) is connected either to one arm of a source of polarization entangled photon pairs (E91) or to a pulsed laser with randomly chosen polarization and mean photon number for each pulse (DSP). The signal photons are transmitted to the CubeSat in a 500 km low-earth orbit (LEO) via a free-space link. OGS and CubeSat point beacon lasers at each other for precise attitude control. The quantum signal is analyzed on board the CubeSat using a randomly switched half-wave plate (HWP) and a polarizing beam splitter (PBS). Measurement outcome, basis choice and time tag of each event are recorded. Information about the latter two is transmitted to the OGS using a classical radio frequency (RF) link. The OGS identifies the matching bits using a cross-correlation analysis ($g^{(2)}$) and tells the CubeSat which ones to use. Both disregard the other bits, perform post-processing and then share a secret key.

In DSP however, Alice encodes information by randomly choosing the polarization of an emitted weak coherent pulse. Alice must also randomly choose the average intensity of each pulse (to designate it as a signal or decoy pulse) to be able to detect a possible photon number splitting attack. Thus each protocol needs a different source on ground as seen in Fig. 1 (such as Ref. [26] for E91 and Ref. [27] for DSP).

2 Error budget

The security proofs for both E91 and DSP show that a secure key can be exchanged only if the QBER E is below a certain value. For E91, the overall limit E_{E91}^{max} is 11.0% [28], assuming optimal classical PP with error correction efficiency $f = 1$. Realistic PP techniques limit E_{E91}^{max} to 10.2%, assuming a PP efficiency of $f = 1.1$ [29]. For DSP with the same f and assuming the values from Table 1, the limit E_{DSP}^{max} is about 6.2%.[c] These security requirements can be reformulated in terms of the more familiar Signal to Noise Ratio (SNR) as

$$SNR = \frac{1}{E} - 1. \tag{1}$$

For unconditional security, any and all noise must be attributed to Eve. This requires a minimum SNR for E91 (DSP) of 8.8 (15.1) for realistic PP with $f = 1.1$. Nevertheless, we shall continue using E (instead of the SNR) to be compatible with existing literature. Based on the formulas devised in Ref. [30], the QBER for the E91 protocol can be written as

$$E_{E91} = e_0 - \frac{1}{Q_{E91}} \times \left[\frac{(e_0 - e_d)\Lambda_A \Lambda_B \mu_{E91}(1 + \frac{\mu_{E91}}{2})}{(1 + \Lambda_A \frac{\mu_{E91}}{2})(1 + \Lambda_B \frac{\mu_{E91}}{2})(1 + \Lambda_A \frac{\mu_{E91}}{2} + \Lambda_B \frac{\mu_{E91}}{2} - \Lambda_A \Lambda_B \frac{\mu_{E91}}{2})} \right], \tag{2}$$

where

$$Q_{E91} = 1 - \frac{1}{(1 + \Lambda_A \frac{\mu_{E91}}{2})^2} - \frac{1 - Y_{0B}}{(1 + \Lambda_B \frac{\mu_{E91}}{2})^2} + \frac{1 - Y_{0B}}{(1 + \Lambda_A \frac{\mu_{E91}}{2} + \Lambda_B \frac{\mu_{E91}}{2} - \Lambda_A \Lambda_B \frac{\mu_{E91}}{2})^2}, \tag{3}$$

Table 1 List of parameters and values for which we assigned fixed values. Justification of these values is given in Sect. 3

Symbol	Parameter	Value
d_B	Diameter of active detector area on CubeSat	20 μm
D_A	OGS telescope diameter	30 cm
D_B	CubeSat telescope diameter	10 cm
e_0	Probability of noise count to be correct	50%
e_d	Probability of erroneous detection	2%
$E_{E91/DSP}^{max}$	Maximum tolerable QBER for E91/DSP	10.2% /6.2%
η_A	OGS multiplexed SNSPD efficiency (E91 only)	70% (–1.5 dB)
η_B	CubeSat detector efficiency	15% (–8.2 dB)
f	Error correction protocol efficiency	1.1
f_B	Effective focal length CubeSat telescope	40 cm
f_{SYN}	Repetition rate of OGS's beacon laser	10 MHz
FoV	Field of view CubeSat (full angle)	50 μrad
λ	Signal photon wavelength	810 nm
Λ	Total loss	–62.7 dB (max)
Λ_A	Total loss OGS arm (source to detector) (E91 only)	60% (–2.3 dB)
Λ_H	Heralding efficiency (E91 only)	85% (–0.7 dB)
Λ_{TA}	OGS telescope loss (only E91)	–1.0 dB
Λ_{TB}	CubeSat telescope loss	–1.5 dB
Λ_{OB}	CubeSat optical elements loss	–1.0 dB
Λ_{PB}	CubeSat pointing loss	–2.5 dB
Λ_{SB}	CubeSat basis switch loss	–0.5 dB
Λ_{SYN}	Loss due to errors in clock sync.	–0.5 dB
μ_{DSP}	Mean photon number per signal pulse (DSP only)	0.64
μ_{E91}	Mean photon number per coincidence window (E91 only)	0.01
r_0	Fried parameter	5 cm–40 cm
R_A	OGS count rate (E91 only)	60 Mcps
R_B	CubeSat count rate (including noise)	3 kcps (max)
R_B^{max}	CubeSat detectors' maximum count rate	100 kHz
R_{BG}	CubeSat background counts (total)	80–180 cps
R_{DC}	CubeSat dark count rate (per detector)	200 cps
R_{B+D}	CubeSat total noise counts	480–580 cps
R_{DSP}^P	Effective signal photon rate (DSP only)	315 Mcps
R_{E91}^P	Pair rate of entangled photon source (E91 only)	100 Mcps
R_{rep}	Repetition rate of single photon source (DSP only)	1 GHz
σ_A	OGS pointing precision (rms, full angle)	2.4 μrad
σ_B	CubeSat pointing precision (rms, full angle)	40 μrad
t_A	Combined OGS detectors + time tagging jitter	16 ps
t_B	CubeSat detector + time tagging jitter	37 ps
τ	Coincidence window	80 ps
t_{SB}	CubeSat basis switching time	100 μs
t_{TT}	Time tagging resolution (on board CubeSat)	10 ps
t_{MD}	Measurement duration of each chunk for clock sync.	100 ms
t_{QC}	Maximum duration of quantum connection per pass	220 s

is the gain (or the probability of coincident photon detection per trial), Λ_A (Λ_B) is the total transmission efficiency of the channel to Alice on ground (to Bob on the satellite), e_0 denotes the probability of a dark count to yield an error and e_d is the probability of a photon being detected in the wrong detector. The average photon number per trial is $\mu_{E91} = R_{E91}^P \tau$ (where R_{E91}^P is the E91 source's pair production rate and τ is the coincidence time window). The dark count yield (or probability that a dark count occurs per trial) at the satellite is defined as $Y_{0B} = R_{B+D} \cdot \tau$ (where R_{B+D} is the total rate of noise counts on the CubeSat). The effect of even several thousand noise counts on the ground based detectors is negligibly small compared to expected single count rates of $\approx 10^7$ cps, thus we neglect the probability of a noise count occurring at Alice ($Y_{0A} \approx 0$). The secure key rate (i.e., bits

per second) R^S_{E91}[d] follows directly from these quantities:

$$R^S_{E91} \geq \frac{1}{2}\frac{Q_{E91}}{\tau}\left[1-(1+f)H_2(\overline{E_{E91}})\right], \tag{4}$$

where the factor $\frac{1}{2}$ is due to the fact that only half of all basis choices are compatible, $H_2(x)$ is the binary Shannon entropy

$$H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x), \tag{5}$$

and $\overline{E_{E91}}$ is the QBER averaged over one measurement run where start and stop of the measurement have been chosen such that the temporal integral of R^S_{E91} over one connection is maximized. Actual protocols might require a subdivision of the raw key into chunks with different QBER, however we use the average as a good approximation to many varying approaches. These quantities can analogously be defined for DSP, this time following Ref. [9]. The total QBER E_{DSP} is given by

$$E_{DSP} = \frac{e_d(1-e^{-\mu_{DSP}\cdot\Lambda_B}) + e_0 Y_{0B}}{Q_{DSP}}, \tag{6}$$

with the total gain Q_{DSP} given by

$$Q_{DSP} = 1 - e^{-\mu_{DSP}\cdot\Lambda_B} + Y_{0B}. \tag{7}$$

We choose the mean photon number per trial (or signal pulse) $\mu_{DSP} = 0.64$ in order to maximize the secure key rate R^S_{DSP}. Unlike μ_{E91}, the mean photon number per pulse in DSP, μ_{DSP}, can in practice be tuned more easily, since the pulses originate directly from a (strongly attenuated) pulsed laser and not from inefficient spontaneous parametric down-conversion (SPDC) taking place in a nonlinear crystal. We define the true single-photon pulse QBER E^1_{DSP} and gain Q^1_{DSP} according to Ref. [9]:

$$\begin{aligned} E^1_{DSP} &= \frac{e_d\Lambda_B + e_0 Y_{0B}}{\Lambda_B + Y_{0B}}, \\ Q^1_{DSP} &= (\Lambda_B + Y_{0B})\mu_{DSP}e^{-\mu_{DSP}} \end{aligned} \tag{8}$$

and thus we can calculate the secure key rate as

$$R^S_{DSP} \geq \frac{1}{4}R_{rep}\mu_{DSP}\left[Q^1_{DSP}\left(1-H_2\left(\overline{E^1_{DSP}}\right)\right) - fQ_{DSP}H_2(\overline{E_{DSP}})\right], \tag{9}$$

where the factor $\frac{1}{4}$ is due to the fact that only half of the photons are measured in the right basis and another half are decoy states which will not be considered for the key [31]. R_{rep} is the repetition rate of the DSP source. Analogous to Eq. 4, $\overline{E^1_{DSP}}$ and $\overline{E_{DSP}}$ denote the QBERs averaged over one measurement run. Using the realistic values shown in Table 1, we can calculate the amount of loss each protocol can tolerate. The total link transmission to the satellite, Λ_B, for E91 (DSP) must be better than −62.7 dB (−61.2 dB) in order to obtain a secure key, i.e. achieve a SNR of more than 8.8 (15.1). Accounting for losses in the apparatus of Alice and Bob, the required minimum link transmission Λ_L from sending lens to receiving lens alone is −43.6 dB (−42.2 dB) for E91 (DSP).

