Mendes et al. *EPJ Quantum Technology* (2024) 11:48
https://doi.org/10.1140/epjqt/s40507-024-00254-w

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Optical payload design for downlink quantum key distribution and keyless communication using CubeSats

Pedro Neto Mendes[1,2], Gonçalo Lobato Teixeira[2,3], David Pinho[1], Rui Rocha[2], Paulo André[1,2], Manfred Niehus[2,4], Ricardo Faleiro[2], Davide Rusca[5,6,7] and Emmanuel Zambrini Cruzeiro[1,2*]

*Correspondence:
emmanuel.cruzeiro@lx.it.pt
[1]Departamento de Engenharia Electrotécnica e de Computadores, Instituto Superior Técnico, Av. Rovisco Pais, 1049-001, Lisbon, Portugal
[2]Instituto de Telecomunicações, Av. Rovisco Pais, 1049-001, Lisbon, Portugal
Full list of author information is available at the end of the article

Abstract

Quantum key distribution is costly and, at the moment, offers low performance in space applications. Other more recent protocols could offer a potential practical solution to this problem. In this work, a preliminary optical payload design using commercial off-the-shelf elements for a quantum communication downlink in a 3U CubeSat is proposed. It is shown that this quantum state emitter allows the establishment of two types of quantum communication between the satellite and the ground station: quantum key distribution and quantum keyless private communication. Numerical simulations are provided that show the feasibility of the scheme for both protocols as well as their performance. For the simplified BB84, a maximum secret key rate of about 80 kHz and minimum QBER of slightly more than 0.07% is found, at the zenith, while for quantum private keyless communication, a 700 MHz private rate is achieved. This design serves as a platform for the implementation of novel quantum communication protocols that can improve the performance of quantum communications in space.

Keywords: CubeSat; Quantum key distribution; Quantum keyless private communication

1 Introduction

1.1 Long distance quantum communication

In quantum communication, physical systems are exploited to encode and transfer information between parties. Thanks to C. Shannon [1] and to the second quantum revolution, physicists began to develop a new understanding of what information is. This has led to newly emerging technological applications, such as quantum communication, quantum computation, quantum sensing, and quantum thermodynamics [2, 3].

Quantum communication promises unconditional security based on the laws of nature without needing to impose requirements on the computational power available to an eavesdropper, which might, at first sight, seem surprising. The most celebrated variant of quantum communication is Quantum Key Distribution (QKD), which is proven to achieve, under certain assumptions, such unconditional security. The most impres-

sive demonstrations of QKD were implementations of so-called device-independent QKD protocols, which allow unconditional security with no assumptions about the inner workings of the devices used to distribute the key. These demonstrations were only performed very recently [4–6], almost 40 years after the proposal of the first QKD protocol, the BB84 [7].

QKD has seen considerable progress in the last decade, as illustrated by the development of commercial systems [8] since the early 2000s. Nevertheless, the available devices carry a glaring limitation: the rate-distance trade-off. Even with low-loss fibers, commercial QKD systems are limited to a few hundred kilometers for a useful key rate [9, 10]. Therefore, in terms of long-distance telecommunications, QKD is still in its infancy [11]. There are two main approaches to extending QKD to distances of hundreds to thousands of km: quantum repeaters and space-based QKD. This work focuses on the latter, by implementing the simplified BB84 protocol [12] between a nanosatellite in Low-Earth Orbit (LEO) and a ground station.

Although it is the most popular form of quantum communication, the assumptions behind the security proofs of QKD are very strong, as they consider a wide generality of possible attacks by a malicious agent. In fact, these assumptions may be unnecessarily demanding for satellite-to-ground station communication, due to physical limitations on Eve's ability to completely intercept and resend information without being detected. A more reasonable solution, in this case, is quantum keyless communication [13], whereby information is directly sent over the quantum channel, encoded in the quantum states of light. There is no key generation in this case. Therefore a design that can serve as a quantum state emitter both for QKD, and to implement Quantum Keyless Private Communication (QKPC) is proposed.

In this work, the initial design of an optical payload for a 3U CubeSat downlink is described. The optical payload consists of a source of quantum states which may be used to both implement the simplified BB84 and QKPC. To this end, a compact version of the usual simplified BB84 setup [12], adapted to fit in the restricted volume and power budget of the nanosatellite, is designed. An implementation of the preliminary design is proposed, taking into account optical, mechanical, and electrical design, along with celestial mechanics considerations, and realistic simulations of both protocols are provided.

This proposal is innovative compared to other proposals for nanosatellite quantum communication for its versatility: it may implement various novel quantum communication protocols, which is demonstrated by its ability to implement QKD and QKPC. In other words, this solution serves as a starting point for future research in novel quantum communication protocols for space-based applications. The main purpose of this article is to propose a platform for satellite quantum communication experiments beyond quantum key distribution. Additionally, it is shown that the quantum state emitter can fit inside a 3U CubeSat, using only commercial off-the-shelf elements.

1.2 Satellites for quantum communication - overview

In terms of satellite communication, QKD is still in its infancy [14, 15]. In 2003, an experiment in the Matera Laser Ranging Observatory (Italy) demonstrated the feasibility of sending single photons through the atmosphere in a ground-LEO-ground link [16]. This showed that a global QKD network may indeed be created in the future with a mix of satellite and ground nodes. Japan and China both created road maps to develop this technology which led to the launch of SOCRATES [17] and Micius [18] in 2014 and 2016 respectively.

SOCRATES is a Japanese micro-satellite in LEO orbit, weighing 48 kg, measuring 496 × 495 × 485 mm, and whose goal is to establish a standard micro-satellite bus technology applicable to missions of various purposes. Inside it, SOTA (Small Optical TrAnsponder), the small and light (6 kg weight, 17.8 × 11.4 × 26.8 cm) optical quantum-communication transmitter, allowed to perform various experiments that culminated in LEO-to-ground quantum communication in 2017 [17].

Micius is a Chinese satellite in LEO orbit, weighing 635 kg part of QUESS, a proof-of-concept mission designed to facilitate quantum optics experiments over long distances to allow the development of quantum encryption and quantum teleportation technology. The satellite consists of two transmitters. Transmitter 1, weighing 115 kg, incorporates eight laser diodes and a BB84 coding module to facilitate QKD through preparation and measurement. The second transmitter, weighing 83 kg, is specifically designed to distribute quantum entanglement from the satellite to two distinct ground stations. Within a year of the launch, three key milestones for a global-scale quantum communication network were achieved: satellite-to-ground decoy-state QKD with KHz rate over a distance of up to 1200 km; satellite-based entanglement distribution to two locations on Earth separated by $\approx$ 1200 km and the subsequent Bell test, allowing possible effective link efficiencies through satellite of 12-20 orders of magnitudes greater than direct transmission; ground-to-satellite quantum teleportation [18].

1.3 Quantum CubeSats state of the art

Recently, the focus on space-based quantum communication shifted to smaller satellites, specifically CubeSats, which are the most common type of nanosatellite. In the last decade, the use of CubeSats has grown considerably [19]. These systems are interesting because they are cost-effective, are easier and faster to develop, and can ride along in rockets designed for different payloads. This has allowed companies, non-profit organizations, and even educational institutions to participate in their development and launch.

This contributed to the creation of various research projects to develop CubeSats for quantum communication all around the world. These projects started with path-finders works like CQuCoM [20], followed by specific missions. Germany started the QUBE project [21] to develop a 3U CubeSat for downlink QKD implementation. In France, the Grenoble University Space Center is leading the development of NanoBob, a 12U CubeSat to demonstrate the feasibility of quantum communication over a distance of 500 km. NanoBob [22, 23] is expected to launch in 2024 and Grenoble University Space Center is already engaged in a more ambitious project, financed by the French Space Agency CNES and with TAS-F as the leading partner, that investigates the requirements and specification of a future Quantum Information Network that includes one or more Space links. Companies are also collaborating with academia in satellite-based QKD projects, like ROKS mission [24], a 6U CubeSat with a 1/3U size optical module employing a 4-state BB84 with Weak Coherent Pulse (WCP), set to launch in 2024. Other missions include QEYSSat [25] and QUARC [26], aiming to demonstrate the feasibility of quantum links in uplink and downlink configuration.

