Communication distance and security improvement in satellite based quantum key distribution via photon polarization pseudo-random bases encoding

TENE Alain Giresse[1], **YIANDE DEUTO Germain**[1], **AZANGUE KOUMETIO Armel**[1], **TCHOFFO Martin**[1,2]

[1]Department of Physics, Faculty of Science, University of Dschang, Cameroon, P.O.Box 67, Cameroon
[2]Centre d'Etude et de Recherche en Agronomie et en Biodiversité, FASA, Université de Dschang, Cameroun

E-mail: alain.tene@aims-cameroon.org

Abstract. New protocol to achieve very long-distance and secure communication between two legitimate users (Alice and Bob) namely, the pseudo-random entangled photon based QKD protocol using a low-earth-orbit (LEO) type satellite as the photon source relay is proposed. We assume the combined type-I and type-II SPDC as photon source distributing entangled photons pairs to Alice and Bob, and the quantum logistic map (QLM) as PRNG in order to pseudorandomly select photon polarization states measurement bases. Under these considerations, the secure key rate upper bound is evaluated and numerical simulations show that, the maximum communication distance increases significantly with the photon block size, and with the error correction function. One also observes that the protocol can tolerate a secure communication up to about 19000 km under lower background error (or lower atmosphere diffraction). The secure key privacy is strongly improved since public discussion is avoided due to the use of PRNG, which guarantees identical measurement bases choice between Alice and Bob. Based on the above, our protocol is more efficient. In addition, the secure key privacy is significantly amplified.

1. Introduction

In our nowadays communication networks, truly secret communication channel between two or more operators has become a major problem with an increasing in computer's power and speed. That is, scientists continuously think about a better way to secretly share sensitive information or a secure and unbreakable key for information encryption. Quantum mechanics properties of particles have been recently presented as a suitable candidate to solve the problem [1, 2, 3, 4]. Based on this idea, several research works have been developed in the past few decades to implement new strategies which employed quantum effects to manipulate and transmit information more secretly, here we refer to as quantum cryptography (QC) [5, 6]. The latest mentioned notion mainly focuses on sharing a secret key for information encryption between two or more legitimate users (Alice and Bob), namely quantum key distribution (QKD) and has been proved to significantly improve the security of information, since Alice and Bob could be alert by the presence of any eavesdropper (Eve) intending to intercept the communication between them.

Indeed, the concept of QKD first introduced by Bennett and Brassard in 1984, is nowadays known as the best method of sharing a secret key and has therefore, been successfully implemented [6]. For this reason, numerous QKD protocols have been developed so far namely: the BB84 [6], the Ekert91 (proposed by Ekert in 1991, [7]), the B92 (proposed by Bennett in 1992 [8]), the SSP (six-state protocol proposed by Bechmann-Pasquinucci in 1999 [9, 10]) protocols, just to list a few. Despite their huge security, these protocols still present some limits as they require single photon measurement which induces losses due to photon splitting. In addition to the security, two other properties characterize good QKD protocol, which are the quantum bit error rate (QBER) and the maximum tolerable communication distance between legitimate users. However, the above mentioned protocols were found to present lower QBER and very limited communication distance. To overcome these drawbacks, new protocols that used entangled photons as well as Bell's entangled states were developed [11, 12, 13]. Whereas, it was demonstrated that with a spontaneous parametric-down conversion (SPDC) photon pairs source based QKD, noisy quantum channels can achieve a maximum of up to 144 *km* as communication distance, which is acceptable but not enough to achieve long-distance communication [14, 15]. Experiments proved that for any pure-loss quantum channel with transmittance efficiency η, the secure key rate scales linearly with η [16, 17, 18], inducing a fundamental limit to the maximum tolerable communication distance. Due to this problem, new approaches which are based on sharing a secret key over free space with very lower loss rate using low-earth-orbit (LEO), medium-earth-orbit (MEO) or geostationary orbit (GEO) satellites as an intermediate relay between legitimate communication users were very recently introduced [19]. However, LEO and GEO are the most suitable candidates due to their altitude (160 to 3000 km or usually below 900 km for LEO and 35786 km precisely for GEO). Thus, due to the proximity of LEO to the earth's surface, we assume in this work our SPDC entangled photon source to be located in a LEO-type satellite in order to reduce losses due to beam diffraction.

In fact, satellite based QKD has attracted significant interests of researchers, and has been successfully implemented in real physical experiments [16, 20, 21, 22, 23, 24]. Although significant results have been achieved, the security of the protocol still requires deep studies. Whereas, Jian-Yu *et al.* [25] demonstrated that free-space links could provide the most appealing solution to long-distance and secure communication. The experiment was conducted using a floating platform hot-air balloon fulfilling the conditions of a LEO-type satellite. In similar conditions, Wang *et al.* [25] will later investigate long-distance QKD with the floating hot-air balloon platform under rapid motion, altitude change and they found a quantum bit error rate (QBER) of 4.04%. Moreover, Pan [26] established the space platform with long-distance satellite-to-ground quantum channel and he was able to achieve the BB84 QKD up to 1200 km with a QBER of about 1%. In the same idea, using retro-reflectors in LEO satellite, space-to-ground transmission of quasi-single photon has been investigated by Yin *et al.* [27]. They realized a signal-to-noise ratio of 16:1, sufficient for unconditionally secure QKD links. In addition, Nauerth *et al.* [28] found that, the BB84 QKD between ground station and airplane moving at regular angular velocity similar to LEO-type satellite is feasible, and the experiment demonstrated a QBER of 4.8% at 20 km range. However, the first downlink microsatellite QKD experiment was just realized very recently in 2017 with a QBER less than 3% and 99.4±4.4% degree polarization by Takenaka *et al.* [29]. Several authors investigated the protocol using single photons and demonstrated the feasibility of free space satellite-to-ground QKD with significant improvements regarding the QBER, the communication distance and the sifted key rate in the night-time as well as under noisy-like sunlight daytime [20, 22, 30, 31, 32, 33]. Further achievements using entangled photons showed that, the latest can more significantly improve the key rate and the communication distance as well. Moreover, it turns out that downlink QKD in night-time presents lower loss compared to uplink QKD in similar conditions [34, 35]. Nevertheless, all the previously mentioned protocols use most often true random number generators (TRNGs) for photon bases choice. This usually costs sifting in the key raw and may reduce up to half in its size, since the legitimate users (Alice and Bob) must perform their measurement with incompatible bases choices.