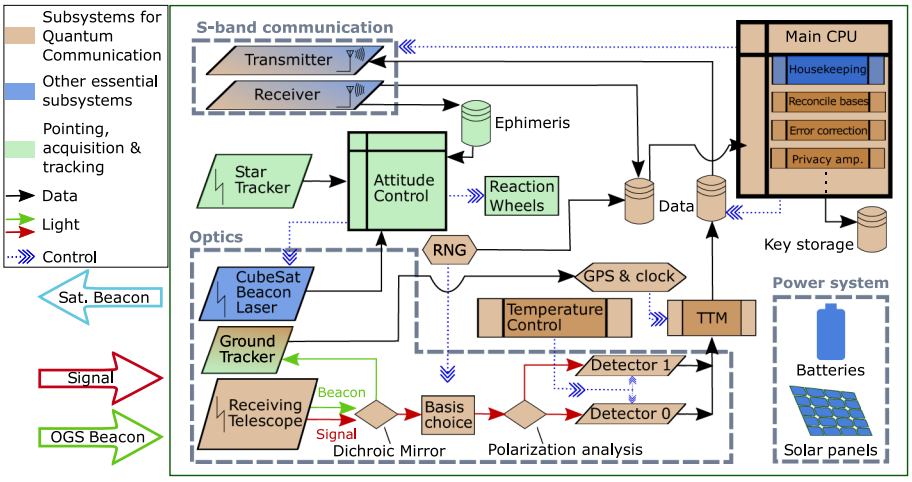

Figure 2 Block diagram of the 3U CubeSat. Components in brown are those used for quantum communication while those in green relate to the pointing, acquisition and tracking system. Other essential subsystems are blue. The subsystems can also be classified based on the type of components used as indicated by the grey dashed lines. All components are fixed to the CubeSat frame, communicate with the main CPU and supply/draw power to/from the CubeSat bus (all of which are not shown). TTM: Time Tagging Module, RNG: Random Number Generator.

3 Preliminary design

The advantage of the uplink scenario is that most of the mission's complexity is ground-based and multiple protocols/experiments can be implemented without making changes to the CubeSat. Consequently we first discuss the design of the OGS (Sect. 3.1) and then that of the CubeSat (Sect. 3.2). Figure 1 shows an overview of the experiment consisting of space and ground segments. Table 1 provides reasonable reference values for the specifications and performance of all components as used below. Figure 2 shows a block diagram of all payload components necessary for the Q.Com mission.

3.1 The ground segment

To implement different Q.Com protocols, different photon sources have to be deployed within the OGS. E.g. the E91 protocol requires an entangled photon source with a pair production rate R^P_{E91} = 100 Mcps [32] and an intrinsic heralding efficiency Λ_H of 85% (−0.7 dB) [33]. For Alice to detect these extreme count rates on ground, we suggest using multiplexed arrays of superconducting nanowire single photon detectors (SNSPDs) with a detection efficiency η_A of 70% (85% for one single SNSPD without multiplexing) and a total timing jitter (including electronics) t_A of 16 ps (15 ps for the SNSPD alone) [34]. This results in a total $\Lambda_A = \eta_A \cdot \Lambda_H$ = 60% (−2.3 dB) and a ground based detector noise rate of less than 100 cps which we ignore in comparison to the total E91 singles rate of $R_A \approx$ 60 Mcps. DSP requires a source capable of producing a controllable mean photon number per pulse $\mu_{DSP} \approx 0.64$ (0.1) for the signal (decoy) pulse where 50% of all pulses carry a signal[e] with a repetition rate of >1 GHz. This results in an actual signal photon rate R^P_{DSP} = 315 Mcps at Alice. The notion of heralding efficiency Λ_H is not applicable for DSP and can be set to 1. The same is true for imperfections in the sender optics, since any losses prior to the free-space link itself can be utilized to realize the desired μ_{DSP} value [37]. All sources can be designed to produce a quantum signal at wavelength $\lambda \approx$ 810 nm,

which is a good compromise taking into account atmospheric absorption, Mie scattering effects, diffraction, suitable lasers for producing entanglement and suitable space based detectors (low power consumption, low dark counts and high temporal resolution). All sources also share a common sending telescope with an unobstructed diameter (to ensure a better Gaussian mode and to limit the ground telescope attenuation $1/\Lambda_{TA}$ to 1.0 dB [38]) of $D_A = 30$ cm. The tracking precision σ_A and slew rates of modern telescopes (typically $\sigma_A < 2.4$ µrad RMS (full angle) over 5 minutes with 13°/s slew) are an order of magnitude better than necessary to track and maintain an optical link with the CubeSat. For link calculations we assumed the OGS to be located on La Palma, where both experience from previous experiments and weather data were easily available to us. However, our design is not restricted to this location and need only be slightly adapted for areas with e.g. more cloud coverage. A suitable location for a second OGS still has to be fixed (see Sect. 4.3).

3.2 The CubeSat

The CubeSat requires several subsystems as listed in Table 2. Their interrelationships are shown in Fig. 2. For a 3U CubeSat, its components must be arranged to fit within a total volume of $0.1 \times 0.1 \times 0.32$ m^3, have a combined mass of less than 4 kg and consume a maximum of 21 Wh per orbit (with deployable $\approx 30 \times 30$ cm^2 off-the-shelf solar panels

Table 2 The results of our Size, Weight and Power (SWaP) analysis along with a complete list of subsystems and their control circuits. "Energy per orbit" refers to consumption per one full orbit while performing a quantum measurement and takes into account different operation times for each device.

Subsystem name	Size (U)	Mass (g)	Peak power (mW)	Energy per orbit (mWh)
Optics + Detection				
Telescope	1	400	–	–
Shutter		100	5000	1
Dichroic mirror + PBSs	0.75	100	–	–
Phase shifter		100	see corresponding circuit below	
Detectors + Shielding		100	see corresponding circuit below	
Detector cooling (Peltier)		50	see corresponding circuit below	
Ground tracking photo diodes		100	see corresponding circuit below	
Measurement control				
Phase shifter circuit + RNG	0.02	75	50	18
Peltier circuit	0.01	50	1000	330
Detector circuit (AQ)	0.07	50	250	46
Photo diode circuit	0.07	100	500	375
Time tagging electronics	0.2	150	15,000	2750
Positioning				
Beacon + electronics	0.01	70	1000	250
XACT attitude control	0.5	900	2000	3000
GPS + main computer	0.2	100	1000	1500
RF Communication				
S-Band + UHF transceiver	0.25	114	6000	9000
Antennas	0.07	100	60	90
Energy				
Batteries	0.1	200	67,000	60,000
Solar cells	–	450	21,000	21,000
Radiator	–	200	–	–
Frame	–	250	–	–
Total consumption	3.25	3759	31,860	17,360
Available	3.25	4000	67,000	21,000

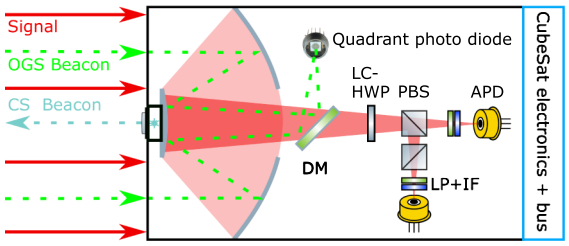

Figure 3 Schematic of the optics payload on board the 3U CubeSat. The signal and beacon beams from ground are collected by a Cassegrain-type mirror telescope. The back side of the secondary mirror carries the earth-facing beacon laser necessary for tracking of the CubeSat. The input signal and beacon are separated by a dichroic mirror (DM). The latter is tracked with a fast quadrant detector for precise attitude sensing and clock synchronization while the former passes a binary liquid-crystal-based half-wave plate switch (LC-HWP). It randomly shifts the polarization of incoming photons by either 0 or $\frac{\pi}{4}$. This effectively acts as a measurement basis switch in combination with the polarizing beam splitter (PBS) separating horizontally (vertically) polarized photons by transmitting (reflecting) them. The second PBS is used for enhanced extinction ratios. Longpass (LP) and interference filters (IF) are used to block out stray light and the photons are detected by silicon-based avalanche photo diodes (APD).

[39]). We discuss the trade-offs, design choices and compromises of the deployed components in Sect. 3.3. Here we focus on the quantum payload which consists of receiving telescope, basis choice, polarization analysis and detection subsystems (see Fig. 3). We estimate all optical losses $1/\Lambda_{OB}$ within the CubeSat (between telescope and detectors) to be 1.0 dB, using only standard commercially available devices [40–42].

3.2.1 Limiting noise counts

The most challenging aspect of designing a CubeSat is minimizing total noise counts R_{B+D} which therefore influences many design parameters. Unavoidable stray light collected by the CubeSat's receiving telescope (i.e., background counts R_{BG}) and the intrinsic thermal/radiation damage counts of the detectors (i.e., dark counts per detector R_{DC}) add up to $R_{B+D} = R_{BG} + 2R_{DC}$ and significantly degrade the SNR. R_{DC}, which we assume to be constant, has to be below 200 cps per detector to achieve a reasonable SNR. Firstly, the detector noise is reduced when operating at low temperatures. −30°C diode temperature is desirable. Two 250 cm^2 radiators on the sun-averted sides of the CubeSat could dissipate the 0.6 W of thermal energy required to cool both detectors. A heating resistor should be used to further regulate the temperature to within ±1°C. While R_{DC} of such a cooled detector can be less than 5 cps in laboratory conditions [43], it is increased by damage due to energetic particles and ionizing radiation in space. This can be mitigated by using very small active detector areas d_B. The smallest commercially available ones have a d_B of 20 µm, which we expect to be small enough to keep R_{DC} well below the 200 cps limit [44] despite a radiation damage equivalent to a 2 year mission lifetime. Using other satellite components such as high density batteries accounts for additional radiation shielding. Other procedures to further lower the dark count rate, such as annealing the diodes, could also be implemented if necessary [45]. We therefore assume a constant 200 cps of thermal and radiation noise per detector which is, at least for the first months of operation, a conservative estimate.