For now, efforts for space-based quantum communication have focused mostly on LEO orbits. This is because of the relative ease of reaching the orbit, the possibility to cover the entire planet in a matter of hours with a single satellite (rapid round trip and many orbit inclination options), and the more relaxed link budget making it easier to develop a

communication system. Nevertheless, this type of orbit has its limits as the passage over a ground terminal is limited to just a few minutes of effective link (lower communication window) and the tracking system has to be more precise. Recently, the first experimental single-photon exchange with a Medium-Earth Orbit (MEO) satellite at 7000 km was realized [27] followed by a feasibility study for quantum communication at Geostacionary Orbit (GEO) orbits (allowing 24-hour link coverage) [28].

These approaches to quantum communication in space focus on QKD and, to our knowledge no other quantum communication protocols have been proposed.

2 Concept and implementation

A versatile CubeSat design that allows for various types of quantum communication schemes is proposed. In this section, two protocols that can be implemented with the design are described. The first protocol is a recent variant of the BB84 protocol, called the simplified BB84 [12]. The second is a QKPC scheme for keyless secure communications [13]. Then, the setup realizing the protocols is described, and a Size, Weight, and Power analysis of the preliminary design is conducted to validate it.

2.1 Protocols

In polarization-based BB84, Alice sends a number of states picked from the following qubit basis,

$$
\begin{aligned}
&|\mathrm{H}\rangle, |\mathrm{V}\rangle,\\
&|\mathrm{D}\rangle := \frac{1}{\sqrt{2}}\big(|H\rangle + |V\rangle\big), \qquad |\mathrm{A}\rangle := \frac{1}{\sqrt{2}}\big(|H\rangle - |V\rangle\big),\\
&|R\rangle := \frac{1}{\sqrt{2}}\big(|H\rangle + i|V\rangle\big), \qquad |L\rangle := \frac{1}{\sqrt{2}}\big(|H\rangle - i|V\rangle\big),
\end{aligned} \tag{1}
$$

where $|.\rangle$ are the polarization states. Taking advantage of a different subset of the above states, several variants of BB84 exist. The original BB84 used four states, and a more noise-robust version exists with six states, the so-called six-state BB84 protocol [29, 30]. Moreover there exists variants which uses only three states (two for the computational basis and one for the monitoring basis) which keep the secret key rate almost unchanged with respect to the original BB84 but allow for a simpler implementation [31–35]

A naive implementation of BB84 using WCPs is not secure due to the photon number splitting attack [36, 37]. To mitigate this problem, one uses decoy states, i.e. states with different intensities which allow the users to determine more easily the presence of an eavesdropper [38–43]. In [44, 45], a comparison was made between BB84 protocols taking advantage of decoy states. Following these works we found that the best protocol in terms of security and experimental simplicity for our purpose is the simplified BB84 protocol, which uses three states and one decoy and allows for a simpler receiver scheme.

A version of the simplified BB84 protocol with one decoy was first implemented in polarization in [12], in the following, the idea of the protocol is summarized. For the computational basis Z, the protocol runs exactly as the original BB84. However, in the monitoring basis X, Alice prepares only $|D\rangle$, while Bob's measurement corresponds to a projection onto $|A\rangle$. In this protocol, only three preparations and three detections are necessary. The detections can be implemented with two detectors, as in [12].

The protocol is similar to the original BB84,

1. *State preparation*: random encoding in bases X and Z with respective probabilities p_X^A and $p_Z^A = 1 - p_X^A$. In the Z basis, Alice emits $|H\rangle$ and $|V\rangle$ uniformly, while in the X basis she always emits $|D\rangle$. The mean photon number of the pulses is chosen randomly between two values μ_1 and μ_2 with probabilities p_{μ_1}, p_{μ_2}.
2. *Measurement*: Bob performs measurements X and Z with respective probabilities p_X^B and $p_Z^B = 1 - p_X^B$. He records each basis and measurement outcome.
3. *Basis reconciliation*: Alice and Bob announce their basis choices for each detection event. Events from the Z basis are used to generate the raw key, while those from the X basis are used to estimate the eavesdropper's potential information. After collecting a number of n_Z raw key bits, they proceed to the next step.
4. *Error correction/Information reconciliation*: Alice and Bob employ an error correction algorithm on their block of n_Z bits, during which $\lambda = f \cdot n_Z \cdot h(Q_Z)$ bits are disclosed, where f is the reconciliation efficiency, $h(x)$ the binary entropy, and Q_Z the error rate. The procedure succeeds with probability $1 - \epsilon_{\text{corr}}$. After $k = n_Z^*/n_Z$, where both n_Z^* and n_Z are chosen by the users, they proceed to the final step.
5. *Privacy amplification*: Alice and Bob apply privacy amplification on a block of size n_Z^* to obtain a secret key of l bits (Secret Key Length (SKL)), where

$$l = \left\lfloor s_{Z,0} + s_{Z,1}\left[1 - h(\phi_Z)\right] - \lambda_{\text{EC}} - 6\log_2\left(\frac{\alpha}{\epsilon_s}\right) - \log_2\left(\frac{2}{\epsilon_c}\right)\right\rfloor, \tag{2}$$

where $s_{Z,0}$ is the number of vacuum events, $s_{Z,1}$ is the number of single photon events, and ϕ_Z is the phase error rate in the sifted Z basis. ϵ_c and ϵ_c are prescribed security parameters, the correctness, and secrecy of the key, respectively. λ_{EC} is an estimate of the number of bitsrevealed during the error correction. $\alpha = 19(21)$ for one (two) decoy(s). Finally, $h(\cdot)$ is the binary entropy function.

The numbers of vacuum and single-photon events $s_{Z,0}$, $s_{Z,1}$ and the phase error rate ϕ_Z can be evaluated as described in the SatQuMa documentation [46]. For the evaluation of λ_{EC}, method 1 is used. Statistical fluctuations are evaluated using the Chernoff bound.

The Secret Key Rate (SKR) is simply the SKL divided by the duration of the transmission $T_{\text{trans.}}$,

$$\text{SKR} = \frac{\text{SKL}}{T_{\text{trans.}}} \tag{3}$$

For the Quantum Bit Error Rate (QBER) of the X basis, [35],

$$Q_X = \frac{1}{2}\frac{P_Z^A P_Z^B}{n_Z}\left[\frac{n(A,D)}{P_X^A P_X^B} + \max\left(0, \frac{n(A,D)}{P_X^A P_X^B} + \frac{n(A,Z)}{P_Z^A P_X^B} - \frac{n(Z,D)}{P_X^A P_Z^B} + 2\frac{n_Z}{P_Z^A P_X^B}\right)\right] \tag{4}$$

is used, where $P_{X(Z)}^{A(B)}$ is the probability of Alice (Bob) sending (measuring) a bit in the X (Z) basis. n_Z is the total number of detected bits in the Z basis and the $n(b,a)$ is the number of detections when Alice sends state a and Bob measures state b.

The QKPC protocol, proposed in [13], is based on the classic wiretap model, first proposed by Shannon in 1949 [47] and later rigorously defined by Wyner in 1975 [48] where the author introduced the concept of secret capacity (maximum communication rate at which legitimate users can communicate securely in the presence of an eavesdropper). In the wiretap model, Alice wants to send a message to Bob over a communication channel but a wiretapper (Eve) is listening to the channel. The goal is to encode the data in such a way that maximizes the wiretapper's confusion making it impossible for her to recover the message sent.

The QKPC protocol consists of the following steps:

1. *Encoding*: Alice selects a n-bit codeword X^n for her secret message M. The secrecy depends on the encoder, which is characterized by the rate $R = k/n$, where k is the number of secret bits, the error probability ϵ_n, and the information leakage measured by an information-theoretical measure denoted δ_n.
2. *State preparation*: Alice prepares a coherent state modulated by the random variable $X \in \{0, 1\}$, where $X = 0$ with probability q. The On-Off Keying (OOK) states are the vacuum state $|\alpha_0\rangle$ and a weak coherent state

$$|\alpha_1\rangle = e^{-|\alpha_1|^2/2} \sum_{n=0}^{\infty} \frac{\alpha_1^n}{(n!)^{1/2}} |n\rangle \tag{5}$$

   The probability q needs to be optimized depending on the assumptions at the detection and the physical propagation channel.
3. *Measurement*: After n transmissions, Bob receives B^n and Eve E^n. Bob obtains Y^n by estimating his received coherent state. Eve can use the best quantum detection strategy to obtain Z^n.
4. *Decoding*: Bob and Eve send their estimated received states to the decoder.