To overcome this serious drawback, we propose in this research paper to use pseudo-random number generators (PRNGs) for photon measurement bases choices, which guarantees identical measurement bases selection by Alice and Bob. Similar procedure was very recently studied in our previous works, but in the case of optical link based QKD protocol [36], and the results proved its efficiency. We thus, suggest a new protocol that uses quantum chaotic systems, which are very good PRNGs, can be easily implemented and strongly improve the efficiency of the QKD protocol security. If this protocol is successfully implemented, it will significantly enhance the maximum communication distance and the efficiency of the security due to random-like behavior and high sensitivity to initial conditions of chaotic systems [37, 38]. We therefore, assume our random bases selection to be guaranteed by the quantum logistic map (QLM) [39] and the SPDC-photon source to be our entangled photons generator located in a LEO-type satellite to ensure downlink communication with lower loss. This is realized following the structure below: Sec. 2 presents in detail the procedure to generate random bases for photons polarization measurement using QLM. In Sec. 3, the SPDC-entangled photons Hamiltonian is presented, following by the derivation of the wave function and the probability distribution. We also present in detail the scheme for photon polarization state measurement in the same section. The satellite-to-ground based QKD protocol using entangled photons and QLM as PRNG is described in detail in Sec. 4, with the derivation of the QBER and the secure key rate. In addition, numerical simulations of our main results are presented in Sec. 5. We end the work with some concluding remarks and discussion in Sec. 6.

2. Pseudo-random bases generation for photon state polarization measurement via quantum logistic map

Existing QKD protocols provide most often the condition to randomly choose photons polarization states measurement bases. This requires the legitimate users to utilize true-random number generators (TRNGs). However, this procedure costs sifting in the key raw and may induces a loss of half in the secure key size. To avoid the problem, other QKD protocols that use pseudo-random number generators (PRNGs) have been introduced [40, 41, 42]. Using PRNGs in QKD for photons states measurement bases choice and post-processing procedures can highly improve the secure key security. But, there exist a limited number of PRNGs. As developed in our previous works [43], chaotic systems have been found to be very efficient for the purpose. This is the reason why in this section we describe in detail the procedure to generate pseudo-random bit sequences (PRBSs) used for photon states polarization bases encoding via quantum logistic map (QLM). Under quantum error corrections, QLM can be assimilated to classical system, where its dynamics is given by [36, 43, 44]:

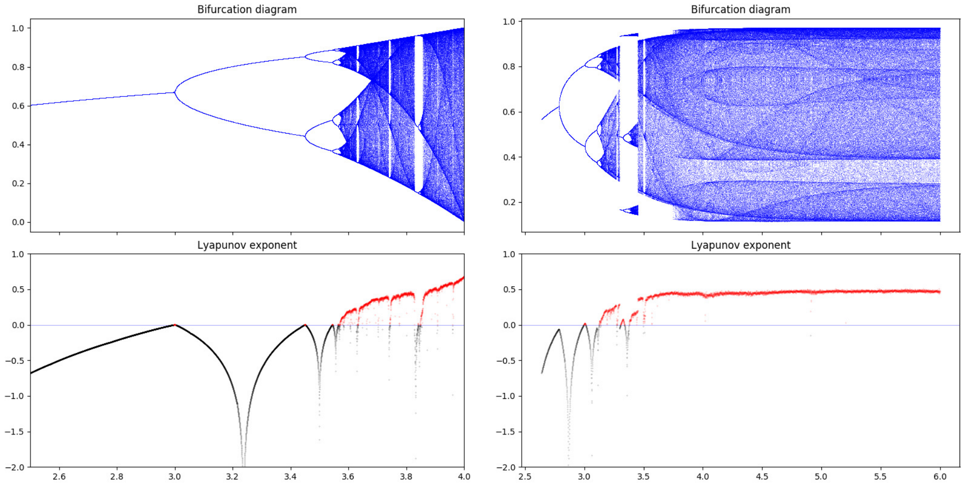
$$\begin{cases} x_{j+1} = r(x_j - |x_j|^2) - ry_j, \\ y_{j+1} = -y_j e^{-2s} + re^{-s}[(2 - x_j - x_j^*)y_j - x_j z_j^* - x_j^* z_j], \\ z_{j+1} = -z_j e^{-2s} + re^{-s}[2(1 - x_j)z_j - 2x_j y_j - x_j], \end{cases} \tag{1}$$

with r and s the bifurcation parameters. Fig.1 shows its bifurcation diagram behavior with respect to r (fig.1a) and s (fig.1b).

One can observe that, all the values of the variable x always belong to the interval $[0,1]$ and display period doubling, implying that Eq. (1) displays chaotic behavior, given r and s kindly selected such that $4 \geq r > 3.85$ and $s \geq 3.5$. It is worth noting that, the values of x, y and z are real given real initial conditions. Similar figures can be obtained for variables y and z, which also exhibit chaotic behavior and always fall in the interval $[-1,1]$. We notice that, the variables x, y and z which help to define the set of Eq. (2) are function of the bifurcation parameters r and s, which are shared between the communication users before they start running the QKD protocol to provide more security. Whereas, any eavesdropper intending to guess these values will not be able to get the set of Eq. (2), and thus cannot select good bases for photon polarization state measurement. Therefore, system (1) provides an efficient and secure PRNG for quantum state bases choice in QKD protocols. The procedure to generate these pseudo-random bases choices is described below:

Let S be a sequence defined by $S = \{s_k\}_{k=1,\cdots,N}$, with $s_k = \lceil 1000 * (x_k + y_k + z_k) \rceil mod(2)$, which are either 0 or 1, each appearing at random. For example, if $N = 3000$ then, using system (1), the following sequence is obtained,
$S = \{1111111 \cdots 1000110001110111110111011\}$. Based on the NIST TS[1] randomness test [45], we

[1] National Institute of Standards and Technology Test Suite



(a) (b)

Figure 1: Bifurcation diagrams and Lyapunov exponents of the variable x, with respect to r (fig.1a) and s (fig.1b).

found a P-value of 0.5347 which is far greater than 0.01 showing that our sequence S is random with 99.99% confidence. Thus, under the same initial conditions x_0, y_0, z_0 and the same parameters r and s, truly random and identical sequences S_A and S_B are generated on Alice's and Bob's sides, respectively in order to prepare their random-basis for photon polarization state measurement. For this reason, let $|\Phi\rangle=\cos(\phi)|0\rangle+\sin(\phi)|1\rangle$ where $\{|0\rangle,|1\rangle\}$ is the standard basis. Using the sequences S_A and S_B, Alice and Bob can generate the following random sequence bases:

$$B_i=\left\{|\phi_{s_k^i}\rangle,|\phi_{s_k^i}+\frac{\pi}{2}\rangle\right\}, \tag{2}$$

with $\phi_{s_k^i}=\frac{s_k^i\pi}{2}2^{-s_k^i}$, $i=A,B$, and s_k^i take its values in S_A for Alice or S_B for Bob. It can be observed that, if $s_k^i=0$, then $\phi_{s_k^i}=0$ and one get the basis $\left\{|0\rangle,|\frac{\pi}{2}\rangle\right\}$ (rectilinear basis), while for $s_k^i=1$, then $\phi_{s_k^i}=\frac{\pi}{4}$ and one get the basis $\left\{|\frac{\pi}{4}\rangle,|\frac{3\pi}{4}\rangle\right\}$ (diagonal basis). Therefore, following the sequences S_A and S_B obtained respectively by Alice and Bob, the photon state polarization measurement bases are either $\left\{|0\rangle,|\frac{\pi}{2}\rangle\right\}$ or $\left\{|\frac{\pi}{4}\rangle,|\frac{3\pi}{4}\rangle\right\}$ each appearing in a random manner and always coincide for the two legitimate users. Fig.2 illustrates the above described bases rotation:

3. The combined type-I and type-II spontaneous parametric-down conversion entangled photons pairs source

As previously mentioned, the combined type-I and type-II SPDC is assumed in this work to be the entangled photons pairs generator. It is fully described in our previous works [36], where its degenerated Hamiltonian is derived as:

$$H_I=i\kappa(a_H^+b_H^+ + a_V^+b_V^+ + a_H^+b_V^+ - a_V^+b_H^+)+H.c., \tag{3}$$

with κ describing both the crystal's properties and the field pump amplitude, H and V the directions of polarization (H for horizontal and V for vertical). Let $\xi=\kappa t$ the time step, the wave function associated to (3) is derived by:

$$|\Psi\rangle=\frac{1}{\cosh^2(\sqrt{2}\mid\xi\mid)}\sum_{n=0}^{\infty}\frac{\xi^*}{\mid\xi\mid}\sqrt{(n+1)(\alpha^{2n}+\beta^{2n}+\gamma^{2n}+\vartheta^{2n})}\left(\tanh(\sqrt{2}\mid\xi\mid)\right)^n|\Phi_n\rangle, \tag{4}$$

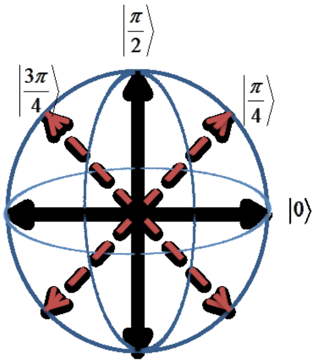

$\left|\frac{\pi}{2}\right\rangle$
$\left|\frac{3\pi}{4}\right\rangle$
$\left|\frac{\pi}{4}\right\rangle$
$|0\rangle$

Figure 2: Polarization state measurement pseudo-random rotation bases.

where

$$|\Phi_n\rangle = \frac{1}{(n+1)\sqrt{\alpha^{2n}+\beta^{2n}+\gamma^{2n}+\vartheta^{2n}}}\sum_{k=0}^{n}[\alpha^n|k,k\rangle_a|(n-k),(n-k)\rangle_b + \beta^n(-1)^{n-k}|k,(n-k)\rangle_a|(n-k),k\rangle_b + \gamma^n(-1)^k|(n-k),k\rangle_a|k,(n-k)\rangle_b + \vartheta^n|(n-k),(n-k)\rangle_a|k,k\rangle_b]. \tag{5}$$

Considering P_k the density probability to generate k-entangled photons pairs, we get :

$$P_k = \mid\langle\Phi_k|\Psi\rangle\mid^2 = \frac{1}{\cosh^4(\sqrt{2}\mid\xi\mid)}(k+1)\tanh^{2k}(\sqrt{2}\mid\xi\mid). \tag{6}$$

Letting $\nu = \sinh^2(\sqrt{2}\mid\xi\mid)$, the photon mean number, which only depends on the light pulse amplitude and the crystal's properties, one obtains:

$$P_k = \frac{\nu^k}{(1+\nu)^{k+2}}(k+1). \tag{7}$$

Fig. 3 presents the comparison between P_k and Poisson distribution. It can be observed that, the probability distribution of photons follows Poisson distribution, which implies the photon pairs that have been produced are non-correlated each to other.

4. Satellite based quantum key transmission with PRB photon polarization state measurement

4.1. Protocol description

As already discussed, we assumed the SPDC-photon source to be located in a LEO-type satellite and emitting a stream of entangled photon pairs directed to the ground by a Cassegrain-type telescope, which are redirected by two other similar telescopes on the ground, to Alice's and Bob's stations, both receiving half of entangled photons pairs. Fig.4 presents the schematic diagram of the process: The strength of the protocol lies on two main fundamental laws of quantum physics namely *"the no-cloning theorem"* and *"the measurement principle"*. Based on this idea and assuming that an eavesdropper (Eve) does not have any useful information regarding the chaotic system's properties (initial conditions and bifurcation parameters) pre-shared between Alice and Bob used for pseudo-random basis selection, the following steps are therefore used to generate the private key:

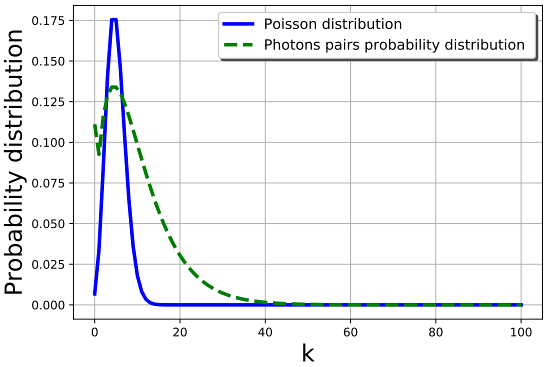


Figure 3: Comparison between the combined type-I and type-II SPDC entangled photons pairs probability density and Poisson distribution.

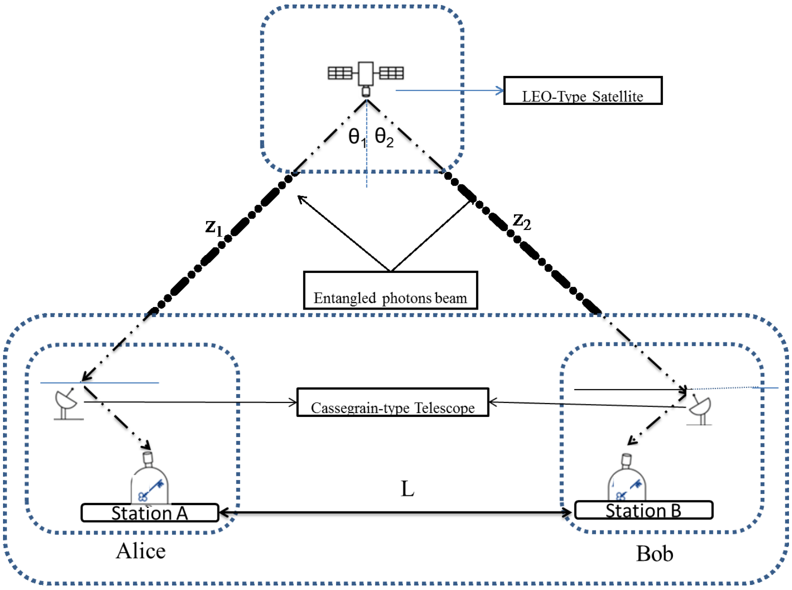


Figure 4: LEO-type satellite based QKD scheme, with each station containing a photon detector device, a photon polarization state measurement device and a photon beam splitter as the procedure requires single photon measurement. Here, an entangled photons source on a satellite emits a stream of entangled photon pairs, directed to the ground by a moving Cassegrain-type telescope. Two other Cassegrain-type telescopes on the ground receive the photons and whatever direction they come from, and send them to the detection apparatus. Due to the relative motion between the satellite and the ground station, there is a relative rotation of the polarization axes between satellite and ground. The Cassegrain-type telescopes are made of pointing mirrors, with the role to ensure lower change in the photon state polarization. The quantities z_1 and z_2 are respectively the distance between Alice's station and the satellite, and the distance between Bob's station and the satellite, while L denotes the distance between Alice's and Bob's stations, which will later be considered as the communication distance between both parties.