R_{BG} are the erroneous measurement clicks due to near-infrared noise photons originating from the ground area which are not blocked by the spectral filters. We estimate the magnitude of this effect by using measurements of earth's luminous intensity from

space [46] considering the spectral response of the Visible Infrared Imaging Radiometer Suite (VIIRS) [47] in use. More than 50% of the European Union's land area have less than 270 μcd/m^2 night sky brightness. We divide this background intensity into contributions of artifical (light pollution mainly by high pressure sodium (HPS) lamp based street lights [48] which undergoes absorption through the atmosphere [49])[f] and natural (earthshine [50]) sources. These calculations are valid for new moon conditions. Additionally, as a worst-case scenario, we account for scattered sunlight from a full moon (brightness: 4000 cd/m^2 [51]) reflected from earth (mean albedo: 0.3 [52]) into to the CubeSat (we used the solar radiation spectrum). We then translate the luminous intensity into photons [53] per second per m^2 footprint impinging on the CubeSat telescope with aperture D_B = 10 cm and calculate how many of these photons would pass through our 3 nm wide bandpass filters centered at 810 nm. We arrive at values of 0.55 photons s^{-1}m^{-2} in zenith and 0.17 photons s^{-1}m^{-2} for the lowest elevations (because of the larger distance between OGS and satellite). This effect of decreasing background counts per area for low elevations is however less significant than the increase in area because of the larger footprint on ground. The closer the CubeSat is to the horizon, the more ground area is covered by the satellite's FoV since the circular footprint in zenith changes to a substantially larger elliptical one. Optical losses and detection efficiency of the CubeSat on the other hand reduce the background count value again (see below in this section).

In total this gives us a worst-case estimate of total noise counts which we use for all orbits regardless of the moon phase: R_{B+D} varies from ≈480 cps in zenith to ≈575 cps at 30° elevation from horizon. This assumption is very conservative, especially when considering the 350 cps total noise counts at full moon of a similar uplink experiment [54].[g]

3.2.2 Field of view (FoV) and attitude control

For a given orbit height (we chose 500 km, see Sect. 4.3) and imperfect filters, R_{BG} can only be reduced by reducing the field of view (FoV = d_B/f_B where f_B is the CubeSat telescope's effective focal length). This has two additional benefits: A long f_B improves the polarizing beam splitter's (PBS) extinction ratio since it reduces the divergence of the impinging beam within the PBS. More importantly, a small d_B strongly reduces the radiation damage to the detector due to its small cross sectional area. However, the FoV must be large enough to maintain the OGS in view despite the pointing errors of the CubeSat. Until recently, the attitude control of small CubeSats was too imprecise, requiring a large FoV that would have resulted in too many background counts to make the mission possible. The latest commercially available CubeSat attitude control systems based on star trackers have shown a body pointing precision σ_B of better than 40 μrad RMS (full angle) [55, 56].[h] The resulting pointing losses Λ_{PB} due to this error, which are caused by an effective spot size broadening on the detectors when averaging over time, can be shown to be

$$\Lambda_{PB} = 1 - \exp\left[-\frac{\frac{1}{2}\mathrm{FoV}^2}{(\frac{2\lambda}{\pi D_B})^2 + \sigma_B^2}\right]. \tag{10}$$

This attitude precision allows us to limit the FoV < 50 μrad while introducing pointing losses $1/\Lambda_{PB}$ of 2.5 dB. These comparably high losses are outbalanced by the strongly reduced R_{BG} because of the narrow FoV. Roll axis precision is about a factor of 10 worse [57], however misalignment here only leads to an increase in erroneous detections e_d on

the CubeSat. Even with misalignment in the order of tens of mrad, its contribution to e_d stays below 0.1%. Optically tracking the beacon signal holds the potential to further improve Λ_{PB}. Another attitude system requirement is a sufficient slew rate. To keep the OGS in view, the CubeSat should turn with at least 1°/s; this can easily be provided by the system in consideration (10°/s slew rate in pitch and yaw axes for a 4 kg 3U CubeSat [55]).

To achieve an optimal f_B, a Cassegrain-type reflector is a good choice for the receiving telescope despite the decreased telescope transmission Λ_{TB} due to the secondary mirror (which we estimate to be −1.5 dB in total). This is because the overall design is lightweight and the required f_B of 40 cm can be realized with a 10 cm long telescope. The telescope covers the CubeSat's square Z+ surface of about 9 × 9 cm. For simplicity, our calculations assume a circular telescope with D_B = 10 cm.

3.2.3 Basis choice and polarization analysis

Another significant challenge of Q.Com with a CubeSat is the random basis choice at the start of every trial. This is necessary because Eve can exploit any predictability (or similarity between consecutive trials) of the measurement bases to gain knowledge about the key. Mechanical rotation of a HWP, while sufficient for a proof-of-principle demonstration, is far too slow. Larger satellites can either use a passive basis choice (i.e. a combination of a 50:50 beam splitter (BS), two PBSs, a HWP and four detectors, such as proposed for the 12U CubeSat of Ref. [16]) or an extremely fast active one (e.g. rapid Pockels cells). The former requires longer focal length telescopes and twice the number of detectors including their shielding, cooling and high voltage electronics. The latter is either power hungry or waveguide-based and extremely lossy even with small pointing errors due to the necessity of coupling into the waveguide. Our mission design overcomes the above limitations by using a relatively slow (response times $t_{SB} \approx 100$ µs [58]) liquid crystal half wave plate (LC-HWP) [59] similar to those on board the Singaporean quantum CubeSat [19]. The security of the Q.Com link can be maintained by only considering the first detection event after each random basis choice and discarding the rest. This leads to the additional basis switching efficiency factor

$$\Lambda_{SB} = \frac{1 - e^{-R_B t_{SB}}}{R_B t_{SB}}, \tag{11}$$

where R_B is the combined total count rate of the CubeSat detectors (including noise). For a very high single count rate of R_B = 3 kcps, Λ_{SB} amounts to less than −0.5 dB,[i] assuming that the basis change is conditional to a detection event which can simply be achieved electronically using a gate. If a slower LC-HWP (e.g. t_{SB} = 3 ms) is deployed, Λ_{SB} can go down to −8.5 dB. If one keeps all measured bits irregardless of some being measured in the same basis setting, there are no such losses, but measures would have to be taken to improve privacy amplification, which would inevitably also reduce the total secure key length. The LC-HWP can be driven by a trusted random number generator, e.g. consisting of shot-noise limited measurements of the noise on a diode [60].

After passing the LC-HWP, the photons are spatially separated by a PBS, depending on their polarization. As seen in Fig. 3, the receiving telescope focuses the beam through the polarizing optics onto the detectors. To compensate for the angle dependent extinction ratios of the PBS and ensure $e_d \leq 2\%$, another polarizer (we suggest a second PBS rotated by 90° due to its high transmission) must be used in the reflected arm of the first PBS. To

minimize polarization detection errors due to misalignment between the CubeSat and the ground station, the CubeSat has to rotate around its Z axis to maintain the same frame of reference. Another possibility would be to calculate the CubeSat's rotation and precompensate on ground via a half-wave plate, analogous to Ref. [3].

3.2.4 Dead time and timing resolution

To ensure that saturation and dead time effects do not cause losses >0.1 dB, we require a maximum count rate of each CubeSat detector $R_B^{max} \gg R_B$ in the order of 100 kHz. The detectors consist of actively quenched silicon-based avalanche photo diodes (APDs) operated in Geiger mode, placed at the output ports of the PBS. The detector diameter d_B of only 20 μm strongly reduces the cross sectional area for harmful radiation. Therefore little to no radiation shielding is required, which has a positive effect on the mass budget (see Table 2).

Errors in Q.Com arise from accidental coincidences and are therefore related to the coincidence detection time window τ. To correctly identify and distinguish at least 98% of all pairs, τ has to be greater than $\approx 2\sqrt{t_A^2 + t_B^2}$, where $t_A = 16$ ps is the total timing jitter on ground and t_B that on the CubeSat. Thus t_B, including the jitter of the detectors [43] and the time tagging electronics that note the arrival time of each pulse [61, 62], should be less than 37 ps to ensure that we can choose $\tau = 80$ ps which is crucial to improving the SNR. The detection efficiency of the detectors we chose is $\eta_B = 15\%$. This might seem low, however we trade this for excellent temporal resolution. There is a trade-off between these two parameters: Higher detection efficiency can increase the secure key rate, however then the link becomes more susceptible to noise counts because of an extended coincidence detection window (see Fig. 4).

In addition to the quantum payload, the CubeSat optics should also accommodate an earth-facing beacon diode to aid in the ground station's tracking of the CubeSat. There should also be a dichroic mirror to separate the quantum signal from the OGS beacon.

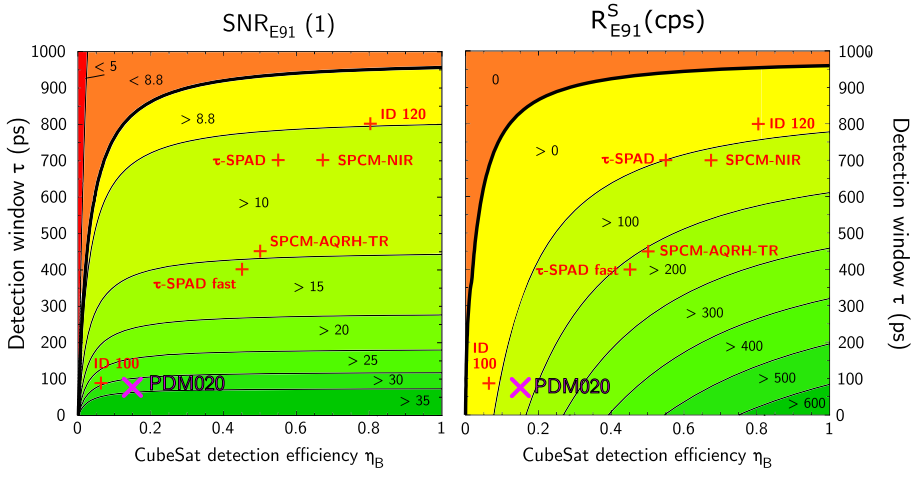

Figure 4 Contour plots of signal-to-noise ratio (SNR_{E91}, *left*) and secure key rate (R^S_{E91}, *right*) for an E91 scheme with a typical Fried parameter $r_0 = 20$ cm and an elevation of 60°, showing the trade-off between CubeSat detection efficiency η_B and timing resolution $\tau \approx 2\sqrt{t_A^2 + t_B^2}$ where we assume $t_A = 16$ ps to be fixed. For our study, since we want to show principal feasibility, we chose the PDM020 detector [43] (shown with a cross) which provides a good compromise between SNR and key rate. Other detectors are shown for comparison.