The choices of encoder and decoder are assumed to be public. The values of ϵ_n and δ_n depend on these choices.

According to wiretap theory, even if the eavesdropper is computationally unbounded, then

$$\lim_{n \longrightarrow \infty} \epsilon_n = \lim_{n \longrightarrow \infty} \delta_n = 0 \tag{6}$$

as long as R is an achievable rate. This means the error probability and information leakage towards Eve can be made arbitrarily low. See [49, 50] for exact definitions of the parameters ϵ_n and δ_n.

2.2 QKPC protocol security

For the QKPC protocol, when considering satellite and ground station space links some physically motivated limitations on Eve's power can be naturally assumed, like the impracticality of a successful and unnoticed intercept and resend attack over free space. Under such limitations, an eavesdropping attempt can be assumed to exist only for a fraction of the communicated signal, implying that the model used to prove security against Eve may be relaxed, say to a quantum wire-tap model. This in turn opens the door to physical-layer security as a legitimate alternative to QKD for establishing secure satellite-to-ground quantum communication [13, 51, 52]. QKPC allows for much higher rates than QKD with

current technology [13] and even allows daylight operation, which is presently impractical for QKD.

A single-mode free-space quantum bosonic channel is assumed, following [13]. The efficiency of the channel is η. The channel degradation is described by a parameter $\gamma \in (0,1)$. Therefore the efficiency of Eve's channel is $\gamma\eta$. Bob is assumed to have a single photon detector with limited efficiency (included in η) and dark count probability p_{dark}. The stray light is modeled as a Poisson photon number distribution with average $\eta_0\Delta$, where η_0 is the optical loss between the telescope input lens of the receiver and the detector, and Δ is the average number of noise photons for a given collection angle and the given frequency and time window, see Appendix D in [13].

The conditional probabilities of Bob detecting y given that Alice has sent x are given by

$$\epsilon_0 = (1 - p_{\text{dark}})e^{-\eta_0\Delta}, \qquad \epsilon_1 = (1 - p_{\text{dark}})e^{-(\eta\mu+\eta_0\Delta)}, \tag{7}$$

where $\mu = |\alpha_1|^2$.

Eve is assumed to perform an optimal quantum detection, which leads to an optimal error probability ϵ^*, given explicitly by

$$\epsilon^*(\gamma) = \frac{1 - \sqrt{1 - 4q(1-q)e^{-\eta\gamma\mu}}}{2} \tag{8}$$

The private capacity of OOK is then

$$C_P(\gamma) = \left[h\big(\epsilon^*(\gamma)\big) + h\left(\frac{\epsilon_0 + \epsilon_1}{2}\right) - \frac{h(\epsilon_1) + h(\epsilon_0)}{2} - 1 \right]_+ \tag{9}$$

where $[]_+$ is the positive part and $h(\cdot)$ is the binary Shannon entropy.

Finally, the Devetak-Winter rate for this protocol is given by

$$R_{\text{DW}}(\gamma) = I(X,Y) - \chi(X;E|\gamma), \tag{10}$$

where $I(X;Y)$ is the Shannon mutual information of Alice's choice of the input probability, measured by a photon counting detector. $\chi(X;E|\gamma)$ is the Holevo bound for Eve, see [13].

Finally, the rate reduces to

$$R_{\text{DW}} = \left[h\left(\frac{\epsilon_0 + \epsilon_1}{2}\right) - \frac{h(\epsilon_1) + h(\epsilon_0)}{2} - h\left(\frac{1 + \epsilon(\gamma)}{2}\right) \right]_+ \tag{11}$$

2.3 Experimental concept

The satellite is controlled by an onboard computer that manages the satellite systems (payload, power, etc.), handles data storage and communication, and monitors the health status of the satellite. This system is represented in Fig. 1 as an Field-Programmable Gate Array (FPGA) and while a detailed study on how to optimize the on-board computer will be left for future work, an initial estimation of its parameters is used based on information from [53], as it has a similar system. Another solution can be found in [23] by using a commercial Zync-based on-board computer.

A Quantum Random Number Generator (QRNG) is used to supply a random seed for the choice of basis. The IDQ20MC1 (QRNG chip for space applications) from ID Quantique meets all the requirements making it a viable option. Additionally, a GPS module,

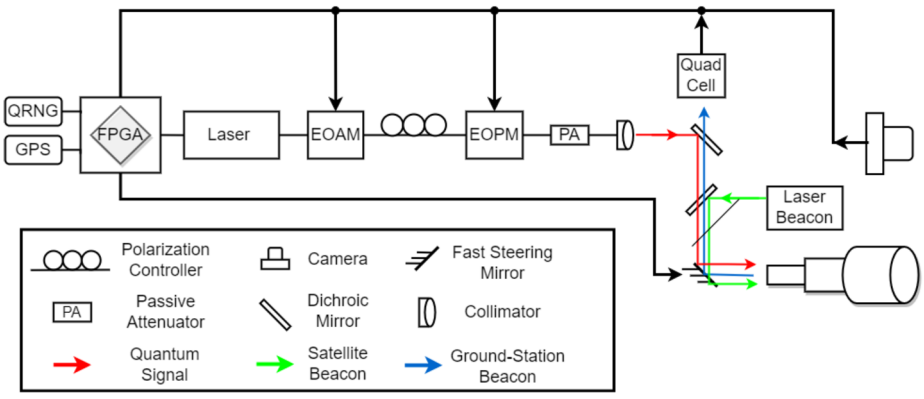

Figure 1 Setup capable of implementing both the QKPC and the Simplified BB84 in a 3U Cubesat

ACC-GPS-NANO from Accord, is used for time stamping and, as it ensures an accurate determination of orbital position and time, it is also used for the coarse step of the pointing system.

The setup includes a gain-switched distributed feedback (Distributed-Feedback (DFB)) laser source from Anritsu, specifically the DFB 1550. Gain-switched lasers are essential to ensure phase randomization of the initial light pulses, as referenced in studies by [54] and [55]. This source provides coherent phase-randomized pulses at 1550 nm with a pulse duration of 93 ps, triggered at 1 GHz with mW of power. This wavelength is chosen for its easy integration into a fiber-based quantum network, availability of off-the-shelf components due to terrestrial-fiber developments, and high transmittance in the atmosphere [56].

The laser is directly coupled into an electro-optic amplitude modulator (Electrooptic Amplitude Modulator (EOAM)), specifically the LN81S-FC from Thorlabs, to encode decoy states via amplitude modulation. A variable waveplate from Phoenixphotonic (Polarization Controller (PC)) prepares the state polarization, allowing it to be rotated to any of the three linearly polarized states required for the simplified BB84 protocol. This is achieved by a polarization switch, the PSW-LN-0.1-P-P-FA-FA from IxBlue. Finally, the pulses are attenuated by a passive attenuator, the FA25T from Thorlabs, and exit the fiber through a collimator, the RC04APC-P01 from Thorlabs.

Compared to Grunenfelder *et al.*, this setup was simplified by removing the polarization controller and the high-birefringence fiber after the Electrooptic Polarization Modulator (EOPM), as they can be delegated to the ground station, and instead of a variable attenuator, a passive one is used. Such modifications are important for a CubeSat design, for which the dimension and electrical power consumption must be minimized. The first modification reduces the dimensions of the setup, while the second reduces its electrical consumption. The system setup is shown in Fig. 1.