Step 1: Alice and Bob first agree on the initial conditions (x_0, y_0 and z_0) and the bifurcation parameters (r and s) of the QLM as presented in Sec. 2 to be later used for random selection of photon polarization state measurement bases. This process is termed as pseudo-random basis (PRB) selection.

Step 2: Assuming the SPDC-entangled photon source to be placed in a LEO-type satellite with an automatic command that can be used to lunch the module at any moment and with the command module on Alice's side, she therefore runs the SPDC module to generate N entangled photon pairs which are shared between her and Bob following the scheme of Fig.4. They also set the value of s which should be increased by step of $\varepsilon = (s_{max} - s_{min})/N$ in the range of 3.5 to 6 as the control parameter.

Step 3: They notify each to other the detection of the entangled photon exchanged via classical channel. The process termed as "information reconciliation" which is invoked for correcting the dependencies between Alice's and Bob's key, which may include for example the dependencies arising from errors inflicted by atmosphere diffraction as well as those due to measurements by Eve. In this case, Alice should repeat the process to satisfy the receptions otherwise, they abort the process.

Step 4: Upon receiving the half entangled photon pair, both Alice and Bob run their QLM module after each pulse and following the procedure kindly described in Sec. 2, they generate two identical PRBs, which should be either rectilinear ($\left\{|0\rangle, |\frac{\pi}{2}\rangle\right\}$ or diagonal ($\left\{|\frac{\pi}{4}\rangle, |\frac{3\pi}{4}\rangle\right\}$)) as shown on Fig.2 to perform their photon polarization state measurement.

Step 5: Following the outcome of the basis they obtained in **Step 4**, they perform the measurement on their detected photon to determine the polarization state, which maps bit 0 onto 90^0- or 135^0-polarization and bit 1 onto 0^0- or 45^0-polarization.

Step 6: Alice and Bob therefore construct two sequences S_A for Alice and S_B for Bob, respectively. Both sequences should be identical given that the photons state polarization is not affected by the measurement device.

Step 7: Alice and Bob simultaneously increment the value of the control parameter s with the step of ε, repeat the process. After performing those steps, the identical sequences S_A and S_B should be only known to Alice and Bob since the photons on which Eve has an information are canceled in **Step 3**.

Step 8: In the worth case where Eve may acquire information about the secret key by guessing the measurement basis at each pulse as well as by listening to the private information shared during the error reconciliation process, for the sake of reducing this information, the technique of "privacy amplification" is invoked. Explicitly, privacy amplification generates a shorter key from the corrected key of **Step 6**, hence reducing Eve's information about the shared key.

4.2. Theoretical evaluation of the QBER and the secure key rate

Optical fiber link based QKD systems offer limited communication distance, and thus cannot be applied for long-distance communication, due to attenuation along the fiber. To overcome this drawback, free-space links QKD systems were proposed [24, 43, 46, 47, 48], which uses GEO, MEO or LEO type satellite as relay between the sender (Alice) and the receiver (Bob). Based on this idea, we propose in this section a QKD protocol that uses a LEO-type satellite in which a SPDC entangled photons source is located with the role of producing and distributing entangled photons pairs to Alice and Bob through free-space. It is important to mention that, the almost non-birefringent character of the atmosphere guarantees the preservation of photon pairs polarization state [24, 46, 47]. However, attenuation of photon's signal is non-negligible due to three main effects, which are: (i) atmospheric propagation, (ii) diffraction and (iii) detector efficiency. As regard to the attenuation due to atmospheric propagation, absorption, scattering and turbulence are the main effects. Thus, atmospheric attenuation can be evaluated taking into consideration the latest effects with the relation:

$$\eta_{atm} = \eta_{abs}\eta_{scatt}\eta_{turb}, \tag{8}$$

with η_{abs}, the attenuation rate due to absorption, η_{scatt} the attenuation rate due to scattering and finally, η_{turb} the attenuation rate due to turbulence. The light is absorbed and scattered by gas molecules and aerosols present in the atmosphere [24, 46, 47]. But, the most relevant contribution to atmospheric propagation attenuation is caused by turbulence, which is due to thermal fluctuations that produce refractive index variations. It mostly depends on the atmospheric condition and the position of the ground station [47]. It causes divergence rate of the light beam, and is evaluated following the work of Moli-Sanchez *et al.* [47] by:

$$\eta_{turb} = \frac{1}{1+\frac{\theta_{turb}^2 R_t^2}{\lambda^2}}, \tag{9}$$

with $\theta_{turb} = \frac{\lambda}{\pi\omega_0}$ the additional divergence angle in radian caused by atmospheric turbulence, λ the signal wavelength, R_t the radius of the transmitting primary pointing mirror and ω_0 the divergence half-angle for Gaussian beams. In most of satellite based QKD protocols, η_{turb} is chosen as constant, since it does not depend on the distance satellite-to-ground, but only on atmospheric conditions.

As regard to signal attenuation due to diffraction, the effect is very important and strongly depends on the satellite-to-ground distance in additional to other telescope's parameters. The Cassegrain-type telescope is used in the sender's and receiver's stations as well as in the satellite to ensure satellite-to-ground downlink transmission. In the present work, we assume such telescope to be used for entangled photons pairs exchange, and also the produced photon beam to be of Gaussian-type [21]. Under these assumptions, the attenuation rate due to diffraction can be calculated following refs. [21, 49] as:

$$\eta_{diff} = \left[\exp\left(-2\frac{r_t^2}{w_t^2}\right) - \exp\left(-2\frac{R_t^2}{w_t^2}\right)\right]\left[\exp\left(-2\frac{r_r^2}{w_r^2}\right) - \exp\left(-2\frac{R_r^2}{w_r^2}\right)\right], \tag{10}$$

with the subscript t representing the transmit telescope and r the receive one. R and r refer to the radii of the primary and secondary mirrors, respectively; λ is the light wavelength; $\omega_{t,r}$ denotes the beam radius at the transmit/receive side, with $\omega_t = R_t$, $\omega_r = \omega(z) = \omega_0\sqrt{1+\frac{z^2}{z_R^2}}$. The quantity $z_R = \frac{\pi\omega_0^2}{\lambda}$ denotes the so called Rayleigh length or Rayleigh range [50], which is the distance along the propagation direction of the beam from waist to the place where the area of the cross section is doubled. z is the distance between the telescopes (i.e. the link distance). In satellite based QKD protocols, one has $z \gg z_R$, and ω_r in this case becomes $\omega_r = \frac{\omega_0 z}{z_R} = \frac{\lambda z}{\pi\omega_0}$, where ω_0 denotes the minimum value of ω.