The latter assists in locating and tracking the OGS and can be detected by a fast quadrant photo diode. The OGS's beacon signal is pulsed to facilitate clock synchronization, and the detection pulses from the fast photo diode (along with GPS signals) are used to discipline the local clock on board the CubeSat.

3.2.5 Classical communication

In addition to the transmission of photons, classical communication and processing is required to generate a secure key. The amount of processing done on board the CubeSat must be minimized. Thus the CubeSat will need to transmit all detection events to the OGS, which will compute coincidence events and share data identifying these sparse events with the CubeSat. Therefore the amount of data transmitted by the CubeSat far exceeds the amount of data received. We use an S-band transceiver for the actual transmission of data. Additionally, we deploy a slower UHF transceiver for housekeeping communications [63]. For the SWaP budget, we assume peak power consumption during the whole orbit as a worst-case scenario and to account for the use of several successive OGS connections. Details about the data rates can be found in Sect. 4.5 while the processing power and time required for the CubeSat to calculate the secure key is estimated in Sect. 4.6.

3.3 Preliminary SMaP analysis

Using commercially available CubeSat components, we optimized the secure key rate produced by the CubeSat while adhering to the strict SWaP limitations. Our results are shown in Table 2. All systems not described in Sect. 3.2 are based entirely on readily available standard CubeSat components. Further customizing of certain parts would significantly lower the total SWaP consumption. The only component that would have to be modified is the time tagger, which is however within reach of current technology [61].

A standard 3U CubeSat is $10 \times 10 \times 34.1$ cm^3 excluding the solar panels (with a maximum protrusion limit of 6.5 mm) [64]. We used a CAD model (a simplified version of which is shown in Fig. 5) to study the actual assembly of components. Please note that we did not include size margins into our calculations since the telescope could be redesigned for a size surplus of 7%. Also, the optics payload would allow for additional space e.g. for the batteries (as shown in Fig. 5). However, since we restrict ourselves to off-the-shelf components, a 5% margin is sufficient for the harness/electrical connections. Another way to gain more space would be to use the less common 4U standard ($10 \times 10 \times 45.4$ cm) [65].[j]

The CubeSat standard mass limit is 4 kg for a 3U. We can include a 6% mass margin and remain below this value. However this requirement can be relaxed to 5 kg depending on the launch provider [66]. This is useful if an operational lifetime of more than 6 months is desired which necessitates heavier shielding of the APDs (not included in the current SWaP). The type of solar panels [39] and the orbit of the CubeSat (see Sect. 4.3) limit the total power production per orbit to 21 Wh. We consume only 83% of this value. The satellite is within line of sight of the OGS for a maximum of 11 min (if it passes with 0° inclination), of which at most 220 s can be used for key generation. Thus most subsystems only operate for a fraction of each orbit. Together these consume 17.4 Wh[k] while the always-on systems (attitude control, UHF-band communications, GPS and main computer) consume a further 13.5 Wh per orbit. The CubeSat's single-photon detector system must operate only at night to avoid excessive background counts. Therefore a large set of

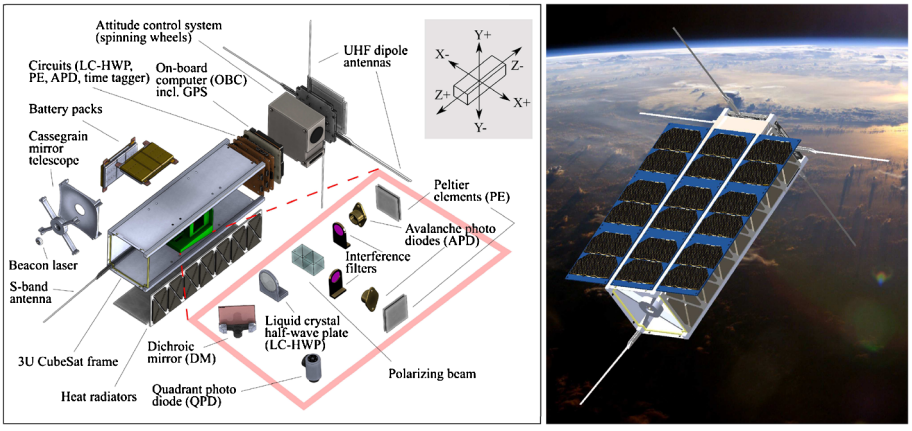

Figure 5 *Left*: Exploded view of our preliminary 3U CubeSat design. The solar panels as well as any electric connections have been omitted for clarity. The optical elements shown in the red box are out of scale. *Right*: Artistic depiction of the 3U CubeSat with deployable solar panels in bird-wing configuration. They are mounted to the sun-facing side of the CubeSat, the other three long sides of the surface can be covered with radiators for detector cooling.

batteries are necessary. To preserve battery life and provide a safety margin we assumed that the batteries are never drained by more than 30% . Thus we require a total battery capacity of at least 58 Wh. Our design provides for 60 Wh [67]. The CubeSat consumes a total of 17.4 Wh per orbit while its solar panels can produce a maximum of 21 Wh. The typical performance of this class of triple junction solar panels degrades to ≈85% of the above beginning of life value over 10 to 15 years [68, 69]. Thus with our short 1 to 2 year mission lifetime we can safely ignore this degradation. This means that the CubeSat is capable of one Q.Com connection per orbit. Larger satellites would be needed for continuous operation of the Q.Com link with more than one OGS per orbit, however this drastically increases the cost.

4 Performance analysis

Having specified the key parameters for the design of our CubeSat, we now want to give an estimate on the amount of secret key the satellite could acquire with two sufficiently separated OGS[l] over one year (Sect. 4.7). To this end, we derive a model for geometric losses due to beam divergence (Sect. 4.1) while incorporating long-time measurements of atmospheric turbulence and weather influences (Sect. 4.2) to calculate different loss scenarios for our uplink. We also carry out an orbit assessment (Sect. 4.3). Lastly, we evaluate the requirements for an on board clock (Sect. 4.4) and estimate the data storage and -transmission needs (Sect. 4.5) as well as the computational requirements of the CubeSat (Sect. 4.6).

4.1 Optical loss model

The total transmission Λ consists of several contributions:

$$\Lambda = \Lambda_A \cdot \Lambda_B = \eta_A \cdot \Lambda_H^2 \cdot \Lambda_{TA} \cdot \Lambda_L \cdot \Lambda_{PB} \cdot \Lambda_{TB} \cdot \Lambda_{OB} \cdot \Lambda_{SB} \cdot \Lambda_{SYN} \cdot \eta_B, \tag{12}$$

where $\eta_A \cdot \Lambda_H^2 \cdot \Lambda_{TA}$ is 1 for DSP, Λ_{SYN} is the transmission factor due to clock synchronization (see Sect. 4.4) and Λ_L is the link transmission from sender to receiver lens which

we want to assess in this section. For a detailed justification of the values in use (listed in Table 1), see Sect. 3 of this manuscript. Assuming Gaussian optics, Λ_L can be estimated as

$$\Lambda_L(\varphi) = \left[1 - \exp\left[-\frac{1}{2}\left(\frac{D_B}{w_{LP}(\varphi)}\right)^2\right]\right] \cdot \Lambda_{ATM}(\varphi), \tag{13}$$

where $w_{LP}(\varphi)$ is the effective beam waist of the uplink signal at the satellite, depending on the zenith angle φ:

$$w_{LP}(\varphi) = \sqrt{w_L^2(\varphi) + \left(\sigma_A \cdot L(\varphi)\right)^2}. \tag{14}$$

Here, we assumed that the OGS's pointing error σ_A follows a normal distribution, effectively increasing the divergence of the up-going beam. This is equivalent to the effect of an OGS pointing loss $1/\Lambda_{PA}$. $L(\varphi)$ is the distance OGS-satellite. $w_L(\varphi)$ is the beam waist at the CubeSat prior to pointing errors:[m]

$$w_L(\varphi) = L(\varphi)\frac{\lambda}{0.316 D_A \pi}\left[1 + 0.83 \cdot \sec(\varphi)\left(\frac{D_A}{r_0}\right)^{5/3}\right]^{3/5}, \tag{15}$$

where $\lambda = 810$ nm is the photon wavelength (see Sect. 3.1) and r_0 is the Fried parameter in zenith. The atmospheric transmission factor $\Lambda_{ATM}(\varphi)$ in Eq. 13 is given by

$$\Lambda_{ATM} = \exp\left[-\beta \cdot \sec(\varphi)\right], \tag{16}$$

where $\beta = 0.22$ is the extinction optical thickness at sea level for 800 nm [70].

4.2 Weather considerations

Weather conditions are crucial especially for optical uplinks since atmospheric disturbance happens immediately after the sending aperture. The Fried parameter r_0 gives an estimate of the atmosphere's coherence length and directly influences the upgoing beam's divergence, similar to an optical aperture. Measurements of the RoboDIMM on La Palma [71] over 9 years allow us to estimate the atmospheric link quality for an OGS stationed there (see Fig. 6). For days with cloud coverage and other meteorological effects hindering optical links, no r_0 data is available. Where this is the case, we assumed a quantum link to be impossible, resulting in a total of 228 nights per year where a key exchange could

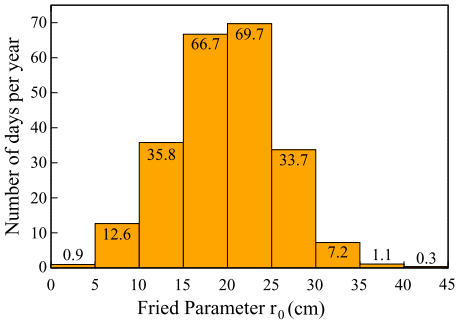

Figure 6 Histogram of days per year with certain Fried parameters r_0, averaged over nine years starting in February 2008. Insufficient weather conditions (clouds, rain, winds) as well as technical problems lead to $N = 228$ instead of 365. The average daily r_0 is 19.7 cm.

be done in principle. Optical loss estimates for different Fried parameters can be found in Sect. 4.7, assuming a 500 km orbit and 0° inclination w.r.t. the OGS. Deployment of adaptive optics systems on ground correcting for atmospheric turbulence could further decrease Λ_L.