A pointing subsystem is added which is necessary for aligning the CubeSat with the ground station. The setup proposed is inspired by the CubeSat Laser Infrared CrosslinK Mission (CLICK) system [57] due to its tested ability to achieve a pointing error below 1 μrad with optical data rates exceeding 20 Mbps while adhering to our Size, Weight and Power (SWaP) constraints. The satellite pointing system incorporates a telecom wavelength (1310 nm) from Anritsu, DFB 1310, for downlink alignment and classical data

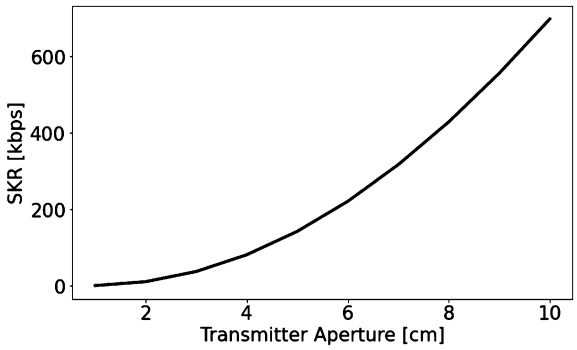

Figure 2 Optimized SKR at zenith for different values of the transmitter aperture D_T, for the simplified BB84

transmission purposes. The system comprises a coarse pointing stage where the satellite and the ground station align with each other using provided ephemeris information and guaranteed by the Altitude Determination and Control System (ADCS) [58] and GPS. By detecting the beacon signal with a wide field of view camera, MyBlueFox from Matrix Vision, the satellite can adjust its attitude to enable the narrow field of view Quad Cell, PDQ30C from Thorlabs, to acquire the signal. This marks the initiation of the fine-pointing stage, where tracking is performed using a fast steering mirror from Mirrorcle. The option with a mirror diameter of 2.4 mm, a resonant frequency of around 860 Hz, and a maximum tilt angle of −6° to +6° should provide the necessary tracking requirements. The various optical signals are of different wavelengths and are separated or combined into the correct optical paths using dichroic mirrors from Thorlabs.

In a preliminary test, piezoelectric motored mirrors, a CMOS camera, and a closed-loop control system were used to test the satellite pointing. The camera captured laser signals at 635 and 532 nm wavelengths, an image processing algorithm determined the centroids of these signals and a PID controller ensured a swift and seamless response to pointing errors. The system tracks a dynamic reference with precision up to 3.4 mrad. The preliminary pointing and tracking control design will iterated in an upcoming free-space demonstration.

For classical data transmission, the system utilizes classical OOK. The pointing signal is modulated and sent to the ground station.

2.4 Optical payload design

2.4.1 CubeSat description and characteristics

CubeSats are nanosatellites composed of 10 cm × 10 cm × 11.35 cm modules. Each module is referred to as 1U. For a 3U CubeSat, the components must fit a $10 \times 10 \times 32\ \text{cm}^3$ cuboid, have a total mass of less than 4 kilograms, and consume at most 21 Wh per orbit [53]. The 21 Wh are estimated using $30 \times 30\ \text{cm}^2$ off-the-shelf solar panels.[1]

In Table 1, the volume (in ml), the weight (g), and the power consumption (mW), of the commercial off-the-shelf Components, are specified, (Size, weight, and Power analysis).

The primary goal of the SWaP analysis was to proactively evaluate the fit of the components within the 2U of the CubeSat. By examining their physical dimensions, volume, and

[1] Values taken from https://www.cubesatshop.com/wp-content/uploads/2016/07/EXA-DSA-Brochure-1.pdf.

Table 1 SWaP analysis of the proposed preliminary design for a 3U CubeSat

Item	Volume (ml)	Weight (g)	Power (mW)
FPGA	110	94	500
QRNG	1	-	83
GPS	49	45	500
Laser source	24	270	800
EOAM	19	180	650
EOPM	33	180	900
Variable Waveplate	2	150	700
FC/APC Collimator	13	60	-
Passive Attenuator × 2	4	20	-
Connector × 2	13	20	-
Alice payload	268	1019	4133
Quad Cell	4	30	-
Camera + Lens	109	390	2500
Mems mirror	3	30	85
Laser source	24	270	800
Dichroic Mirror × 2	1	40	-
Tracking payload	141	760	3385
Telescope	119	400	-
Payload	528	2179	7518
ADCS	500	900	2000
UHF + S-band	250	114	6000
Antennas	70	100	60
Batteries	100	200	-
Solar panels	-	450	-
Platform	920	1764	8060
Total	1448	3943	15,578
3U Maximum	3200	4000	

relevant specifications, the goal was to determine if the components could be seamlessly integrated into the allocated space for the optical payload. This evaluation is crucial as it helps to avoid potential design iterations and modifications in the later stages of development and guides the component selection. Although these values were taken or estimated from available datasheets and may not be exact, they offer a strong basis for making informed decisions and guiding the subsequent design phases.

An estimate of the SWaP characteristics of the system outside the payload (platform section of Table 1) and the telescope was also done based on similar works [53].

This optical system (payload) is divided into two parts, the Alice payload, and the tracking payload.

The Alice payload will generate and encode the quantum states. These will then be sent to the telescope. As seen in Table 1, this subsystem's devices will only take a fraction of the total available volume. As it has most of the active components (lasers and modulators), it consumes a significant part of the power budget. Nevertheless, it only needs to be turned on during the communication window when the alignment with the ground station is guaranteed. This results in energy consumption within the mission budget.

The tracking payload houses the necessary components to guarantee a pointing error sufficiently small for the mission's success. This part of the setup occupies a bigger volume and a significant fraction of the power budget due to the use of a wide field-of-view camera but it is still below the total values available.

Finally, to transmit the optical signals, a telescope is necessary. To choose the aperture size for the emitter telescope, the secret key rate for the simplified BB84 as a function of

the aperture was estimated, Fig. 2. This was done for a fixed value of the aperture of the receiver's telescope.

A 4 cm aperture is chosen to deal with the restrictions of the 3U CubeSat. For a larger CubeSat e.g. 6U or 12U, a larger aperture could be considered to increase the rates as shown in Fig. 2. It can be seen that for an aperture of 10 cm one can achieve a SKR of 700 kbps.

This takes a significant part of the remaining available volume but the design is still within the limit. The SWaP analysis with the chosen commercial off-the-shelf components demonstrates that the payload design is ready for its next stage: the custom design of optoelectronic and mechanical components, the miniaturization, and prototyping.

2.4.2 Classical communication

In Sidhu et al. [59], an estimation of classical communication cost and data storage requirements can be found.

Large satellites can work in the X and K bands, with frequencies of the order 10–40 GHz, which can use efficient modulations for communication rates of several Gbps [60]. Due to their size restrictions, CubeSats are much more limited with their typical bands being UHF, S, X, and Ka. The most mature bands used for CubeSat communication are VHF and UHF frequencies but there has been a shift in recent years towards S and X, with Ka being NASA's intended band for future small satellite communications. The move to higher frequency bands has been driven by a need for higher data rates with typical numbers being around in the dozens of kbps. [61]

It is possible to supplement radio communication using classical optical communication. Recently, a laser-based C2G (CubeSat-to-Ground) link from an LEO 1.5U CubeSat at a 450 km altitude to an optical ground station was established [62]. This communication link achieved a data rate of up to 100 Mbps with bit error rates near 10^{-6}. Since, pointing and acquisition are major problems for free-space optical communications, a hybrid RF-and-optical approach is introduced in [63], where CubeSats are used as relay satellites between the GEO satellites and the ground station using both RF and optical links.

As the system already has a laser link to the ground station through the pointing beam, it can use on-off keying to transmit information. CLICK-A, with a similar system, is expected to achieve a greater than 10 Mbps data downlink from spacecraft at an altitude of approximately 400 kilometers, to a 28-centimeter telescope on the ground [64]. The final system would then use a hybrid RF-and-optical approach as has been shown in [63].

3 Results

This section showcases the results from simulations of both communication protocols in realistic scenarios, followed by a direct comparison between them. The aim is to illustrate their performance differences.

3.1 Losses

For this analysis, three main types of losses are considered, geometric losses, atmospheric losses, and intrinsic system efficiency. Geometric losses appear from the limited receiver aperture to catch the incoming beam spread through divergence. Atmospheric losses can manifest in various forms, such as scattering, absorption, and turbulence. Intrinsic losses correspond to beam misalignment and internal losses inherent to the optical payload (e.g.

