Security and Communication Distance Improvement in Decoy States Based Quantum Key Distribution Using Pseudo-Random Bases Choice for Photon Polarization Measurement

Martin TCHOFFO (mtchoffo2000@yahoo.fr)
UNIVERSITY OF DSCHANG
Alain Giresse TENE
Universite de Dschang Faculte des Sciences

Research Article

Keywords: Quantum key distribution , entangled photons , decoy states , secure key size , secure key rate

Posted Date: June 25th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-634167/v1

Version of Record: A version of this preprint was published at Optical and Quantum Electronics on August 7th, 2021. See the published version at https://doi.org/10.1007/s11082-021-03124-2.

myjournal manuscript No.
(will be inserted by the editor)

Security and communication distance improvement in decoy states based quantum key distribution using pseudo-random bases choice for photon polarization measurement

TCHOFFO Martin[1,2] · **TENE Alain Giresse**[1]

Received: date / Accepted: date

Abstract This paper proposes a new quantum key distribution(QKD) protocol, namely the pseudo-random bases entangled photon based QKD (PRB-EPQKD) protocol. The latest mainly focuses on three properties, including the security of the protocol, the secure key size and the maximum communication distance between legitimate communication users (Alice and Bob). To achieve this, we first consider a spontaneous-parametric-down (SPDC) photon source located in a low-earth-orbit (LEO) type satellite capable of producing and distributing entangled photons pairs to Alice and Bob. Secondly, we assume that Alice's and Bob's photons state measurement bases are identically generated via a pseudo-random number generator (PRNG), namely the quantum logistic map (QLM). Finally, we also assume that in addition to their photons states, Alice and Bob intentionally share a set of decoy states at each pulse with randomly selected intensity, and with the goal to detect the presence of the eavesdropper (Eve). Under these considerations, the secure key rate upper bound is evaluated applying the Gottesman-Lo-Lutkenhaus-Preskill's (GLLP) formula, for two different implementations, namely the non-decoy states and the infinite active decoy states based QKD. It is observed a significant improvement in the secure key size and the communication distance as well, compared to existing protocols, since we realize that under daylight, downlinks satellite conditions, a kindly selected light source, and good crystal's properties, the maximum communication distance can reach up to 70000 km. In addition, using the combined type-I and type-II SPDC photons source as our entangled photons pairs generator, significantly improved the photon mean number and render our protocol more robust against photon number division attack and against attenuation-induced atmospheric propagation. Furthermore, the protocol is more secure as compared to existing ones, given that any eavesdropper must crack simultaneously the chaotic system used as PRNG and the QKD system, before getting any useful information as regards to the measurement bases used by Alice and Bob, and thus the secure key.

Keywords Quantum key distribution · entangled photons · decoy states · secure key size · secure key rate

PACS 03. 67. Dd, 03. 67. Hk

1 Introduction

The last few decades have known true evolution in quantum information processing theory, and several methods have been developed to protect sensitive information. Among them, one denotes quantum cryptography, very well known as quantum key distribution (QKD), which is the process of sharing a secret key for cryptography purpose between two distant partners using quantum mechanics laws [1–9]. Originated from Bennett and Brassard [1], QKD offers an unconditional security to a secure key, guaranteed by quantum physics laws, and has been already implemented in real-life experiments [1, 10–12]. However, as regards to its imperfections, a real gap between its theory and practice remains a major problem and thus, all the investigations in the field include fulfilling this gap. Hence, an eavesdropper can use this imperfection to perform an attack against the QKD module, since imperfect single photon source and detectors are commercially available to anyone, making the secrete key vulnerable. To overcome this weakness, several QKD schemes based on multiple photons source were developed [10, 13–17]. In addition, entangled photon source based QKD protocols were proved to be more secure, as compared to simple multi-photon source based QKD protocols, since the latest are vulnerable to photon splitting attack, which can be directly detected from the legitimate communication users in the entanglement based QKD protocol [18].