The telescopes can be also designed as refractors, which is realistic in particular for the transmitter. Eq. (10) is still valid after setting the corresponding value of r to zero. The effect of Pointing errors or misalignment of the optics can be readily taken into account by including an additional attenuation term η_{err}, which is constant. Given that the SPDC photon source distributes entangled photons pairs to Alice and Bob situated each to distant stations on the ground, one must define two quantities, namely, T_A and T_B representing the overall transmission efficiency on Alice's and Bob's sides respectively as follows:

$$\begin{cases} T_A = \eta_{err}\eta_{atm}\varepsilon_A\eta_{diff}^A, \\ T_B = \eta_{err}\eta_{atm}\varepsilon_B\eta_{diff}^B, \end{cases} \tag{11}$$

where ε_A and ε_B define respectively the detector efficiencies of Alice's and Bob's detectors. From Fig.4 describing the protocol, we have assumed a straight line separating Alice's and Bob's stations by a distance of L, which can be expressed as a function of z_1, the distance between Alice's station telescope and the satellite telescope and z_2, the distance between Bob's station telescope and the satellite telescope as:

$$L = \sqrt{z_1^2 + z_2^2 + 2z_1z_2\cos(\theta)}. \tag{12}$$

Inversely, the distances z_1 and z_2 can be expressed as function of L by:

$$\begin{cases} z_1 = \frac{1}{\cos(\theta_1)}\frac{L}{\tan(\theta_1)+\tan(\theta_2)}, \\ z_2 = \frac{1}{\cos(\theta_2)}\frac{L}{\tan(\theta_1)+\tan(\theta_2)}, \end{cases} \tag{13}$$

In the approximation case (i.e. we assume Alice's and Bob's stations at sea level such that one can have $z_1 \approx z_2$), we also have $\theta_1 \approx \theta_2 = \frac{\theta}{2}$, and in this case, we get $z_1 = z_2 = \frac{L}{\sin(\frac{\theta}{2})}$. Taking into account the above assumptions, we get the photons transmission efficiencies on Alice's and Bob's sides with respect to the distance L separating their stations, known as communication distance between legitimate users. Due to the above described phenomena, some photons may thus be lost during the exchanging process and should not be taken into consideration during the secure key extraction process. Below are therefore described in detail the procedure Alice and Bob must perform for the purpose of secure key extraction.

Considering the above relations, the overall transmittance of k-photons state is defined by:

$$T_k = [1-(1-T_A)^k][1-(1-T_B)^k] = 1-(1-T_A)^k-(1-T_B)^k+[(1-T_A)(1-T_B)]^k, \tag{14}$$

It is important to mention that detection may occur on Bob's and Alice's detectors given zero incoming photon. This is known as dark count in existing QKD protocols. In this case the probability to detect a quantum state given an incoming quantum state, is a conditional probability defined by [51]:

$$\Upsilon_k = [T_k + \Upsilon_{0A} - \Upsilon_{0A}T_k][T_k + \Upsilon_{0B} - \Upsilon_{0B}T_k], \tag{15}$$

with Υ_{0A} and Υ_{0B} the dark count probability for the sender's and receiver's detectors, respectively. The overall photon gain can therefore be evaluated as:

$$G_\nu = \sum_{k=0}^{\infty} P_k\Upsilon_k = 1 + \frac{(1-\Upsilon_{0A})(1-\Upsilon_{0B})}{(1+\nu T_A+\nu T_B-\nu T_A T_B)^2} - \frac{1-\Upsilon_{0A}}{(1+\nu T_A)^2} - \frac{1-\Upsilon_{0B}}{(1+\nu T_B)^2}. \tag{16}$$

During the conversion process into sequence of bits of photons state polarization, an error may occur with probability E_0 because of dark count detection. In addition, due to detector device imperfection, one may also record an error with probability E_d. Considering both assumptions, an error of detecting k-photons with probability E_k may occur given by:

$$E_k = \frac{1}{k+1}\sum_{j=0}^{k}\left(E_0 - \frac{E_0-E_d}{\Upsilon_k}\left[(1-T_A)^{k-j}-(1-T_A)^j\right]\left[(1-T_B)^{k-j}-(1-T_B)^j\right]\right). \tag{17}$$

Thus, one can easily evaluate the quantum bit error rate (QBER), which is the probability that detection occurs given erroneous detection as:

$$\begin{aligned} E_\nu =& \frac{\sum_{k=0}^{\infty} P_k\Upsilon_k E_k}{\sum_{k=0}^{\infty} P_k\Upsilon_k} = E_0 - 2\frac{E_0-E_d}{G_\nu(1+\nu)}\frac{1}{T_B-T_A}\left(\frac{1-T_A}{1+\nu T_A} - \frac{1-T_B}{1+\nu T_B}\right) \\ & -2\frac{E_0-E_d}{G_\nu(1+\nu)}\left(\frac{1}{1-(1-T_A)(1-T_B)} + \frac{(1-T_A)(1-T_B)(1-(1-T_A)(1-T_B))^{-1}}{1+\nu-\nu(1-T_A)(1-T_B)}\right). \end{aligned} \tag{18}$$

Analogically to the procedure described in [43], the secure key rate can be derived as:

$$R_n = \frac{1}{N}(NG_\nu(1-H_2(E_\nu+\mu_n)) - K_{leak} - K_{secure}), \tag{19}$$

where, [36]

$$K_{secure} = -log(\frac{2}{\varepsilon_{sec}^2\varepsilon_{co}}),\ K_{leak} = NG_\nu f(E_\nu)H_2(E_\nu), \tag{20}$$

with μ_n the statistical fluctuation known as the maximum optical tolerable noise defined as, $\mu = \sqrt{(\frac{1}{N}+\frac{1}{n})(1+\frac{1}{n})\log(\frac{2}{\varepsilon_{sec}})}$, N the photon pairs block size produced and n the number of photon pairs involved in the key generation. K_{leak} defines the error correction leakage, $H_2(e) = -e\log_2(e) - (1-e)\log_2(1-e)$ the binary Shannon entropy. It is worth noting that ε_{co} introduces the upper bound of the probability that the secret key is correct. This implies that if S_A and S_B are the sender's and receiver's secret key respectively, then the protocol is known to be ε_{co}-correct providing that $Probability(S_A \neq S_B) \leq \varepsilon_{co}$. In the other words, ε_{co} introduces the probability of error induced measurement bases authentication. It is more smaller in this protocol since public discussion is avoided due to the use of PRNG instead of TRNG for measurement bases choice, which guarantees identical measurement bases selection for Alice and Bob.