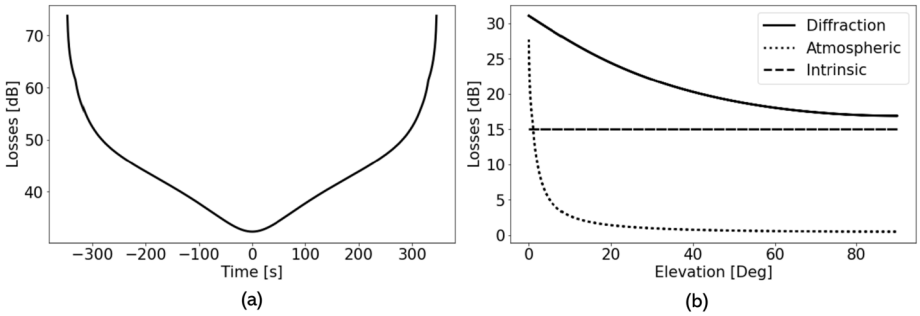

Figure 3 Estimated losses for the setup. The geometric losses are estimated using the parameters in Table 2. A conservative value of 15 dB for the intrinsic losses is chosen. For the atmospheric losses, realistic data provided with the SatQuMA toolbox is used. (a) Optical losses as a function of time for the chosen orbit. At time t = 0, the satellite is above the ground station at 90° of elevation (zenith). (b) Loss contributions from the different sources with respect to the elevation angle

optical components insertion loss and single-photon detectors efficiency). To detect the signal (single-mode), single-mode detectors are considered and although using these detectors is difficult, recent results show promising technologies with larger detection areas to overcome this challenge [65]. The analysis describes the total channel's loss throughout a satellite overpass through the zenith, Fig. 3.a, where the satellite's trajectory starts and ends at the horizon level (0° of elevation), and reaches a maximum elevation of 90° at $t = 0$. The contribution of all types of loss for each value of the satellite's elevation is described in Fig. 3.b.

The primary factor that limits the optical losses is the diffraction loss, which, throughout the trajectory, ranges from 17 dB to 31 dB. At low elevations, the atmospheric loss is at the highest effect and starts to decrease exponentially with the elevation reaching 3 dB at approximately 9° of elevation. For the analysis of Bob's intrinsic loss, it was chosen a conservative of 15 dB.

The main factor for atmospheric losses is the transmissivity of the chosen wavelength. However, for some applications, there can be slight benefits from a different wavelength due to pollution or weather conditions. The SatQuMA toolbox provides realistic data for an 850 nm signal used in the analysis. The atmospheric losses can be evaluated also for 1550 nm using software such as MODTRAN [66] and libradtran [67], which is left for future work as the objective here is only to validate the design under realistic conditions, and the atmospheric transparencies for 850 nm and 1550 nm allow for transmission close to 1 Gbps using classical optical communication [68]. As shown in [69], some advantages for the 1550 nm choice can be found as atmospheric turbulence has less impact, and the coherence length is longer. While these are not major advantages, they corroborate the choice to use this wavelength

3.2 Operation parameters

In Table 2, all the parameters used for the numerical simulations of the quantum communication protocols are presented.

The satellite will orbit in LEO and it will be considered that no communication is possible below 10°of elevation, a regime where the atmospheric losses become much more important. For the quantum communication signal, a wavelength of 1550 nm is used for

Table 2 Parameter values for the communication system simulations

Parameter	Symbol	Value
Orbit height	h	500 km
Minimum Transmission Elevation	θ_{min}	10°
Transmitter aperture diameter	D_T	0.04 m
Receiver aperture diameter	D_R	0.7 m
Beam waist	ω_0	0.02 m
Wavelength	λ	1550 nm
Offset angle of satellite orbital plane	ξ	0
Correctness parameter	ϵ_C	10^{-15}
Secrecy parameter	ϵ_S	10^{-9}
Intrinsic Quantum Bit Error Rate	QBER_I	0.001
Extraneous count probability	P_{EC}	10^{-8}
After pulse probability	P_{AP}	0.001
Source repetition rate	f_s	1 GHz

more efficient integration with fiber-based telecommunication networks, which in turn allows for a compact setup inside the CubeSat and the use of high-speed electro-optical modulators. The choice of parameters for the beam size and telescope apertures is done to optimize the rate while keeping the design compact enough to fit inside a 3U CubeSat.

3.3 QKD simulation

For the numerical simulations, the python package SatQuMA was modified[2] to implement the simplified BB84, three-state and one-decoy described in [35, 44]. SatQuMA is an open-source software that models the efficient BB84 protocol with four-state two-decoy using WCPs in a downlink configuration, described in [70, 71]. The 3-state protocol was chosen for its simpler setup, making it easier to meet the SWaP constraints. The simplified BB84 has been shown to achieve experimental secret key rates close to the ideal four-state BB84 implementation, showing that there is no performance loss by choosing this protocol [72]. The secret key analysis for a three-state one-decoy described in was added to simulate and optimize the SKR through a satellite overpass.

The chosen orbit path transits through the zenith, ensuring maximum coverage and visibility from the ground station. In Table 2, the values used in the simulation are given. The satellite's sun-synchronous orbit is fixed to an altitude of 500 km and the downlink transmission is made by a laser source of 1550 nm of wavelength, a common choice for high-speed optical communication networks. The telescope aperture diameter of the transmitter is fixed to 4 cm as previously explained. For the ground station telescope, an aperture of 70 cm was chosen. The beam waist is set to be half the transmitter aperture diameter, as done in SatQuMA, so as not to clip too much of the Gaussian beam. This choice affects the system's performance, as a larger beam waist would lead to better signal strength and more efficient transmission.

To optimize the performance of the satellite to ground station communication system, the parameter P_Z^B was fixed to 0.9, which is a common value for a BS, and the parameters k, P_k and P_Z^A (with $k = \{\mu_1, \mu_2\}$) were set to vary according to the losses of the system and the transmission time window. Figure 4 shows the numerical simulation of optimized SKR and QBER during a satellite overpass.

The simulation assumes a perfect satellite overpass with a maximum elevation of 90 degrees. In this analysis, the SKR values range up to 80.8 kHz, and the total transmission

[2]The code is available on the Github page https://github.com/QuLab-IT/QuantSatSimulator.git.

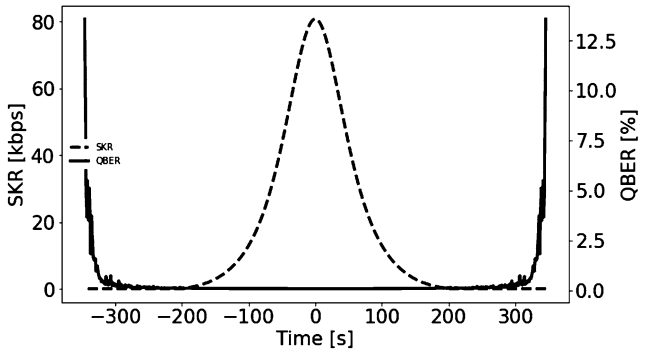

Figure 4 Satellite-to-ground QKD Simulation. Secret Key Rate (dashed line) and Quantum Bit Error Rate (solid line) over a satellite pass

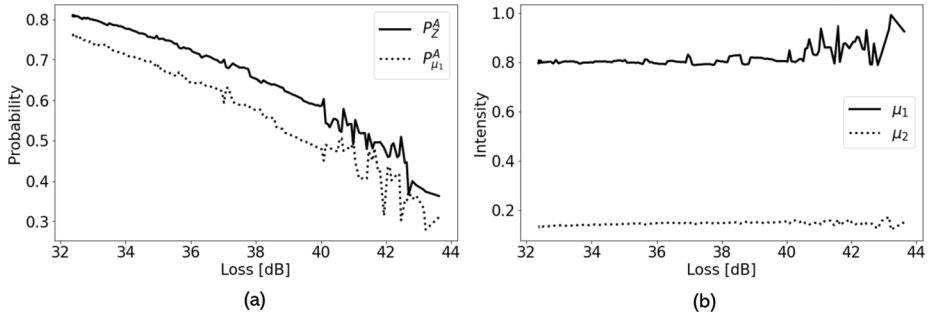

Figure 5 Optimised parameters as a function of the system loss. (a) Probabilities of Alice sending an Z basis state, P_Z^A (solid line), and of sending a state state, P_{μ_1} (pointed line). (b) Intensity of state signal μ_1 (solid line) and decoy signal μ_2 (pointed line)

window is approximately 304 seconds per pass. Consequently, the total secure block size after one satellite pass is approximately 9.9 Mbits. Each value of SKR was obtained by optimizing the SKL within a 1-second time window (time interval between values of channel's attenuation, see Fig. 3.a). The Secret Key Length encompasses both the transmitted secret key bits and the final leaked bits, denoted as λ_{EC}, used for QBER deduction.

The minimum QBER value occurs at the zenith, at 0.08%, and increases rapidly for lower elevations. The simulation is designed to maximize the SKR, which results in the optimizer being unable to converge at a fixed value for QBER, when the SKR is zero, as evidenced by the oscillations in the figure. Nevertheless, within the total transmission window, the QBER remains below 1%.