Indeed, in the entanglement based QKD protocol, photon pairs are produced and shared between the sender (Alice) and the receiver (Bob), usually via a spontaneous parametric down conversion (SPDC) [19–21], whose polarization orientation measurement are used for secrete key generation. Moreover, to provide unconditional security of this protocol, a decoy states source can be associated to reduce indiscreet losses and detect the presence of an eavesdropper (Eve). First introduced by Hwang [22], the decoy states based QKD enhances the performance in terms of security of a QKD protocol. Its usefulness was

[1]Department of Physics, Faculty of Science, University of Dschang, Cameroon
Dschang, P.O.Box, Cameroon
E-mail: alain.tene@aims-cameroon.org, mtchoffo2000@yahoo.fr

[2]Centre d'Etude et de Recherche en Agronomie et en Biodiversité, FASA, Université de Dschang, Cameroun
P.O.Box 67, Dschang-Cameroon

demonstrated in the contest of local and classical communication [23,24], for an imperfect photon source. Since usual QKD protocols use multi-photon source, which make them sensitive to photon number division attack as we previously mentioned, this weakness is addressed in decoy states based QKD protocol by using multiple intensity levels at the transmission source. Here, we mean that Alice transmits photons using randomly chosen intensity level, one signal state and multiple decoy states, inducing the variation of photon number statistic in the channel.

In fact, the key point of this protocol is that Alice prepares a set of states, namely decoy states in addition to photon states. The purpose of decoy states being to detect the presence of Eve intending to intercept the communication between her and Bob, while the photons states are used for the purpose of key generation. Although this protocol provides unconditional security, it does not allow long-distance communication. This is the reason why, we propose in this research paper to locate both the SPDC entangled photon source and the decoy states source into a satellite, which has the role to producing and distributing entangled photon pairs and decoy states to Alice and Bob to enhance the communication distance and used pseudo-random bases for photon polarization states measurement to enhance the key size. This process is referred to as satellite based decoy states QKD with pseudo-random bases choice for photon polarization state measurement protocol.

Indeed, this protocol is based on sharing a secret key over free-space with very lower loss rate using either a low-earth-orbit (LEO) satellite, a medium-earth-orbit (MEO) satellite or a geostationary orbit (GEO) satellite as an intermediate relay between Alice and Bob [25]. However, LEO and GEO are the most suitable candidates because of their altitude (160 to 3000 km or usually below 900 km for LEO and 35786 km precisely for GEO). Due to the proximity of LEO to the earth's surface, it is the most used to locate the photon and the decoy states source in order to reduce losses due to beam diffraction. The satellite based QKD protocol offers the possibility of achieving very long-distance communication as well as the possibility of generating highly secure key. The satellite based QKD has attracted significant interests of researchers, and has been successfully implemented in real physical experiments [21,26–33]. Although significant results have been achieved, the security of the protocol still requires deep studies. Thus, Jian-Yu *et al.* [34] 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.* [34] 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 [35] 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.* [36]. They realized a signal-to-noise ratio of 16:1, sufficient for unconditionally secure QKD links. In addition, Nauerth *et al.* [37] 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.* [38]. 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 [26,29,39–42].

Nevertheless, the above protocols mostly use true random number generators (TRNGs) for photon bases selection, which cost sifting procedure in the key rate as the legitimate users (Alice and Bob) must perform their measurement with incompatible bases choices. To overcome this weakness we, in this research paper propose to use pseudo-random number generators (PRNGs) for photon bases selection which has already been successfully demonstrated in the case of optical link QKD by Trushechkin et al. [43], with the randomness guaranteed by the Legendre symbols. We thus, suggest a new protocol that uses quantum chaotic systems as the PRNG which can be easily implemented and strongly improve the efficiency of the QKD protocol security. If this protocol namely, pseudo-random bases entangled photon based QKD (PRB-EPQKD) is successfully implemented in photonics, it will significantly enhance the efficiency of the quantum key sharing process due to random-like behavior and high sensitivity to initial conditions of chaotic systems [44,45]. We therefore, assume our random bases choice to be guaranteed by the quantum logistic map (QLM) [46], the SPDC-photon source to be our entangled photons generator and a decoy states source 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 model formalism, where the SPDC entangled photon Hamiltonian is presented and the wave function including the probability distribution are deduced. In Sec.3, the procedure of generating pseudo-random bases for photons polarization state measurement using QLM as the PRNG is developed. It follows in Sec.4 with the decoy states based satellite-to-earth link QKD protocol. We present in Sec.5 the main results and discussion, and we end the work with some concluding remarks presented in Sec.6.