5. Numerical results and discussions

In this section, we numerically present the main results of this research paper. For this reason, the photon gain mean (PGM) and the quantum bit error (QBE) are simulated with respect to the communication distance separating Alice's and Bob's stations on one hand and the results are depicted in fig.5.

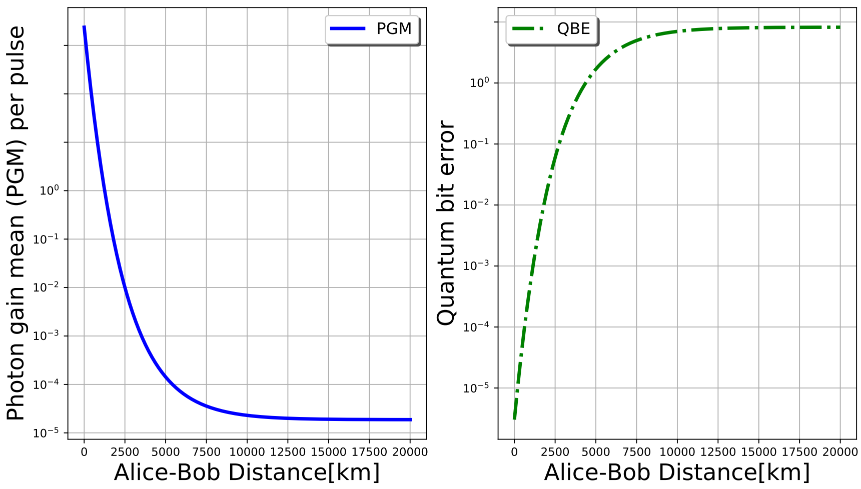
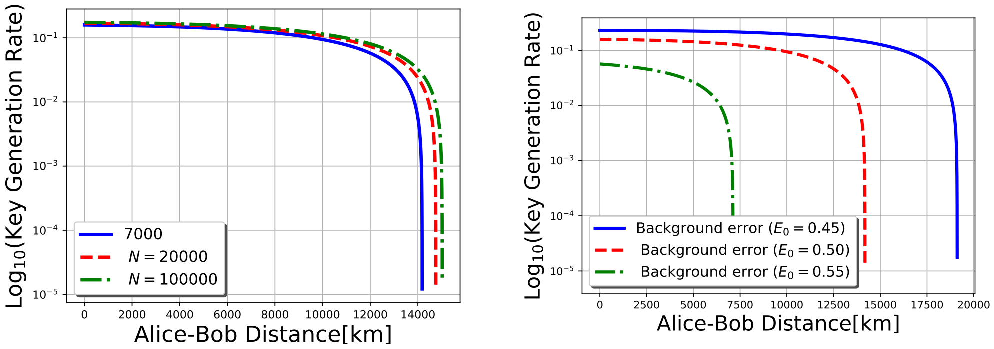


Figure 5: quantum bit error (QBE) and photon gain mean (PGM) per pulse with respect to the communication link distance between Alice's and Bob's stations, taking $E_0 = 0.5$, $E_d = 0.015$, $\eta_A = \eta_B = 0.9$, $\Upsilon_{0A} = \Upsilon_{0B} = 5.50 \times 10^{-5}$, $\nu = 0.373$, and with a maximum tolerable atmospheric link loss of $2 \times 10^{-4} dB/km$, $\varepsilon_{co} = \varepsilon_{sec} = 10^{-14}$.

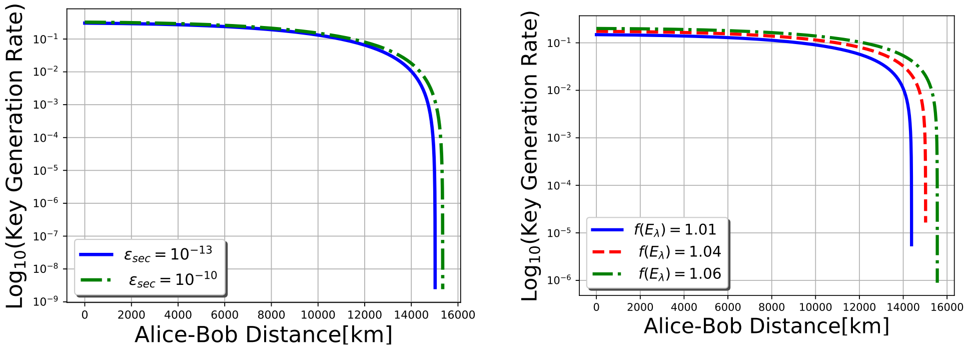
It can be observed that the PGM decreases asymptotically and very fast with almost a similar speed as the QBE increases confirming the predicted effects of noises and atmosphere diffraction on photon transfer. On the other hand, fig.6 and 7 plot the secure key generation rate with respect to the communication distance between Alice's and Bob's stations as function of the maximum photon block size (fig.6a), the background error due to atmosphere diffraction (fig.6b), the security parameter ε_{sec} (fig.7a) and the error cost function (fig.7b). The first observations lead to conclude that, with this protocol we could be able to achieve very long distance communication, since we can observe that the protocol can tolerate up to about 19000 km under lower atmosphere diffraction ($E_0 = 0.45$) as the communication distance between Alice and Bob, while for high background error ($E_0 = 0.55$), the maximum communication distance is not much significant (about 7400 km). However, most protocols whose maximum communication distances are even less than 10000 km usually considered



(a)

(b)

Figure 6: The secure key rate as function of N, the maximum photon block size (fig.6a) and the background error E_0 due to atmosphere diffraction (fig.6b) both with respect to the communication distance (L) separating Alice's and Bob's stations, considering the following parameters, $E_d = 0.015$, $\eta_A = \eta_B = 0.9$, $\Upsilon_{0A} = \Upsilon_{0B} = 5.50 \times 10^{-5}$, with a maximum tolerable atmospheric link loss of $2 \times 10^{-4} dB/km$, $n = 4 \times 10^3$, $\varepsilon_{co} = \varepsilon_{sec} = 10^{-14}$.