Figure 5 represents the optimal set of values for the protocol parameters as a function of the total loss of the system. To ensure a maximal SKR, the values of probabilities of P_Z^A and P_{μ_1} decrease rapidly with the increase of loss, the values of the intensities μ_1 and μ_2 vary very little compared with the probabilities but their value increase slightly with the system losses. For high values of loss (close to a zero SKR), the simulator has difficulty converging to a set of parameters. However, there is a clear tendency in the figures. After 43.6 dB of loss, the system cannot maintain transmission of secret key bits. Thus, the values of the parameters can no longer optimize the communication. The optimal values for the parameters at the zenith position are presented in Table 3.

Table 3 Optimal Communication parameter values for the zenith

Parameter	Symbol	Value
Intensity 1	μ_1	0.81
Probability of sending intensity 1	P_{μ_1}	0.76
Intensity 2	μ_2	0.12
Probability of sending intensity 2	P_{μ_2}	0.24
Probability Alice sends an Z basis signal	P_Z^A	0.88
Probability Bob measures an Z basis signal	P_Z^B	0.9

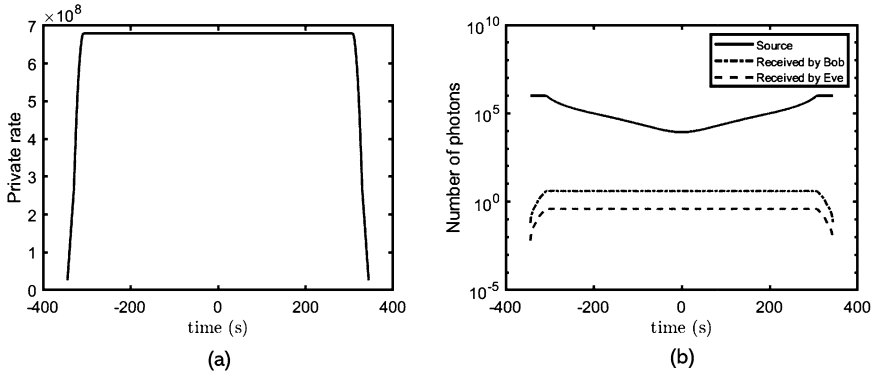

Figure 6 a) QKPC rates based on the private capacity. b) Number of photons required to maximize the private capacity versus time

3.4 QKPC simulation

The QKPC security arguments to a realistic channel are applied, using the same data used for the QKD simulations. The number of photons detected by Bob is $\eta\mu$, where η are the same losses considered in the QKD simulations and shown in Fig. 3.a.

The number of photons detected by Eve is $\gamma\eta\mu$. The realistic value of $\gamma = 0.1$ is chosen based on [13].

In Fig. 6, the results of the simulations are shown. In Fig. 6.a, the rate versus elevation is presented. It is seen for a wide range of elevations that, QKPC can provide a secret transmission rate of 700 MHz. In Fig. 6.b, it can be seen how the number of photons must be varied in order to guarantee the optimal transmission rate. It was found that for optimal rates, the source must send about one million photons per pulse, Bob receives 3–4 photons per pulse, while Eve only receives about 0.3–0.4 photons per pulse. This ensures that while Bob can efficiently discriminate the coherent state from the vacuum, for Eve it is much more difficult.

Figure 6 also shows that the communication window is wider for the QKPC. In the QKD protocol, the losses have to drop below a certain value for the communication to start. In our simulations, only during approximately 304 seconds in a pass will the QKD rate be strictly positive. For the QKPC protocol, the system can adapt to the losses by varying the number of photons it sends. Therefore, in a satellite pass, it can communicate as soon as there is a line-of-sight with the receiver, extending the communication window close to the time of a pass (around 600 seconds) while maintaining the optimal secret transmission rate of 700 MHz. This means the total number of secret bits sent (or generated) in a pass can be close to 420 Gbits as opposed to the 9.9 Mbits of the QKD protocol. Since the QKPC protocol can sustain higher losses, it can also work during situations where

the QKD cannot operate. These situations include bad weather conditions and daytime. Nevertheless, it is important to note that these protocols serve different purposes. QKD is used for key exchange and provides unconditional security while the QKPC is used to transmit a direct message and offers security under more relaxed assumptions.

4 Conclusion

Quantum communication in space is a very promising research field in what concerns information privacy. Recent efforts have focused on QKD solutions, nevertheless, that particular class of quantum communication protocols is far from achieving practical rates for telecommunications. This work goes beyond such approaches, by introducing a nanosatellite design capable of performing both QKD and another class of protocols called QKPC. In this article, a preliminary design for a 3U CubeSat quantum communications downlink is proposed. The CubeSat serves as a platform to implement various quantum communication protocols. This versatility is demonstrated with two examples: QKD with the simplified BB84 and QKPC.

The design is validated via a SWaP analysis using commercial off-the-shelf components. It is argued that all the mission requirements, including pointing and classical communication, can be achieved in a 3U CubeSat. The feasibility of LEO communication is shown using the design via numerical simulations of the simplified BB84 and QKPC. In the case of QKD, we expand an existing toolbox called SatQuMA to achieve a realistic simulation of the simplified BB84 in a downlink configuration. It is found that, under realistic conditions, at zenith, a SKR is obtained for the simplified BB84 slightly over 80 kHz and a QBER slightly larger than 0.07%. It is shown the QKPC scheme achieves an optimal 700 MHz private communication rate for a wide range of elevations, in fact during most of the communication time.

Future study directions to validate the solution include building a demonstration setup with portable optical breadboards, one for Alice, and one for Bob, and building a prototype of the CubeSat which can be used for space validation. There are several options to further miniaturize the solution, and the optimal solution will most likely involve integrated optics. Hence, another important direction to follow is to design photonic integrated circuits implementing at least part of the optical payload proposed. For example, the generation of weak coherent pulses for QKD and QKPC can be done on a photonic integrated circuit, and other CubeSat missions with quantum communication payloads have already started investigating/using those [22, 73]. Other future work planned will include the compatibility of the CubeSat system with the CCSDS standards and with current/planned ground stations. Naturally, such a miniaturization of the optical payload will allow for a better performance of the CubeSat, for example in the most limiting properties such as pointing and classical communication.

Regarding applications, besides long-distance quantum communication, this solution could serve as a payload for free-space quantum communication using airplanes or drones.

Abbreviations

ADCS, Altitude Determination and Control System; DFB, Distributed-Feedback; EOAM, Electrooptic Amplitude Modulator; EOPM, Electrooptic Polarization Modulator; FPGA, Field-Programmable Gate Array; GEO, Geostacionary Orbit; LEO, Low-Earth Orbit; MEO, Medium-Earth Orbit; OOK, On-Off Keying; PC, Polarization Controller; QBER, Quantum Bit Error Rate; QKPC, Quantum Keyless Private Communication; QKD, Quantum Key Distribution; QRNG, Quantum Random Number Generator; SKL, Secret Key Length; SKR, Secret Key Rate; SWaP, Size, Weight and Power; WCP, Weak Coherent Pulse; WCP, Weak Coherent Pulses.

Acknowledgements
Not applicable.

Author contributions
P.N.M. and G.L.T. worked on the setup design, numerical simulations, and writing the manuscript. D.P. contributed to discussions on the satellite design. E.Z.C. supervised the work and contributed to every step of it. R.R., P.A., M.N., R.F. ad D.R. co-supervised the work.

Funding
The authors thank the support from Instituto de Telecomunicações, namely through project QuantSat-PT (UIDB/50008/2020) and the support from the European Commission (EC) through project PTQCI (DIGITAL-2021-QCI-01). E.Z.C. acknowledges funding by FCT/MCTES - Fundação para a Ciência e a Tecnologia (Portugal) - through national funds and when applicable co-funding by EU funds under the project UIDB/50008/2020. E.Z.C. also acknowledges funding by FCT through project 2021.03707.CEECIND/CP1653/CT0002.
D.R. thanks the Galician Regional Government (consolidation of Research Units: AtlantTIC), MICIN with funding from the European Union NextGenerationEU (PRTR-C17.I1) and the Galician Regional Government with own funding through the "Planes Complementarios de I+D+I con las Comunidades Autónomas" in Quantum Communication and The European Union's Horizon Europe Framework Programme under the project "Quantum Security Networks Partnership" (QSNP, grant agreement No 101114043).