4.3 Orbit considerations

A preliminary assessment of possible orbits has to consider several limitations. To minimize space debris, a CubeSat without an extra de-orbit mechanism cannot exceed an orbit of 650–700 km which limits the lifetime in orbit to less than 25 years [72]. On the other hand, we would like the mission to have an operational lifetime of at least one year. This results in a minimum orbit altitude of around 400 km (which is approximately the height of the ISS orbit). Subsequently, within a range between 400 and 700 km, the choice of orbit altitude is driven by the desire to maximize the link time, relax requirements to the attitude control system as well as alignment considerations and the power budget. Considering the need to conduct the experiments during eclipse times and the fact that a significant amount of (classical) data needs to be sent between OGS and CubeSat, also orbit inclination and right ascension of the ascending node (RAAN) need to be considered. Variation of any of those orbital parameters has significant impact on the amount and duration of passes per day. We arrived at a preliminary orbit height of 500 km (LEO). The type of orbit has an equally significant impact. An initial assessment was done to compare the link budget between a 97.3° inclined sun-synchronous (SSO) and a circular orbit (CO) with 30.0° inclination. The calculations were done such that contact time was restricted to elevations above 30° from horizon and only between local midnight and 6:00 am, such that the passes allow for an actual quantum link. Considering the low altitude of 500 km, those two limitations should ensure that the satellite is in the umbra.[n] For the calculations shown in Fig. 7, a ground station on La Palma was assumed. For this location, the optimum LTAN of the CO is between 37° and 72° (extended maxima). For transmission of classical data via the S-band link, all visible orbits can be used which amounts to another ≈40,000 s (≈200,000 s) for SSO (CO). The results shown in Fig. 7 are for a mission time of one year (June 2020 to June 2021). While the total link time of the SSO is only 37,115 s, the 30° CO offers a significantly higher total link time of 71,435 s. Figure 8 shows the main reason

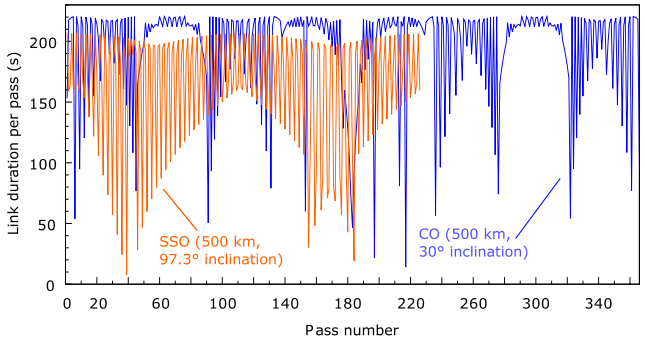

Figure 7 500 km LEO orbits that appear with more than 30° elevation from horizon and are visible between 0:00 and 6:00 am over La Palma for different inclinations. Comparison of the link duration between two 500 km low-earth orbits (LEOs): 97.3° sun-synchronous (red) and the optimal 30° circular orbit (blue). Only passes with more than 30° maximum elevation at night are shown. The average visible time per pass is 195 s (163 s) for CO (SSO), the total visible time per year amounts to 71,435 s (37,115 s) for CO (SSO).

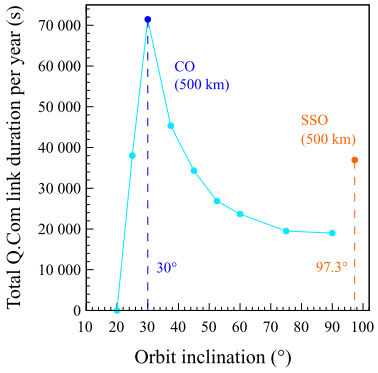

Figure 8 Variation of the total link time (during one year for one OGS on La Palma) for different 500 km circular orbits (CO) and the only possible 500 km sun-synchronous orbit (SSO) as a function of their inclination. We assume that the OGS is located at 28°45′25″ N, 17°53′33″ W. Only passes with more than 30° maximum elevation are considered to be contributing to the total link time.

for this difference. The number of passes for a CO is significantly higher than for an SSO during one year (366 vs. 227). Also, the CO passes have a higher average link time (195 s vs. 163 s). The inclination of a CO and its altitude have a large impact on the link time. The best results in terms of total link time are achieved with an inclination close to the latitude of the ground station, in our case assumed to be on La Palma. It also has to be considered that the trapped proton flux in LEO is a significant source of radiation, possibly causing damage to the detectors. This radiation is significantly lower for a CO than an SSO [73].

We therefore conclude that altogether, a 30° CO would be the optimal choice in terms of performance and reliability of the CubeSat and use it for our further calculations. Nevertheless, launching the CubeSat into an SSO is more common and can be significantly cheaper.

If we assume that an eavesdropper cannot access the secret key exchanged between the ground and the CubeSat, then the CubeSat can be trusted (i.e., it is a trusted node) to exchange another key with a second ground station and securely relay a message. The second OGS should be situated along the path of the CubeSat. Currently, daytime Q.Com is not possible with our scheme. However, an OGS in e.g. Australia would be able to communicate with the CubeSat during daytime in La Palma (assuming the choice of a 30° CO, Brisbane would have as much link-time per year as La Palma).

4.4 Clock synchronization

Both the OGS and the CubeSat measure the arrival time of photons according to their own local clocks (oscillators). Nevertheless, to identify photon pairs, we must synchronize these two clocks. The precision of this clock synchronization along with the timing jitter of the detectors and electronics determines the coincidence window. Improper synchronization leads to otherwise avoidable losses.

Synchronization can be achieved using various methods such as coarse synchronization to 10 ns using GPS [74], exploiting the intrinsic time correlation of entangled photon pairs [75], or using a pulsed beacon laser [2]. GPS alone is insufficiently precise. In order to exploit the time correlations of photon pairs, we must measure a cross-correlation peak in the arrival times between the OGS and CubeSat. The smallest measurement duration where we can unambiguously identify almost every coincidence peak (with the maximum acceptable total loss calculated above) is 100 ms.[o] In LEO, the velocity of the CubeSat is so large that the optical path length between the OGS and satellite can change by as much as ≈6 km/s. Naturally, this causes the coincidence peak to broaden significantly. Orbital

predictions and measurements can be used to correct for this. However, their typical precision is about 10 cm [76]. This still adds a few hundred picoseconds to the coincidence window needed.

Thus we use a pulsed beacon laser on the OGS and fast photo diodes in the CubeSat to implement a phase-locked loop and make sure that the CubeSat clock oscillates at the same frequency as the OGS's. A beacon laser pulsed at a repetition rate of f_{SYN} = 10 MHz coupled with a fast photo diode receiver (≈1 GHz bandwidth) on the satellite can be used to synchronize the two oscillators to within 10 ps. Additionally, turbulence in the atmosphere can account for up to 3 mm (i.e. ≈10 ps) of jitter in the beacon laser's arrival time [77]. The effects of such phase jitter on the received signal can be mitigated to a large extent using a technique called jitter attenuation [78]. Doppler and relativistic shifts could also affect the oscillator synchronization. The latter is corrected for by precompensating the CubeSat oscillator frequency on the ground similar to Ref. [79]. The former can be addressed by adjusting the repetition frequency of the pulsed beacon. Nevertheless, let us conservatively consider a total clock synchronization jitter of 20 ps. Using our chosen coincidence window of 80 ps, the above results in a synchronization loss $1/\Lambda_{SYN} < 0.5$ dB. Alternatively, we could avoid this additional loss by increasing the coincidence window to accommodate the uncertainty in clock synchronization (i.e. the coincidence window would be 100 ps instead of the chosen 80 ps).

4.5 Data storage and transmission

Since the computing power on the CubeSat is limited, Bob should send the list of all his time tags and basis choices (not measurement outcomes) down to the OGS and let Alice identify the coincidences and matching bases to tell him which counts to use. To estimate the size of data packages, we assume a time tag resolution t_{TT} of 10 ps [61]. To keep the data size per tag low, it is beneficial to store just the time elapsed between consecutive events on the CubeSat. The probability η_{sep} that the temporal separation between two successive photons will not exceed a time span t_{max} during a maximum quantum connection of duration t_{QC} = 220 s (see Sect. 4.3) is given by

$$\eta_{sep} = \left(1 - (1 + R_B t_{max}) \cdot e^{-R_B t_{max}}\right)^{\frac{t_{QC}}{t_{max}}}. \tag{17}$$

If one aims for a probability of less than 0.1% for an overflow to occur during one 220 s connection (i.e., $\eta_{sep} > 99.9\%$), assuming a minimum R_B of 1 kcps because of noise counts in both detectors, $t_{max} \approx 20$ ms (result obtained numerically). This is equivalent to $\log_2(\frac{t_{max}}{t_{TT}}) = 33$ bits per time tag including information about measurement basis and outcome. Therefore in one visible pass under optimal conditions (i.e., a 0° inclination overpass with an r_0 of 40 cm), a maximum of 17 Mbit of data is acquired. This means that with an 250 kbps S-band transceiver on board the satellite, the data can be sent down in about 70 s.[p] This is possible still during the Q.Com orbit if the classical transfer can be started right after the quantum link is established. Otherwise, another ground station in the satellite's path could be used or simply the next visible orbit. After Alice has calculated the correlation function and compatible basis choices, she needs to tell Bob which bits to use. Re-sending the time tags of the correct outcomes amounts to a total 3.2 Mbit and requires another orbit since Alice has to calculate the $g^{(2)}$ in advance. In this second

orbit, error correction and privacy amplification can also be carried out. The communication volume required for error correction, assuming a one-way low-density parity check (LDPC), strongly depends on the QBER. In the worst-case scenario, it amounts to 50% of the raw key length (corresponding to a QBER close to 11%; a typical value is 20%, with a QBER of 3% [29]), i.e. less than 200 kbit of data being sent up to the CubeSat. In the present design of the satellite, the operational mode for data transfer via S-band will have different alignment requirements than the standard operation mode for power generation. Considering the relatively short duration of the communication windows needed this is not an issue and sufficient time will be available to recharge the batteries.