(a)

(b)

Figure 7: The secure key rate as function of (ε_{sec}), the security parameter (fig.7a) and the error cost function ($f(E_\lambda)$ due to key authentication (fig.7b) both with respect to the communication distance (L) separating Alice's and Bob's stations, considering the following parameters, $E_0 = 0.5$, $E_d = 0.015$, $\eta_A = \eta_B = 0.9$ $\Upsilon_{0A} = \Upsilon_{0B} = 5.50 \times 10^{-5}$, under a maximum tolerable atmospheric link loss $2 \times 10^{-4} dB/km$, with $N = 10^4$ and $n = 4 \times 10^3$, $\varepsilon_{co} = 10^{-14}$.

as background error $E_0 = 0.5$ [52, 53], and with this value it is observed that we can reach more than 14000 km with our protocol. This achievement holds under an atmosphere rate lost of about $10^{-4} dB/km$ compared to $10^{-6} dB/km$ used in existing works and we also realize that the secure key rate remains very close to 1 for long distance before decreasing quickly. In addition, as far as the photon block size sent is high, the maximum communication distance increases showing that, the protocol is robust against noise if high amount of photon can be produced form the SPDC. Similar conclusion was provided by Chun-Hui *et al.* [54]. The latest point justify the efficiency of the combined type-I and type-II SPDC photon source compared to type-I or type-II photon source separately, since it help to improve the photon block size. Fig.6b shows that the communication distance significantly improves under noiseless down-link QKD conditions. Furthermore, fig.7b clearly explains the predicted effects of error correction on the key raw length as it consists of removing from the key those bits that do not coincide, thus reducing the length of the key. These results are very similar to those found by Mizutani *et al.* [55]. It turnout therefore that, our protocol provides efficient secure key since it can tolerate very long secure communication between legitimate users. Finally, the upper bound of the secure key rate remains very closer to 1 for very long distance inducing high secure key size compared to that of existing protocols. shared

6. Concluding remarks

The present research paper was aimed at providing new strategies to achieve long distance and secure communication using satellite based QKD. For this reason, we proposed a new protocol, namely the pseudo-random bases entangled photons based QKD (PRB-EPQKD) protocol. The originality of the protocol is due to the use of the combined type-I and type-II SPDC-entangled photon pairs source located in a LEO-type satellite instead of the type-I or type-II separately on one hand. On the second hand, the legitimate communication users prepared pseudo-random bases for entangled photon pairs polarization state measurement using the QLM as PRNG. The steps for secure key generation have been provided in detail, the QBER and the secure key rate were evaluated as well. Numerical simulations showed that, the protocol can provide high secure communication between legitimate users and the maximum communication distance has been improved significantly, since we can observe that the protocol can tolerate up to about 19000 km under lower atmosphere diffraction ($E_0 = 0.45$) as the communication distance between Alice and Bob. However, most protocols whose maximum communication distances are even less than 10000 km usually considered as background error $E_0 = 0.5$ [24, 53, 56], and with this value it is observed that we can reach more than 14000 km with our protocol, which is very high compared to a maximum of 1000 km in the case of optical link QKD. Furthermore, we realized that, with our protocol the secure key rate upper bound is strongly enhanced since public discussion that is performed in other protocols for key authentication is avoided, which induced the improvement of the secure key size.

References

[1] Časlav Brukner, Marek Żukowski, and Anton Zeilinger. Quantum communication complexity protocol with two entangled qutrits. *Phys. Rev. Lett.*, 89(19):197901, 2002.

[2] Nicolai Friis, Marcus Huber, Ivette Fuentes, and David Edward Bruschi. Quantum gates and multipartite entanglement resonances realized by nonuniform cavity motion. *Phys. Rev. D*, 86(10):105003, 2012.

[3] Kiyoshi Tamaki, Hoi-Kwong Lo, Akihiro Mizutani, Go Kato, Charles Ci Wen Lim, Koji Azuma, and Marcos Curty. Security of quantum key distribution with iterative sifting. *Quantum Science and Technology*, 3(1):014002, 2017.

[4] Alexander V Sergienko. *Quantum communications and cryptography*. CRC press, 2018.

[5] Monika Jacak, Janusz Jacak, Piotr Jóźwiak, and Ireneusz Jóźwiak. Quantum cryptography: Theoretical protocols for quantum key distribution and tests of selected commercial qkd systems in commercial fiber networks. *International Journal of Quantum Information*, 14(02):1630002, 2016.

[6] Charles H Bennett and Gilles Brassard. Quantum cryptography: public key distribution and coin tossing. *Theor. Comput. Sci.*, 560(12):7–11, 2014.

[7] Artur K Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661, 1991.

[8] Charles H Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *J. Cryptol.*, 5(1):3–28, 1992.

[9] Helle Bechmann-Pasquinucci and Nicolas Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Phys. Rev. A*, 59(6):4238, 1999.

[10] Li Jun-Lin and Wang Chuan. Six-state quantum key distribution using photons with orbital angular momentum. *Chin. Phys. Lett.*, 27(11):110303, 2010.

[11] Gan Gao, Chang-Cheng Wei, and Dong Wang. Cryptanalysis and improvement of dynamic quantum secret sharing protocol based on two-particle transform of Bell states. *Quantum Inf. Process.*, 18(6):186, 2019.

[12] Sha-Sha Wang, Dong-Huan Jiang, Guang-Bao Xu, Yong-Hua Zhang, and Xiang-Qian Liang. Quantum key agreement with Bell states and Cluster states under collective noise channels. *Quantum Inf. Process.*, 18(6):190, 2019.

[13] Martin Tchoffo and Alain Giresse Tene. Entanglement dynamics of a two-qubit xyz spin chain under both dzyaloshinskii-moriya interaction and time-dependent anisotropic magnetic field. *International Journal of Theoretical Physics*, pages 1–17, 2020.

[14] Xiongfeng Ma. Quantum cryptography: theory and practice. *arXiv preprint arXiv:0808.1385*, 2008.

[15] Qinyu Xue and Rongzhen Jiao. The performance of reference-frame-independent measurement-device-independent quantum key distribution. *Quantum Inf. Process.*, 18(10):313, 2019.

[16] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling. Progress in satellite quantum key distribution. *Npj Quantum Inf.*, 3(1):1–13, 2017.

[17] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nat. Commun.*, 8:15043, 2017.

[18] Yoshiaki Tamura, Hirotaka Sakuma, Keisei Morita, et al. Lowest-ever 0.1419-db/km loss optical fiber. In *Optical Fiber Communication Conference*, pages Th5D–1. Optical Society of America, 2017.

[19] Wiley J Larson and James Richard Wertz. Space mission analysis and design. Technical report, Torrance, CA (United States); Microcosm, Inc., 1992.

[20] Juan Yin, Yuan Cao, Yu-Huai Li, et al. Satellite-to-ground entanglement-based quantum key distribution. *Phys. Rev. Lett.*, 119(20):200501, 2017.

[21] Vishal Sharma and Subhashish Banerjee. Analysis of atmospheric effects on satellite-based quantum communication: a comparative study. *Quantum Inf. Process.*, 18(3):67, 2019.

[22] Giuseppe Vallone, Davide Bacco, Daniele Dequal, et al. Experimental satellite quantum communications. *Phys. Rev. Lett.*, 115(4):040502, 2015.

[23] Nedasadat Hosseinidehaj, Zunaira Babar, Robert Malaney, Soon Xin Ng, and Lajos Hanzo. Satellite-based continuous-variable quantum communications: state-of-the-art and a predictive outlook. *IEEE Cmmun. Surv. Tut.*, 21(1):881–919, 2018.