Data Availability
The repository https://github.com/QuLab-IT/QuantSatSimulator.git contains the Python code developed in this work.

Declarations

Competing interests
The authors declare no competing interests.

Author details
[1]Departamento de Engenharia Electrotécnica e de Computadores, Instituto Superior Técnico, Av. Rovisco Pais, 1049-001, Lisbon, Portugal. [2]Instituto de Telecomunicações, Av. Rovisco Pais, 1049-001, Lisbon, Portugal. [3]Departamento de Física, Instituto Superior Técnico, Av. Rovisco Pais, 1049-001, Lisbon, Portugal. [4]Instituto Superior de Engenharia de Lisboa, R. Conselheiro Emídio Navarro 1, 1959-007, Lisbon, Portugal. [5]Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain. [6]Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain. [7]AtlanTTic Research Center, University of Vigo, Vigo E-36310, Spain.

Received: 2 December 2023 Accepted: 26 June 2024 Published online: 30 July 2024

References

1. Shannon CE. A mathematical theory of communication. Bell Syst Tech J. 1948;27(3):379–423.
2. Chugh V, Basu A, Kaushik A, Basu AK. Progression in quantum sensing/bio-sensing technologies for healthcare. ECS Sens Plus. 2023;2(1):015001.
3. Crawford SE, Shugayev RA, Paudel HP, Lu P, Syamlal M, Ohodnicki PR, Chorpening B, Gentry R, Duan Y. Quantum sensing for energy applications: review and perspective. Adv Quantum Technol. 2021;4(8):2100049.
4. Nadlinger DP, Drmota P, Nichol BC, Araneda G, Main D, Srinivas R, Lucas DM, Ballance CJ, Ivanov K, Tan EY-Z et al. Experimental quantum key distribution certified by Bell's theorem. Nature. 2022;607(7920):682–6.
5. Zhang W, van Leent T, Redeker K, Garthoff R, Schwonnek R, Fertig F, Eppelt S, Rosenfeld W, Scarani V, Lim CC-W et al. A device-independent quantum key distribution system for distant users. Nature. 2022;607(7920):687–91.
6. Liu W-Z, Zhang Y-Z, Zhen Y-Z, Li M-H, Liu Y, Fan J, Xu F, Zhang Q, Pan J-W. High-speed device-independent quantum key distribution against collective attacks. 2021. arXiv preprint arXiv:2110.01480.
7. Bennett CH, Brassard G. Quantum cryptography and its application to provably secure key expansion, public-key distribution, and coin-tossing. In: Proceedings of IEEE international symposium on information theory, St Jovite, Canada. 1983.
8. Pljonkin A, Singh P. The review of the commercial quantum key distribution system. 2018. p. 795–799. 12.
9. Zhang Q, Xu F, Chen Y-A, Peng C-Z, Pan J-W. Large scale quantum key distribution: challenges and solutions. Opt Express. 2018;26(18):24260–73.
10. Hosseinidehaj N, Malaney R, Ng S, Hanzo L. Satellite-based continuous-variable quantum communications: state-of-the-art and a predictive outlook. IEEE Commun Surv Tutor. 2017;**PP**.
11. Pirandola S, Andersen UL, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C, Pereira JL, Razavi M, Shamsul Shaari J, Tomamichel M, Usenko VC, Vallone G, Villoresi P, Wallden P. Advances in quantum cryptography. Adv Opt Photonics. 2020;12(4):1012.
12. Grünenfelder F, Boaron A, Rusca D, Martin A, Zbinden H. Simple and high-speed polarization-based qkd. Appl Phys Lett. 2018;112(5):051108.
13. Vázquez-Castro A, Rusca D, Zbinden H. Quantum keyless private communication versus quantum key distribution for space links. Phys Rev Appl. 2021;16(1):014006.
14. Bedington R, Bai X, et al. Nanosatellite experiments to enable future space-based qkd missions. EPJ Quantum Technol. 2016;**3**(12).
15. Polnik M, Mazzarella L, Di Carlo M, Oi DKL, Riccardi A, Arulselvan A. Scheduling of space to ground quantum key distribution. EPJ Quantum Technol. 2020;7(1):3.
16. Villoresi P, Jennewein T, Tamburini F, Aspelmeyer M, Bonato C, Ursin R, Pernechele C, Luceri V, Bianco G, Zeilinger A et al. Experimental verification of the feasibility of a quantum channel between space and Earth. New J Phys. 2008;10(3):033038.

17. 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(8):502–8.
18. Lu C-Y, Cao Y, Peng C-Z, Pan J-W. Micius quantum experiments in space. Rev Mod Phys. 2022;**94**(3).
19. Villela T, Costa CA, Brandão AM, Bueno FT, Leonardi R. Towards the thousandth cubesat: a statistical overview. Int J Aerosp Eng. 2019;**2019**.
20. Oi DKL, Ling A, Vallone G, Villoresi P, Greenland S, Kerr E, Macdonald M, Weinfurter H, Kuiper H, Charbon E, Ursin R. CubeSat quantum communications mission. EPJ Quantum Technol. 2017;4(1):6.
21. Haber R, Garbe D, Schilling K, Rosenfeld W. Qube-a cubesat for quantum key distribution experiments. In: Small satellite conference 18-III-05. DigitalCommons@USU. 2018.
22. de Forges de Parny L, Alibart O, Debaud J, Gressani S, Lagarrigue A, Martin A, Metrat A, Schiavon M, Troisi T, Diamanti E et al. Satellite-based quantum information networks: use cases, architecture, and roadmap. Commun Phys. 2023;6(1):12.
23. Kerstel E, Gardelein A, Barthelemy M, Gilot Y, LeCoarer E, Rodrigo J, Sequies T, Borne V, Bourdarot G, Christidis A, Segura J, Boulanger B, Boutou V, Bouzat M, Chabanol M, Fesquet L, Fourati H, Moulin M, Niot J-M, Bastos RP, Robu B, Rolland E, Toru S, Fink M, Joshi SK, Nanobob RU. A cubesat mission concept for quantum communication experiments in an uplink configuration. EPJ Quantum Technol. 2018;**5**(1).
24. Zhang P, Sagar J, Hastings E, Stefko M, Joshi S, Rarity J. End-to-end demonstration for cubesatellite quantum key distribution. IET Quantum Commun. 2023.
25. Jennewein T, Simon C, Fougeres A, Babin F, Asadi FK, Kuntz KB, Maisonneuve M, Moffat B, Mohammadi K, Panneton D. Qeyssat 2.0–white paper on satellite-based quantum communication missions in canada. 2023. arXiv preprint arXiv:2306.02481.
26. Mazzarella L, Lowe C, Lowndes D, Joshi SK, Greenland S, McNeil D, Mercury C, Macdonald M, Rarity J, Oi DKL. Quarc: quantum research cubesat—a constellation for quantum communication. Cryptography. 2020;4(1):7.
27. Dequal D, Vallone G, Bacco D, Gaiarin S, Luceri V, Bianco G, Villoresi P. Experimental single-photon exchange along a space link of 7000 km. Phys Rev A. 2016;**93**(1).
28. Günthner K, Khan I, Elser D, Stiller B, Bayraktar Ö, Müller CR, Saucke K, Tröndle D, Heine F, Seel S et al. Quantum-limited measurements of optical signals from a geostationary satellite. Optica. 2017;4(6):611–6.
29. Bruß D. Optimal eavesdropping in quantum cryptography with six states. Phys Rev Lett. 1998;81(14):3018.
30. Bechmann-Pasquinucci H, Gisin N. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. Phys Rev A. 1999;59(6):4238.
31. Molotkov SN, Nazin SS. Quantum cryptography based on the time–energy uncertainty relation. In: Quantum devices and circuits, proceedings of the international conference. Singapore: World Scientific; 1996. p. 298.
32. Shi B-S, Jiang Y-K, Guo G-C. Quantum key distribution using different-frequency photons. Appl Phys B. 2000;70(3):415–7.
33. Fung C-HF, Lo H-K. Security proof of a three-state quantum-key-distribution protocol without rotational symmetry. Phys Rev A. 2006;74(4):042342.
34. Tamaki K, Curty M, Kato G, Lo H-K, Azuma K. Loss-tolerant quantum cryptography with imperfect sources. Phys Rev A. 2014;90(5):052314.
35. Rusca D, Boaron A, Curty M, Martin A, Zbinden H. Security proof for a simplified Bennett-brassard 1984 quantum-key-distribution protocol. Phys Rev A. 2018;98(5):052336.
36. Brassard G, Lütkenhaus N, Mor T, Sanders BC. Limitations on practical quantum cryptography. Phys Rev Lett. 2000;85(6):1330.
37. Lütkenhaus N. Security against individual attacks for realistic quantum key distribution. Phys Rev A. 2000;61(5):052304.
38. Hwang W-Y. Quantum key distribution with high loss: toward global secure communication. Phys Rev Lett. 2003;91(5):057901.
39. Lo H-K, Ma X, Chen K. Decoy state quantum key distribution. Phys Rev Lett. 2005;94(23):230504.
40. Wang X-B. Beating the photon-number-splitting attack in practical quantum cryptography. Phys Rev Lett. 2005;94(23):230503.
41. Ma X, Qi B, Zhao Y, Lo H-K. Practical decoy state for quantum key distribution. Phys Rev A. 2005;72(1):012326.
42. Hayashi M, Nakayama R. Security analysis of the decoy method with the Bennett–brassard 1984 protocol for finite key lengths. New J Phys. 2014;16(6):063009.
43. Lim CCW, Curty M, Walenta N, Xu F, Zbinden H. Concise security bounds for practical decoy-state quantum key distribution. Phys Rev A. 2014;89(2):022307.
44. Rusca D, Boaron A, Grünenfelder F, Martin A, Zbinden H. Finite-key analysis for the 1-decoy state qkd protocol. Appl Phys Lett. 2018;112(17):171104.
45. Davide R. Security of quantum cryptography: from quantum random key generation to quantum key distribution. PhD thesis. University of Geneva; 2020.
46. Sidhu JS, Brougham T, McArthur D, Pousa RG, Oi DK. Satellite quantum modelling & analysis software version 1.1: documentation. 2021. arXiv preprint arXiv:2109.01686.
47. Shannon CE. Communication theory of secrecy systems. Bell Syst Tech J. 1949;28(4):656–715.
48. Wyner AD. The wire-tap channel. Bell Syst Tech J. 1975;54(8):1355–87.
49. Cai N, Winter A, Yeung RW. Quantum privacy and quantum wiretap channels. Probl Inf Transm. 2004;40(4):318–36.
50. Devetak I. The private classical capacity and quantum capacity of a quantum channel. IEEE Trans Inf Theory. 2005;51(1):44–55.
51. Hayashi M, Vázquez-Castro Á. Physical layer security protocol for Poisson channels for passive man-in-the-middle attack. IEEE Trans Inf Forensics Secur. 2020;15:2295–305.
52. Ghalaii M, Bahrani S, Liorni C, Grasselli F, Kampermann H, Wooltorton L, Kumar R, Pirandola S, Spiller TP, Ling A, et al. Realistic threat models for satellite-based quantum key distribution. 2022. arXiv preprint arXiv:2212.04807.
53. Neumann SP, Joshi SK, Fink M, Scheidl T, Blach R, Scharlemann C, Abouagaga S, Bambery D, Kerstel E, Barthelemy M et al. Q3sat: quantum communications uplink to a 3U cubesat—feasibility & design. EPJ Quantum Technol. 2018;5(1):4.
54. Yuan ZL, Lucamarini M, Dynes JF, Fröhlich B, Plews A, Shields AJ. Robust random number generation using steady-state emission of gain-switched laser diodes. Appl Phys Lett. 2014;104(26):261112.