4.6 On-board computing requirements

The classical post processing required to obtain a secure key is not trivial and dictates the choice of the on-board processing capabilities of the CubeSat. A detailed overview of these requirements can be found in Ref. [80]. We also base our estimates on the equations provided there.

The first step is to identify coincidence events. This is commonly done by computing a timing cross-correlation histogram which can be a computationally intensive task.[q] We recommend that the CubeSat share the timing of all its detection events with the OGS. The OGS can identify coincidence events and notify the CubeSat. This minimizes the amount of data transferred and the amount of calculations the CubeSat needs to perform. The on board processing of all the n_{tag} time tags should be less than $18n_{tag}$ operations in the worst case. Calculating a sifted a key of length m_{key} is estimated to require roughly m_{key} bits of memory and $15m_{key}$ operations to complete. Error correction requires additional memory and computational power. About 10 to 20 MB of memory are sufficient for this when using algorithms based on LDPC codes. The necessary LDPC matrices can be agreed upon before the mission and be stored locally for different QBER configurations. The same is true for privacy amplification algorithms. Together they consume less than 100 MB of storage space. Privacy amplification can be very memory efficient when using a linear-feedback shift-register-based matrix implementation and only requires memory equal to the sifted key length (i.e., m_{key} bits). To estimate the processing power required, we must keep in mind that a lower SNR increases the amount of error correction and privacy amplification necessary. In the worst case we estimate that all these PP steps will require $\approx$258 million operations per second to calculate the secure key in real time. This can easily be handled by a commercially available space certified on-board computer (OBC) with an ARM9 processor running at 400 MHz with enough spare processing power for other satellite tasks [81]. Considering possible delays and interruptions in the classical communication link, we estimate that PP would require approximately 300 MB of temporary memory. The OBC we consider can provide as much as 4 GB SD card storage space. We note that the on-board operating system, control programs, housekeeping functions etc. will require additional processing power and memory.

4.7 Expected secure key rates

Now that we have shown that Q.Com with a 3U CubeSat is feasible in principle, we will give an estimate of the expected key rates. Measurements by the RoboDIMM seeing monitor on La Palma show that an r_0 of larger than 5 cm can on average be achieved for 228 nights per year (see Fig. 6) or 62% of the time. Therefore, assuming a circular orbit with 30° orbital

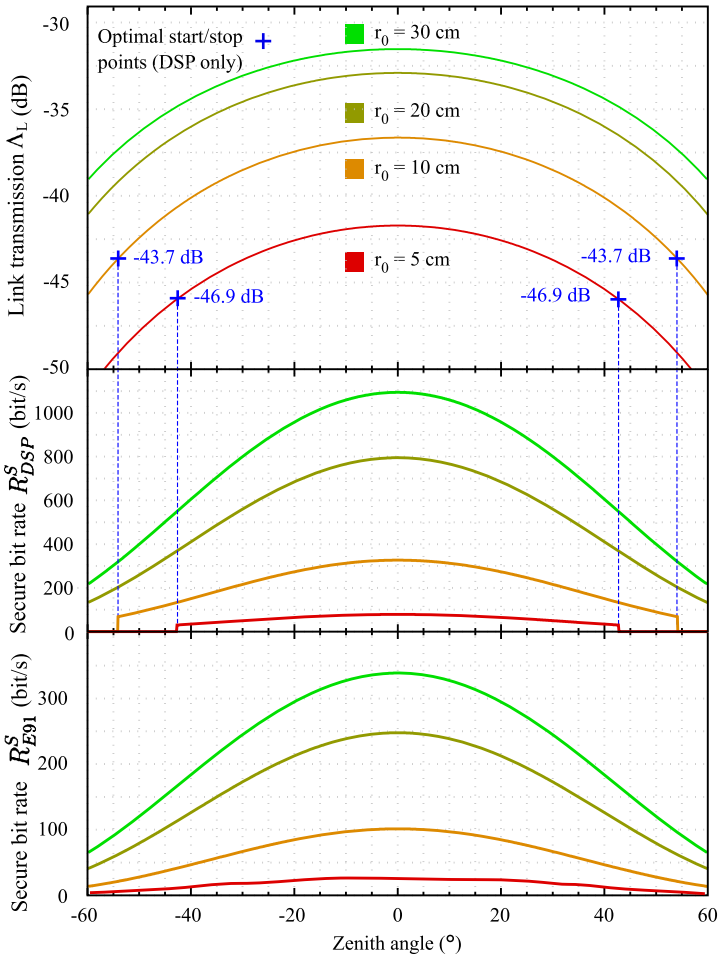

Figure 9 Link Loss Λ_L and secure key rates R^S_{DSP}, R^S_{E91} as functions of zenith angle φ. All curves are shown for 0° incliniation w.r.t. the OGS. Similar curves can be calculated for different inclination angles. *Top:* Link transmission $\Lambda_L(\varphi)$ of a 500 km orbit for different Fried parameters r_0. E91 is more tolerant w.r.t. high link losses because of its immunity to photon number splitting attacks, it can therefore always be performed during the full quantum connection. A minimum elevation from horizon of 30° is required (i.e. $|\varphi| \leq 60°$). *Middle:* Secure key rates for DSP using optimal starting points for those values of r_0 that are too small to allow communication throughout the orbit (marked by pluses). Other contributions to Λ are being accounted for in these points. The temporal integral over these curves, i.e. the total key acquired during one pass, amounts to 6.8 kbit ($r_0 = 5$ cm), 33.9 kbit (10 cm), 95.2 kbit (20 cm) and 137.4 kbit (30 cm) respectively. *Bottom:* Secure key rates of E91 for different r_0. The total key acquired during one pass amounts to 2.6 kbit ($r_0 = 5$ cm), 11.0 kbit (10 cm), 29.4 kbit (20 cm) and 42.0 kbit (30 cm) respectively.

inclination (see Sect. 4.3), it can be assumed that for a total of 44,300 s or 12:20 h each year, the link quality is sufficient to perform Q.Com. The average inclination in zenith as seen from the OGS is 28.3° (unlike the orbital pass shown in Fig. 9 where φ goes down to 0°). Computing for such an average orbit and taking the r_0 measurements of Sect. 4.2 into account, the total key acquired in one year would therefore amount to 4.0 Mbit (13.0 Mbit) for E91 (DSP).

5 Conclusion

Q.Com offers the best security currently possible since it is based on laws of physics as opposed to the difficulty of solving certain problems. However, it is expensive and com-

munication distances are limited. Our complete feasibility study has shown that it is possible to achieve Q.Com over thousands of kilometers, via a single trusted node, using a relatively cheap and easy to construct CubeSat. By miniaturizing the design, optimizing power consumption and minimizing the mass we have shown that full-fledged commercial global Q.Com can be achieved with a simple 3U CubeSat. We have provided an outline for building a Q.Com mission which includes selection guides for the components, trade-offs and optimizations for the secure key rate, choice of orbits etc. We discussed methods to overcome key challenges using currently available technology. We showed that the fine pointing capabilities of CubeSats no longer limit their applicability for Q.Com and optical links.

Using our CubeSat design, a pair of ground stations can exchange $13 \cdot 10^6$ secure bits a year (ignoring finite key effects). Our CubeSat design consists of commercially available components that cost <200,000 € [82]. A typical launch price is <300,000 € [66]. Naturally, the research/development and manpower costs for the first such satellite would be higher and are not included. Assuming a lifetime of two years, information theoretic security could be bought for ≈20 €/kbit,[r] provided that an operational OGS is readily available. If deploying the decoy protocol, such an OGS would be about 100,000 €. For E91, there is no serious assessment possible at the moment due to rapid developments in nanowire technology and its strong dependence on the final detection scheme.

A commercially viable Q.Com satellite needs significant classical computation power, data storage and classical communication bandwidth. We have evaluated these requirements and outlined strategies to achieve all this with minimal resources. Our CubeSat is compatible with the widest possible variety of polarization based Q.Com protocols. It can implement the decoy state protocol to minimize client resources or entanglement-based protocols for best verifiable security. We have provided a CAD model of the CubeSat as well as a detailed discussion of the trade-offs involved in selecting components (such as those between: detection efficiency and timing jitter, radiation damage and FoV, erroneous counts and detector size, E91 and DSP, orbit of the satellite and total key etc.).

In the current design, the CubeSat is a trusted node. This is suitable for useage scenarios like communication between many branches of a single organization. The current state-of-the-art Q.com satellites are prohibitively expensive trusted nodes, for communication across the globe, that can only be built by a few select industries. A CubeSat—such as we have shown above—is cheaper and interested organizations can build their own or carefully supervise the building of these trusted nodes for their own use.

The proposed CubeSat can also be used for fundamental experiments such as Bell tests which require a SNR of only 4.8 (as opposed to the SNR of 8.8/15.1 needed by QKD), clock synchronization, light pollution measurements and earth/atmosphere observation at the beacon wavelengths. It can also be used to study the effect of gravity on quantum systems [83].

Acknowledgements
We would like to acknowledge valuable discussions with Johannes Handsteiner, Bo Liu and Dominik Rauch of IQOQI Vienna.

Funding
FFG/ASAP11 Grant Number: 4927524 / 847964 (QubeSat), FFG Grant Nr. 6238191 / 854022, ESA/ESTEC Grant Nr. 4000112591/14/NL/US.

Availability of data and materials
Simulations and scripts are made available upon request by the corresponding author RU.