2 Model formalism: photon wave function and probability distribution

2.1 SPDC entangled photons source Hamiltonian

Entanglement based QKD usually uses entangled photons, due to the fact that their polarization state may be assimilated to quantum bits. As previously mentioned, SPDC has widely been investigated in the literature as a key resource for QKD [47–49]. Its Hamiltonian may be derived from classical electromagnetic energy in nonlinear media as follows [48,49]:

$$H = \frac{1}{8\pi}\int B^2(r,t)d^3r + \frac{1}{8\pi}\int d^3r \int_0^{D(r,t)} E(r,t)dD, \tag{1}$$

where B and E are the magnetic and the electrical fields, respectively. The parameters r and t are respectively the temporal and spatial variables. D the charge displacement defined by $D = \varepsilon E + 4\pi P^{NL}$, ε being the permittivity, P^{NL} the nonlinear polarization given by [48,49]:

$$P_k^{NL} = \eta_{kp}^{(1)}(\omega_1,\omega_2)E_p(\omega_1) + \eta_{kpq}^{(2)}(\omega_1,\omega_1-\omega_2)E_p(\omega_1)E_q(\omega_2) + \cdots, \tag{2}$$

where $\eta_{kp}^{(1)}(\omega_1,\omega_2)$ and $\eta_{kpq}^{(2)}(\omega_1,\omega_1-\omega_2)$ are respectively a two and three dimensional tensors depending on the frequencies ω_1, ω_2. The indices p and q denote the output photon pairs mode, and k that of the incident photon. Considering Eq. (2), the Hamiltonian (1) becomes:

$$H = \frac{1}{8\pi}\int B^2(r,t)d^3r + \frac{1}{8\pi}\int E^2(r,t)d^3r + \int d^3rX_1(r) + \int d^3rX_2(r) + \cdots, \tag{3}$$

with $X_1(r) = 2\pi\int\int d\omega_1 d\omega_2 \eta_{kp}^{(1)}E_k(r,\omega_1)E_p(r,\omega_2)$ and $X_2(r) = \frac{4\pi}{3}\int\int\int d\omega_1 d\omega d\omega_2 \eta_{kpq}^{(2)}E_k(r,\omega_1)E_p(r,\omega-\omega_2)E_q(r,\omega_2)$.

The first two terms of Eq. (3) introduces the total energy of the system, the remaining terms being the linear term. But due to the fact that we are interested on entangled photon pairs, we will only focus on the nonlinear term to define the interaction energy of the light source with the crystal. In the interaction picture, the type-I or type-II SPDC effective Hamiltonian can be written in the rotative-wave approximation and neglecting the reflection from the crystal surface as follows [48]:

$$H_I = \int_v \eta_{kpq}E_k^+E_p^-E_q^- + H.c. \tag{4}$$

Using the following transformation,

$$E_p^-(\omega) = \sum_k E_{pk}a_{pk}^+e^{i(kr-w_{pk}t)},\ E_q^-(\omega) = \sum_k E_{qk}b_{qk}^+e^{-i(kr-w_{qk}t)}, \tag{5}$$