55. Lovic V, Marangon DG, Lucamarini M, Yuan Z, Shields AJ. Characterizing phase noise in a gain-switched laser diode for quantum random-number generation. Phys Rev Appl. 2021;16(5):054012.
56. Perlot N, Dreischer T, Weinert C, Perdigues J. Optical geo feeder link design. 2012 Future Network and Mobile Summit, FutureNetw 2012. 2012.
57. Cahoy K, Grenfell P, Crews A, Long M, Serra P, Nguyen A, Fitzgerald R, Haughwout C, Diez R, Aguilar A et al. The cubesat laser infrared crosslink mission (click). In: International Conference on Space Optics—ICSO 2018. vol. 11180. Bellingham: SPIE; 2019. p. 358–69.
58. Revés J, Viveiros I, Cunha R, Rocha R, Monteiro JP, Borralho A, André P, Niehus M, Mendes P, Ruas J et al. Quantsat-pt: an attitude determination and control system architecture for qkd. In: 4th symposium on space educational activities. Universitat Politècnica de Catalunya; 2022.
59. Sidhu JS, Brougham T, McArthur D, Pousa RG, Oi DK. Finite key effects in satellite quantum key distribution. npj Quantum Inf. 2022;8(1):1–11.
60. del Portillo Barrios I, Cameron B, Crawley E. A technical comparison of three low Earth orbit satellite constellation systems to provide global broadband. Acta Astronaut. 2019;159:03.
61. Yost B, Weston S, Benavides G, Krage F, Hines J, Mauro S, Etchey S, O'Neill K, Braun B. State of the art: small spacecraft technology. Technical Report 20210021263. NASA Ames Research Center; 2021.
62. Rose TS, Rowen DW, LaLumondiere S, Werner NI, Linares R, Faler A, Wicker J, Coffman CM, Maul GA, Chien DH et al. Optical communications downlink from a 1.5 u cubesat: ocsd program. In: International Conference on Space Optics—ICSO 2018. vol. 11180. Bellingham: SPIE; 2019. p. 201–12.
63. Welle R, Utter A, Rose T, Fuller J, Gates K, Oakes B, Janson S. A cubesat-based optical communication network for low Earth orbit. In: Small satellite conference 17-XI-01. DigitalCommons@USU. 2017.
64. Tomio H, Grenfell P, Kammerer W, Serra P, Čierny O, Lindsay C, Garcia M, Cahoy K, Clark M, Coogan D, Conklin J, Mayer D, Stupl J, Hanson J. Development and testing of the laser transmitter and pointing, acquisition, and tracking system for the cubesat laser infrared crosslink (click) b/c mission. In: 2022 IEEE International Conference on Space Optical Systems and Applications (ICSOS). 2022. p. 224–31.
65. Steinhauer S, Gyger S, Zwiller V. Progress on large-scale superconducting nanowire single-photon detectors. Appl Phys Lett. 2021;**118**(10).
66. Berk A, Bernstein LS, Anderson GP, Acharya PK, Robertson DC, Chetwynd JH, Adler-Golden SM. Modtran cloud and multiple scattering upgrades with application to aviris. Remote Sens Environ. 1998;65(3):367–75.
67. Emde C, Buras-Schnell R, Kylling A, Mayer B, Gasteiger J, Hamann U, Kylling J, Richter B, Pause C, Dowling T, Bugliaro L. The libradtran software package for radiative transfer calculations (version 2.0.1). Geosci Model Dev. 2016;9(5):1647–72.
68. Robinson BS, Boroson DM, Burianek DA, Murphy DV. Overview of the lunar laser communications demonstration. In: Free-space laser communication technologies XXIII. vol. 7923. Bellingham: SPIE; 2011. p. 9–12.
69. Maharjan N, Devkota N, Kim BW. Atmospheric effects on satellite–ground free space uplink and downlink optical transmissions. Appl Sci. 2022;12(21):10944.
70. Brougham T, Oi DKL. Medium-range terrestrial free-space qkd performance modelling and analysis. In: Quantum technology: driving commercialisation of an enabling science II. vol. 11881. Bellingham: SPIE; 2021. p. 14–23.
71. Islam T, Sidhu JS, Higgins BL, Brougham T, Vergoossen T, Oi DKL, Jennewein T, Ling A. Finite resource performance of small satellite-based quantum key distribution missions. Commun Phys. 2023;6(1):210.
72. Boaron A, Boso G, Rusca D, Vulliez C, Autebert C, Caloz M, Perrenoud M, Gras G, Bussières F, Li M-J, Nolan D, Martin A, Zbinden H. Secure quantum key distribution over 421 km of optical fiber. Phys Rev Lett. 2018;**121**(19).
73. Zhu C-X, Chen Z-Y, Li Y, Wang X-Z, Wang C-Z, Zhu Y-L, Liang F-T, Cai W-Q, Jin G, Liao S-K et al. Experimental quantum key distribution with integrated silicon photonics and electronics. Phys Rev Appl. 2022;17(6):064034.

Publisher's Note