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
The satellite design, feasibility study and simulations were done by SN, MF, and SKJ. The mechanical CAD design was created by RB, DB and SN. Orbital calculations were made by CS and SA. EK and MB handled the systems engineering and provided valuable feedback. The effort was conceived and supervised by RU and co-supervised by SKJ. All authors read and approved the final manuscript.

Author details
[1]Institute for Quantum Optics and Quantum Information Vienna, Vienna, Austria. [2]Vienna Center for Quantum Science and Technology, Vienna, Austria. [3]University of Applied Sciences Wiener Neustadt, Wiener Neustadt, Austria. [4]Laboratoire Interdisciplinaire de Physique, University Grenoble Alpes, Saint-Martin-d'Hères, France.

Endnotes
[a] The PP steps also require a classical communication channel. For details see Sect. 4.5.

[b] It is important to note that imperfect implementations of Q.com, such as those with high transmission loss [24] or those where the detectors are susceptible to blinding [25], can be vulnerable to an eavesdropper. However, security can still be guaranteed (and verified in the case of entanglement based protocols) using reasonable assumptions. First we assume that the losses in transmission are reasonably well known and are to a large extent beyond the control of Eve. Second, by maintaining line of sight during communication and securing the area around the Optical Ground Station (OGS) covered by the satellite's FoV, we can prevent a blinding attack.

[c] Because the information entropy factor (in square brackets) depends on the gains for DSP (see Eq. 9), there is no constant limit for DSP, it depends on losses and on the average photon number per pulse. The value given is a mean value for the loss scenarios considered by us.

[d] In information theory, "rate" is a normalized quantity related to entropy. However, throughout this paper we continue to use the common definition of rate as number of occurrences/instances per second.

[e] Our key rate estimation based on the *signal* pulse's μ_{DSP} is just an approximation without taking the photon statistics of the *decoy* states into account, which have a small, but non-negligible effect on the key rate. For simplicity and in order to obtain algorithms compatible with the computing power available to us, we stick to the partial formalism outlined in Ref. [9]. For a more detailed analysis, we refer the reader to [35] and [36].

[f] The recent development of replacing HPS street lights with LEDs positively affects noise counts because the LED spectrum is marginal in NIR and IR. For a conservative estimate, we only considered HPS.

[g] A direct comparison with the results of Ref. [54] is not possible because of differences in the FoV, spectral response etc. of the systems used. Nevertheless, the reported noise count values are in good agreement with our simulations and can be used as an approximate guideline for our design.

[h] It should be noted that the manufacturer's precision performance claims regarding the quoted XACT system are tentative since this performance has only been shown in-orbit for static (inertial) pointing.

[i] For the sake of completeness it has to be noted that $1/\Lambda_{SB}$ is the only attenuation which also acts on intrinsic dark counts (R_{DC}). Since the losses are not very high and we want to avoid underestimating noise counts, this effect is omitted.

[j] This would e.g. be possible by launching the CubeSat from the ISS into an approximately 400 km orbit since the space station has a 4U launcher readily available.

[k] The time each subsystem needs to run is calculated using conservative estimates. The detectors plus cooling are assumed to run at peak power throughout, although they only consume so much during the initial temperature stabilization phase before Q.Com starts. Similarly, fast S-band data transmission is assumed to run continuously, when in reality it need only operate when in line of sight of an OGS.

[l] For our preferred 500 km 30° inclination orbit, e.g. Brisbane on the Australian east coast would be a near choice as second OGS additional to La Palma. If larger global coverage with many OGSs is desired—however leading to less passes over La Palma—, a 97° SSO orbit could be the better choice (see also Sect. 4.3).

[m] The divisor 0.316 results from the fact that any aperture passed by a real beam results in an Airy disk pattern. We consider only the innermost disk since all others' divergence is too great to hit the satellite. Now 0.316 D_A is the beam waist that an ideal Gaussian beam of the same intensity distribution as the innermost airy disk would have at the sending aperture, which allows us in good approximation to stick to Gaussian optics instead of having to apply Bessel functions.

[n] If a more detailed analysis shows that stray sunlight is still a problem, further reducing the allowable time for contact is an option. For example, limiting the time from midnight to 5:00 am reduces the total contact time for one year to 57,700 s which is still acceptable.

[o] Our minimum expected pair rate is about 52 pairs s^{-1}. To be able to correctly identify a peak, we must have more coincidence events than accidentals. With 5 coincidences we can correctly identify the peak >95% of the time. We choose 100 ms as the minimum chunk duration in order to be able to obtain the required number of coincidences.

[p] These data transfer calculations assume an error free S-band link. Additional time or bandwidth will be needed to avoid garbled data.

[q] The computational complexity of this task depends on the range of time delays that need to be scanned. Poor clock synchronization, low count rates and ever changing delays due to the satellite's motion increase the range of delays over which the cross correlation function must be computed.

[r] There are several ways to improve the cost per kbit. First, better radiation resistance and shielding would increase the lifetime of the CubeSat and proportionally decrease costs. Second, the current cost estimate is for the interaction of one CubeSat with a pair of OGSs on opposite sides of the globe. However with careful selection, one can use multiple OGSs with the same satellite during a single orbit provided we can increase the battery capacity of the CubeSat. Third, a mass produced constellation of satellites could reduce the cost by a further order of magnitude. Fourth, key expansion protocols can be used to grow the key with only marginal security implications. And finally, the deployment of detectors with other characteristics can help improve the key rate at cost of the SNR (see Fig. 4).

Publisher's Note

Received: 11 November 2017 Accepted: 20 March 2018 Published online: 27 April 2018

References

1. Azuma K, Mizutani A, Lo HK. Fundamental rate-loss trade-off for the quantum Internet. Nat Commun. 2016;7:13523.
2. Yin J, Cao Y, Li YH, Liao SK, Zhang L, Ren JG, et al. Satellite-based entanglement distribution over 1200 kilometers. Science. 2017;356(6343):1140–4.
3. Liao SK, Cai WQ, Liu WY, Zhang L, Li Y, Ren JG, et al. Satellite-to-ground quantum key distribution. Nature. 2017;549:43–7.
4. Yin HL, Chen TY, Yu ZW, Liu H, You LX, Zhou YH, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys Rev Lett. 2016;117(19):190501.
5. Ursin R, Tiefenbacher F, Schmitt-Manderbach T, Weier H, Scheidl T, Lindenthal M, et al. Free-space distribution of entanglement and single photons over 144 km. Nat Phys. 2007;3:481–6.
6. Takenaka H, Carrasco-Casado A, Fujiwara M, Kitamura M, Sasaki M, Toyoshima M. Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite. Nat Photonics. 2017;11:502–8.
7. Ekert AK. Quantum cryptography based on Bell's theorem. Phys Rev Lett. 1991;67(6):661.
8. Bennett ChH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Int. conf. on computers, systems and signal processing. Bangalore, India. Dec. 1984. 1984. p. 175–9.
9. Lo HK, Ma X, Chen K. Decoy state quantum key distribution. Phys Rev Lett. 2005;94:230504.
10. Bennett CH, Brassard G, Mermin ND. Quantum cryptography without Bell's theorem. Phys Rev Lett. 1992;68(5):557.
11. Bennett CH. Quantum cryptography using any two nonorthogonal states. Phys Rev Lett. 1992;68(21):3121.
12. Ursin R, Jennewein T, Kofler J, Perdigues JM, Cacciapuoti L, de Matos CJ, et al. Space-quest, experiments with quantum entanglement in space. Europhys News. 2009;40(3):26–9.
13. Scheidl T, Wille E, Ursin R. Quantum optics experiments using the International Space Station: a proposal. New J Phys. 2013;15(4):043008.
14. Günthner K, Khan I, Elser D, Stiller B, Bayraktar Ö, Müller CR, et al. Quantum-limited measurements of optical signals from a geostationary satellite. Optica. 2017;4(6):611–6.
15. Jennewein T, Grant C, Choi E, Pugh C, Holloway C, Bourgoin J, et al. The NanoQEY mission: ground to space quantum key and entanglement distribution using a nanosatellite. In: Emerging technologies in security and defence II; and quantum-physics-based information security III. vol. 9254. International Society for Optics and Photonics; 2014. 925402.
16. Kerstel E, Gardelein A, Barthelemy M, Team TC, Fink M, Joshi SK, et al. Nanobob: a Cubesat mission concept for quantum communication experiments in an uplink configuration. 2017. arXiv:1711.01886.
17. Bedington R, Arrazola JM, Ling A. Progress in satellite quantum key distribution. npj Quantum Inf. 2017;3(1):30. https://www.nature.com/articles/s41534-017-0031-5.
18. Oi DK, Ling A, Vallone G, Villoresi P, Greenland S, Kerr E, et al. CubeSat quantum communications mission. EPJ Quantum Technol. 2017;4(1):6.
19. Tang Z, Chandrasekara R, Tan YC, Cheng C, Sha L, Hiang GC, et al. Generation and analysis of correlated pairs of photons aboard a nanosatellite. Phys Rev Appl. 2016;5(5):054022.
20. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Rev Mod Phys. 2002;74(1):145–95.
21. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. Rev Mod Phys. 2009;81(3):1301.
22. Sergienko AV. Quantum communications and cryptography. Boca Raton: CRC Press; 2005.
23. Fung CHF, Ma X, Chau H. Practical issues in quantum-key-distribution postprocessing. Phys Rev A. 2010;81(1):012318.
24. Valivarthi R, Lucio-Martinez I, Chan P, Rubenok A, John C, Korchinski D, et al. Measurement-device-independent quantum key distribution: from idea towards application. J Mod Opt. 2015;62(14):1141–50. https://doi.org/10.1080/09500340.2015.1021725.
25. Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V. Hacking commercial quantum cryptography systems by tailored bright illumination. Nat Photonics. 2010;4(10):686–9.
26. Kim T, Fiorentino M, Wong FN. Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer. Phys Rev A. 2006;73(1):012316.
27. Zhao Y, Qi B, Ma X, Lo HK, Qian L. Experimental quantum key distribution with decoy states. Phys Rev Lett. 2006;96:070502.
28. Shor PW, Simple PJ. Proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett. 2000;85:441–4.
29. Elkouss D, Leverrier A, Alléaume R, Boutros JJ. Efficient reconciliation protocol for discrete-variable quantum key distribution. In: Information theory, 2009. ISIT 2009. IEEE international symposium on. IEEE; 2009. p. 1879–83.
30. Ma X, Fung CHF, Lo HK. Quantum key distribution with entangled photon sources. Phys Rev A. 2007;76(1):012307.
31. Ali S, Saharudin S, Wahiddin M. Quantum key distribution using decoy state protocol. Am J Eng Appl Sci. 2009;2(4):694–8.