[24] Ahmed Ismael Khaleel and Shelan Khasro Tawfeeq. Key rate estimation of measurement-device-independent quantum key distribution protocol in satellite-earth and intersatellite links. *International Journal of Quantum Information*, 16(03):1850027, 2018.

[25] Jian-Yu Wang, Bin Yang, Sheng-Kai Liao, et al. Direct and full-scale experimental verifications towards ground–satellite quantum key distribution. *Nat. Photonics*, 7(5):387, 2013.

[26] Pan Jianwei. Quantum science satellite. *Chinese Journal of Space Science*, 34:547, 2014.

[27] Juan Yin, Yuan Cao, Shu-Bin Liu, et al. Experimental quasi-single-photon transmission from satellite to earth. *Optics Express*, 21(17):20032–20040, 2013.

[28] Sebastian Nauerth, Florian Moll, Markus Rau, et al. Air-to-ground quantum communication. *Nat. Photonics*, 7(5):382, 2013.

[29] Hideki Takenaka, Alberto Carrasco-Casado, Mikio Fujiwara, et al. Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite. *Nat. Photonics*, 11(8):502, 2017.

[30] Heasin Ko, Kap-Joong Kim, Joong-Seon Choe, et al. Experimental filtering effect on the daylight operation of a free-space quantum key distribution. *Scientific Reports*, 8(1):15315, 2018.

[31] Sebastian Philipp Neumann, Siddarth Koduru Joshi, Matthias Fink, et al. Quantum communication uplink to a 3U CubeSat: Feasibility & design. *arXiv preprint arXiv:1711.03409*, 2017.

[32] Yun-Hong Gong, Kui-Xing Yang, Hai-Lin Yong, et al. Free-space quantum key distribution in urban daylight with the SPGD algorithm control of a deformable mirror. *Optics Express*, 26(15):18897–18905, 2018.

[33] Sheng-Kai Liao, Hai-Lin Yong, Chang Liu, et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nat. Photonics*, 11(8):509, 2017.

[34] Matthew P Peloso, Ilja Gerhardt, Caleb Ho, et al. Daylight operation of a free space, entanglement-based quantum key distribution system. *New J. Phys.*, 11(4):045007, 2009.

[35] Erik Kerstel, Arnaud Gardelein, Mathieu Barthelemy, et al. Nanobob: a CubeSat mission concept for quantum communication experiments in an uplink configuration. *EPJ Quantum Technol.*, 5(1):6, 2018.

[36] M Tchoffo and AG Tene. Privacy amplification of entanglement parametric-down conversion based quantum key distribution via quantum logistic map for photon bases choice. *Chaos, Solitons & Fractals*, 140:110110, 2020.

[37] Alain Giresse Tene and Timoleon Crépin Kofane. Chaos generalized synchronization of coupled mathieu-van der pol and coupled duffing-van der pol systems using fractional order-derivative. *Caos Soliton Fract.*, 98:88–100, 2017.

[38] Alain Giresse Tene and Timoleon Crépin Kofane. Novel cryptography technique via chaos synchronization of fractional-order derivative systems. In *Advanced Synchronization Control and Bifurcation of Chaotic Fractional-Order Systems*, pages 404–437. IGI Global, 2018.

[39] ME Goggin, B Sundaram, and PW Milonni. Quantum logistic map. *Phys. Rev. A*, 41(10):5705, 1990.

[40] AS Trushechkin, PA Tregubov, EO Kiktenko, et al. Quantum-key-distribution protocol with pseudorandom bases. *Phys. Rev. A*, 97(1):012311, 2018.

[41] Valerio Scarani, Antonio Acin, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys.Rev. Lett.*, 92(5):057901, 2004.

[42] Zhantong Qi, Cong Du, Xiaojuan Qin, Jindong Wang, Zhengjun Wei, and Zhiming Zhang. Improvement of the safe transmission distance via optimization of the photon number distribution for the faint optical pulse in practical quantum key distribution systems. *The European Physical Journal D*, 73(8):161, 2019.

[43] Martin Tchoffo and Alain Giresse Tene. Security and communication distance improvement in decoy states based

quantum key distribution using pseudo-random bases choice for photon polarization measurement. *Optical and Quantum Electronics*, 53(8):1–24, 2021.

[44] A Akhshani, A Akhavan, A Mobaraki, et al. Pseudo random number generator based on quantum chaotic map. *Commun. Nonlinear Sci. Numer. Simul.*, 19(1):101–111, 2014.

[45] Andrew Rukhin, Juan Soto, James Nechvatal, et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, Booz-Allen and Hamilton Inc Mclean Va, 2001.

[46] S Ali and MRB Wahiddin. Fiber and free-space practical decoy state QKD for both BB84 and SARG04 protocols. *Eur. Phys. J. D*, 60(2):405–410, 2010.

[47] L Moli-Sanchez, A Rodriguez-Alonso, and Gonzalo Seco-Granados. Performance analysis of quantum cryptography protocols in optical earth-satellite and intersatellite links. *IEEE Journal on Selected Areas in Communications*, 27(9):1582–1590, 2009.

[48] Gláucia Murta, Suzanne B van Dam, Jérémy Ribeiro, Ronald Hanson, and Stephanie Wehner. Towards a realization of device-independent quantum key distribution. *Quantum Science and Technology*, 4(3):035011, 2019.

[49] Saikat Guha, Hari Krovi, Christopher A Fuchs, Zachary Dutton, Joshua A Slater, Christoph Simon, and Wolfgang Tittel. Rate-loss analysis of an efficient quantum repeater architecture. *Phys. Rev. A*, 92(2):022357, 2015.

[50] Pavel Penchev, Stefan Dimov, and Debajyoti Bhaduri. Experimental investigation of 3D scanheads for laser micro-processing. *Optics & Laser Technology*, 81:55–59, 2016.

[51] Kyongchun Lim, Heasin Ko, Changho Suh, and June-Koo Kevin Rhee. Security analysis of quantum key distribution on passive optical networks. *Optics express*, 25(10):11894–11909, 2017.

[52] Cristian Bonato, Andrea Tomaello, Vania Da Deppo, et al. Feasibility of satellite quantum key distribution. *New J. Phys.*, 11(4):045017, 2009.

[53] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature photonics*, 7(5):378, 2013.

[54] Chun-Hui Zhang, Chun-Mei Zhang, and Qin Wang. Improving the performance of practical decoy-state measurement-device-independent quantum key distribution with biased basis choice. *Commun. Theor. Phys.*, 70(3):331, 2018.

[55] Akihiro Mizutani, Marcos Curty, Charles Ci Wen Lim, et al. Finite-key security analysis of quantum key distribution with imperfect light sources. *New J. Phys.*, 17(9):093011, 2015.

[56] Yi-Bo Zhao, Wan-Li Zhang, Dong Wang, Xiao-Tian Song, Liang-Jiang Zhou, and Chi-Biao Ding. Proof-of-principle experimental demonstration of quantum secure imaging based on quantum key distribution. *Chinese Physics B*, 28(10):104203, 2019.