with $E_{pk} = i\sqrt{\frac{\omega_{pk}}{2n_{pk}V}}$, $E_{qk} = i\sqrt{\frac{\omega_{qk}}{2n_{qk}V}}$, a_{pk}^+ and b_{qk}^+ being the creation operators in p and q modes satisfying the following commutation relation: $[a_{pk},a_{mn}^+] = [b_{pk},b_{mn}^+] = \delta_{pm}\delta_{kn}$. The three dimensional tensor η_{kpq} defines the dielectric susceptibility and V the crystal volume. Assuming the pump field to be a classical plane wave, we have $E_k^+ = E_0\exp(kr-\omega t)$. Considering the latest relation and Eq. (5), the Hamiltonian (4) becomes:

$$H_I = i\kappa a_p^+b_q^+ + H.c., \tag{6}$$

with the indices p and q denoting respectively the photons mode as previously mentioned which also define their polarization orientation that may be horizontal or vertical. Thus, the degenerated Hamiltonian can be rewritten taking into consideration the above assumptions as [50]:

$$H_I = i\kappa(a_h^+b_h^+ + a_v^+b_v^+ + a_h^+b_v^+ - a_v^+b_h^+) + H.c., \tag{7}$$

where κ is a parameter containing the field pump amplitude and the crystal's properties, h and v denote the polarization direction standing for horizontal and vertical, respectively. H.c. stands for the Hermitian conjugate. The Hamiltonian (7) is written in the limit $\hbar \to 1$, with the operators a and b satisfying $[a_i,a_j] = [a_i^+,a_j^+] = [b_i,b_j] = [b_i^+,b_j^+] = [a_i,b_j] = 0$ and $[a_i,a_j^+] = [b_i,b_j^+] = \delta_{ij}$, $i \in \{h,v\}$. It denotes the combined type-I and type-II SPDC Hamiltonian. The next subsection evaluates the corresponding wave function and the density probability.

2.2 Wave function and probability density

Following the procedure described by Truax [51], one can easily derive the wave function and the probability distribution, associated to Eq. (7) giving the Hamiltonian of entangled photon pairs in two different modes. For this reason, let $U(t)$ be the evolution operator, thus in the time independent Shrödinger picture, one has:

$$U(t) = \exp(-iH_It) = \exp\{\kappa t(a_h^+b_h^+ + a_v^+b_v^+ + a_h^+b_v^+ - a_v^+b_h^+) + H.c.\}, \tag{8}$$

with $U(t_0) = U(0) = I$ (identity operator). The photon state is found by acting the operator $U(t)$ to the vacuum as follows:

$$|\Psi(t)\rangle = U(t)|0\rangle_{ab} = U(t)(\alpha|0_h0_h\rangle_{a_hb_h} + \beta|0_h0_v\rangle_{a_hb_v} + \gamma|0_v0_h\rangle_{a_vb_h} + \vartheta|0_v0_v\rangle_{a_vb_v}), \tag{9}$$

with
$|0\rangle_{ab} = \alpha|0_h0_h\rangle_{a_hb_h} + \beta|0_h0_v\rangle_{a_hb_v} + \gamma|0_v0_h\rangle_{a_vb_h} + \vartheta|0_v0_v\rangle_{a_vb_v}$, the vacuum in the most general form, α, β, γ and ϑ the probabilities to find the states $|0_h0_h\rangle_{a_hb_h}$, $|0_h0_v\rangle_{a_hb_v}$, $|0_v0_h\rangle_{a_vb_h}$ and $|0_v0_v\rangle_{a_vb_v}$ respectively, so that $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\vartheta|^2 = 1$. Let us introduce two operators T_+ and T_- defined by,

$$\begin{cases} T_+ = a_h^+b_h^+ + a_v^+b_v^+ + a_h^+b_v^+ - a_v^+b_h^+ = T_-^\dagger, \\ T_- = a_hb_h + a_vb_v + a_hb_v - a_vb_h = T_+^\dagger, \end{cases} \tag{10}$$

and satisfying the following commutation relations,
$[T_-,T_+]=4T_0$, $[T_0,T_\pm]=\pm T_\pm$, with $T_0=\frac{1}{2}(a_h^+a_h+a_v^+a_v+b_h^+b_h+b_v^+b_v+2)=T_0^\dagger$. Thus, Eq. (8) becomes:

$$U(t)=\exp\{\chi T_+-\chi^* T_-\}, \tag{11}$$

with $\chi=\kappa t$, implying that,

$$|\Psi\rangle=\exp\{\chi T_+-\chi^* T_-\}|0\rangle. \tag{12}$$

In order to explicitly determine the wave function of Eq. (12), let us introduce two unitary operators $U_1(\lambda)$ and $U_2(\lambda)$ defined by:

$$\begin{cases} U_1(\lambda)=\exp\{\lambda(\chi T_+-\chi^* T_-+i\theta T_0)\},\\ U_2(\lambda)=\exp\{\Lambda_+(\lambda)T_+\}\exp\{\Lambda_0(\lambda)T_0\}\exp\{\Lambda_-(\lambda)T_-\}, \end{cases} \tag{13}$$

and require $U_1(\lambda)$ to be equal to $U_2(\lambda)$ and subject to initial conditions $\Lambda_i(0)=0$. It is easy to verify that $U_1(\lambda)$ and $U_2(\lambda)$ are unitary, given that λ is always real. The main goal here is to evaluate the functions $\Lambda_+(\lambda)$, $\Lambda_0(\lambda)$ and $\Lambda_-(\lambda)$, subject to the initial conditions $\Lambda_i(0)=0$ and $U_1(0)=U_2(0)=I$. That is, let us differentiate $U_1(\lambda)$ and $U_2(\lambda)$ with respect to λ and equal their results, thus we obtain:

$$\begin{aligned}(\chi T_+-\chi^* T_-+i\theta T_0)U_1(\lambda)&=(\chi T_+-\chi^* T_-+i\theta T_0)U_2(\lambda)\\ &=\Lambda_+' T_+e^{\Lambda_+T_+}e^{\Lambda_0T_0}e^{\Lambda_-T_-}+\Lambda_0' e^{\Lambda_+T_+}T_0e^{\Lambda_0T_0}e^{\Lambda_-T_-}+\Lambda_-' e^{\Lambda_+T_+}e^{\Lambda_0T_0}T_-e^{\Lambda_-T_-}.\end{aligned} \tag{14}$$

Given that $U_2^{-1}(\lambda)=\exp\{-\Lambda_-(\lambda)T_-\}\exp\{-\Lambda_0(\lambda)T_0\}\exp\{\Lambda_+(\lambda)T_+\}$, multiplying Eq. (14) from the right by the latest relation, we obtain:

$$\begin{aligned}\chi T_+-\chi^* T_-+i\theta T_0&=\Lambda_+' T_++\Lambda_0' e^{\Lambda_+T_+}T_0e^{-\Lambda_+T_+}++\Lambda_-' e^{\Lambda_+T_+}e^{\Lambda_0T_0}T_-e^{-\Lambda_0T_0}e^{-\Lambda_+T_+}\\ &=\Lambda_+' T_++(T_0-\Lambda_+T_+)\Lambda_0'+\Lambda_-' e^{-\Lambda_0}T_--4\Lambda_-' e^{-\Lambda_0}T_0+2\Lambda_-'\Lambda_+^2e^{-\Lambda_0}T_+,\end{aligned} \tag{15}$$

where we have used the Baker-Campbell-Hausdorff (BCH) commutation relations [51]. Identifying the coefficients of the respective basis elements (T_-,T_0,T_+) of the Lie algebra leads to the following set of first order differential equations.

$$\begin{cases} \Lambda_-'=-\chi^* e^{\Lambda_0},\\ \Lambda_0'=i\theta-4\chi^*\Lambda_+,\\ \Lambda_+'=\chi+i\theta\Lambda_+-2\chi^*\Lambda_+^2, \end{cases} \tag{16}$$

where the solution for $\theta=0$ is given by,

$$\begin{cases} \Lambda_-=\frac{\chi}{\sqrt{2}|\chi|}\tanh(\sqrt{2}\mid\chi\mid\lambda),\\ \Lambda_0=-2\log(\cosh(\sqrt{2}\mid\chi\mid\lambda)),\\ \Lambda_+=-\frac{\chi^*}{\sqrt{2}|\chi|}\tanh(\sqrt{2}\mid\chi\mid\lambda). \end{cases} \tag{17}$$