32. Steinlechner F, Trojek P, Jofre M, Weier H, Perez D, Jennewein T, et al. A high-brightness source of polarization-entangled photons optimized for applications in free space. Opt Express. 2012;20(9):9640–9.
33. Giustina M, Versteegh MAM, Wengerowsky S, Handsteiner J, Hochrainer A, Phelan K, et al. Significant-loophole-free test of Bell's theorem with entangled photons. Phys Rev Lett. 2015;115:250401.
34. Single quantum SNSPD spec sheet. 2017. http://www.singlequantum.com/wp-content/uploads/2017/07/Single-Quantum-Eos.pdf. Accessed 2017-10-17.
35. Ma X, Qi B, Zhao Y, Lo HK. Practical decoy state for quantum key distribution. Phys Rev A. 2005;72(1):012326.
36. Achilles D, Rogacheva E, Trifonov A. Fast quantum key distribution with decoy number states. J Mod Opt. 2008;55(3):361–73.
37. Bourgoin J, Meyer-Scott E, Higgins BL, Helou B, Erven C, Huebel H, et al. A comprehensive design and performance analysis of low Earth orbit satellite quantum communication. New J Phys. 2013;15(2):023006.
38. Personal communication with Dr. Zoran Sodnik. ESA/ESTEC. 2017.
39. Brochure for deployable solar panels from cubesatshop.com. 2016. http://www.cubesatshop.com/wp-content/uploads/2016/07/EXA-DSA-Brochure-1.pdf. Accessed 2017-10-17.
40. Aperture Optical Systems CubeSat telescope. 2017. http://www.apertureos.com/products/cube-sat. Accessed 2017-10-17.
41. Thorlabs dielectric filters. 2017. https://www.thorlabs.com/navigation.cfm?guide_id=2210. Accessed 2017-10-17.
42. Thorlabs polarizing beam splitters. 2017. https://www.thorlabs.de/newgrouppage9.cfm?objectgroup_id=739. Accessed 2017-10-17.
43. MPD PDM series data sheet. 2017. http://www.micro-photon-devices.com/Docs/Datasheet/PDM.pdf. Accessed 2017-11-04.
44. Anisimova E, Higgins BL, Bourgoin JP, Cranmer M, Choi E, Hudson D, et al. Mitigating radiation damage of single photon detectors for space applications. EPJ Quantum Technol. 2017;4(1):10.
45. Lim JG, Anisimova E, Higgins BL, Bourgoin JP, Jennewein T, Makarov V. Laser annealing heals radiation damage in avalanche photodiodes. EPJ Quantum Technol. 2017;4(1):11.
46. Falchi F, Cinzano P, Duriscoe D, Kyba CC, Elvidge CD, Baugh K, et al. The new world atlas of artificial night sky brightness. Sci Adv. 2016;2(6):e1600377.
47. Official site of the Visible Infrared Imaging Radiometer Suite (VIIRS) run by NASA and NOAA. 2017. https://jointmission.gsfc.nasa.gov/VIIRS.html. Accessed 2017-10-18.
48. Lamphar HAS, Kocifaj M. Light pollution in ultraviolet and visible spectrum: effect on different visual perceptions. PLoS ONE. 2013;8(2):e56563.
49. MODTRAN WebApp. 2017. http://modtran.spectral.com/modtran_home. Accessed 2017-11-07.
50. Yan F, Fosbury RA, Petr-Gotzens MG, Zhao G, Wang W, Wang L, et al. High-resolution transmission spectrum of the Earth's atmosphere-seeing Earth as an exoplanet using a lunar eclipse. Int J Astrobiol. 2015;14(2):255–66.
51. Luminance and brightness data for the full moon. 2009. http://spaceweather.com/swpod2009/13jan09/Perigee_moon_2009_01_11_corr.pdf. Accessed 2017-10-20.
52. Stephens GL, O'Brien D, Webster PJ, Pilewski P, Kato S, Li Jl. The albedo of Earth. Rev Geophys. 2015;53(1):141–63.
53. Zong Y. From candle to candela. Nat Phys. 2016;12(6):614.
54. Ren JG, Xu P, Yong HL, Zhang L, Liao SK, Yin J, et al. Ground-to-satellite quantum teleportation. Nature. 2017;549(7670):70–3.
55. Blue Canyon XACT data sheet. 2017. http://bluecanyontech.com/wp-content/uploads/2017/07/DataSheet_ADCS_08_F.pdf. Accessed 2017-10-17.
56. This value is expected for the Blue Canyon XB-1 spacecraft bus which is entirely compatible with our design. Personal communication with Josh Duncan. Blue Canyon Technologies. For the XB-1 bus specifications see. 2017. http://mstl.atl.calpoly.edu/~bklofas/Presentations/SummerWorkshop2012/Stafford_XB1.pdf. Accessed 2017-10-20.
57. Mason JP, Baumgart M, Rogler B, Downs C, Williams M, Woods TN, et al. MinXSS-1 CubeSat on-orbit pointing and power performance: the first flight of the Blue Canyon technologies XACT 3-axis attitude determination and control system. 2017. arXiv:1706.06967.
58. Meadowlark ferroelectric liquid crystal data sheet. 2017. http://www.meadowlark.com/store/data_sheet/Liquid%20Crystal%20-%20FLC%20Devices%20NEW.pdf. Accessed 2017-10-17.
59. Chandrasekara R, Durak K, Ling A. Tracking capacitance of liquid crystal devices to improve polarization rotation accuracy. Opt Express. 2017;25(17):20363–8.
60. Schindler W, Killmann W. Evaluation criteria for true (physical) random number generators used in cryptographic applications. In: CHES. vol. 2. Berlin: Springer; 2003. p. 431–44.
61. Picoquant TimeHarp 260 data sheet. 2017. https://www.picoquant.com/images/uploads/downloads/timeharp260.pdf. Accessed 2017-10-17.
62. Personal communication with Dr. Michael Schlagmueller. Swabian Instruments. 2017.
63. Endurosat CubeSat S-band/UHF communication module data sheet. 2017. https://www.endurosat.com/modules-datasheets/COMM_User_Manual_Rev1.6.pdf?x65766. Accessed 2017-10-27.
64. CubeSat design specification rev. 13 by California Polytechnic State University. 2017. http://www.cubesat.org/s/cds_rev13_final2.pdf. Accessed 2017-10-17.
65. NanoRacks CubeSat Deployer (NRCSD interface control document. 2017. http://nanoracks.com/wp-content/uploads/NanoRacks-CubeSat-Interface-Control-Document-CubeSat-Guide.pdf. Accessed 2017-11-02.
66. Spaceflight launch company. 2017. http://spaceflight.com/schedule-pricing/#pricing. Accessed 2017-10-17.
67. CubeSatShop BA0x high energy density battery array Pegasus Class BA01/D. 2017. https://www.cubesatshop.com/wp-content/uploads/2016/11/EXA-BA0x-Brochure.pdf. Accessed 2017-10-27.
68. Bailey S, Raffaelle R. Space solar cells and arrays. In: Handbook of photovoltaic science and engineering. 2nd ed. 2011. p. 365–401.
69. [3]SatImaging. 2017. http://propagation.ece.gatech.edu/ECE6390/project/Sum2015/team3/PowerSystem.html. Accessed 2017-10-27.
70. Elterman L. UV, visible, and IR attenuation for altitudes to 50 km, 1968: environmental research papers. United States Air Force, Office of Aerospace Research, Air Force Cambridge Research Laboratories, Optical Physics Laboratory; 1968. https://books.google.at/books?id=Vt1VAQAACAAJ.

71. RoboDIMM, the ING's new seeing monitor. 2017. http://www.ing.iac.es/PR/newsletter/news7/ins7.html. Accessed 2017-10-17.
72. Oltrogge D, Leveque K. An evaluation of CubeSat orbital decay. In: 25th annual AIAA/USU conference on small satellites. 2011.
73. Ginet GP, Madden D, Dichter BK, Brautigam DH. Energetic proton maps for the South Atlantic anomaly. In: Radiation effects data workshop, 2007 IEEE. IEEE; 2007. p. 1–8.
74. Montenbruck O, Ramos-Bosch P. Precision real-time navigation of LEO satellites using global positioning system measurements. GPS Solut. 2008;12(3):187–98.
75. Ho C, Lamas-Linares A, Kurtsiefer C. Clock synchronization by remote detection of correlated photon pairs. New J Phys. 2009;11(4):045011.
76. Kirschner M, Weigel M, Kahle R, Kahr E, Choi P, Letsch K, et al. Orbit precision analysis of small man-made space objects in LEO based on radar tracking measurements. DLR website. 2012.
77. Prochazka I, Kral L. Atmospheric contribution to the laser ranging jitter. In: Proc. 13th int. laser ranging workshop. 2002.
78. AN513 Jitter attenuation: choosing the right phase-locked loop bandwidth. 2017. https://www.silabs.com/documents/public/application-notes/AN513.pdf. Accessed 2017-11-04.
79. Ashby N. Relativity in the Global Positioning System. Living Rev Relativ. 2003;6:1.
80. Gigov N. Quantum key distribution data post-processing with limited resources. Towards Satellite-Based Quantum Communication [mathesis]. 2013.
81. On-board computer brochure from Cubesatshop. 2017. https://www.cubesatshop.com/wp-content/uploads/2016/06/iOBC-Brochure-v1.pdf. Accessed 2017-10-17.
82. CubeSatShop one-stop webshop for CubeSats and Nanosats. 2018. https://www.cubesatshop.com/. Accessed 2018-02-15.
83. Joshi SK, Pienaar J, Ralph TC, Cacciapuoti L, McCutcheon W, Rarity J, et al. Space QUEST mission proposal: experimentally testing decoherence due to gravity. 2017. arXiv:1703.08036.