Based on the latest relation, with $\lambda=1$, the wave function (12) can be easily written as:

$$\begin{aligned}|\Psi\rangle&=\exp\{\frac{\chi}{\sqrt{2}\mid\chi\mid}\tanh(\sqrt{2}\mid\chi\mid)T_+\}\exp\{-2\log(\cosh(\sqrt{2}\mid\chi\mid))T_0\}\exp\{-\frac{\chi^*}{\sqrt{2}\mid\chi\mid}\tanh(\sqrt{2}\mid\chi\mid)T_-\}|0\rangle\\ &=\frac{1}{\cosh^2(\sqrt{2}\mid\chi\mid)}\sum_{n=0}^{\infty}\frac{\chi^*}{\mid\chi\mid}\sqrt{(n+1)(\alpha^{2n}+\beta^{2n}+\gamma^{2n}+\vartheta^{2n})}\left(\tanh(\sqrt{2}\mid\chi\mid)\right)^n|\Phi_n\rangle,\end{aligned} \tag{18}$$

where

$$\begin{aligned}|\Phi_n\rangle=\frac{1}{(n+1)\sqrt{\alpha^{2n}+\beta^{2n}+\gamma^{2n}+\vartheta^{2n}}}\sum_{k=0}^{n}&[\alpha^n|k_h,k_h\rangle_a|(n-k)_v,(n-k)_v\rangle_b\\ &+\beta^n(-1)^{n-k}|k_h,(n-k)_v\rangle_a|(n-k)_v,k_h\rangle_b\\ &+\gamma^n(-1)^k|(n-k)_v,k_h\rangle_a|k_h,(n-k)_v\rangle_b\\ &+\vartheta^n|(n-k)_v,(n-k)_v\rangle_a|k_h,k_h\rangle_b].\end{aligned} \tag{19}$$

One can easily verify that, for $\alpha=\vartheta=0$, $\beta=\gamma=\frac{1}{\sqrt{2}}$ and $n=1$, we get the Bell state [52] $|\Phi_1\rangle=\frac{1}{\sqrt{2}}[|10\rangle_a|01\rangle_b-|01\rangle_a|10\rangle_b]$ or if $\alpha=\vartheta=\frac{1}{\sqrt{2}}$, $\beta=\gamma=0$ and $n=1$, we get $|\Phi_1\rangle=\frac{1}{\sqrt{2}}[|00\rangle_a|11\rangle_b+|11\rangle_a|00\rangle_b]$, which are maximally entangled states. Thus, we are sure that the produced photon pairs are always entangled. Relations (18) and (19) have been derived considering that $\exp(qT_-)|0\rangle\equiv|0\rangle$, $\exp(pT_0)|0\rangle\equiv\exp(p)$ and $\exp(qT_+)|0\rangle\equiv\sum_{k=0}^{\infty}\frac{q^k}{k!}(T_+)^k|0\rangle$, with the vacuum $|0\rangle$ defined in Eq. (9).

Let P_j be the probability density to generate j entangled photon pairs, therefore

$$P_j = |\langle \Phi_j | \Psi \rangle|^2 = \frac{1}{\cosh^4(\sqrt{2}\,|\,\chi\,|)}(j+1)\tanh^{2j}(\sqrt{2}\,|\,\chi\,|). \tag{20}$$

Setting $\lambda = \sinh^2(\sqrt{2}\,|\,\chi\,|)$, the photon mean number, depending only on the crystal's properties and the light pulse amplitude, we get

$$P_j = (j+1)\frac{\lambda^j}{(1+\lambda)^{j+2}}. \tag{21}$$

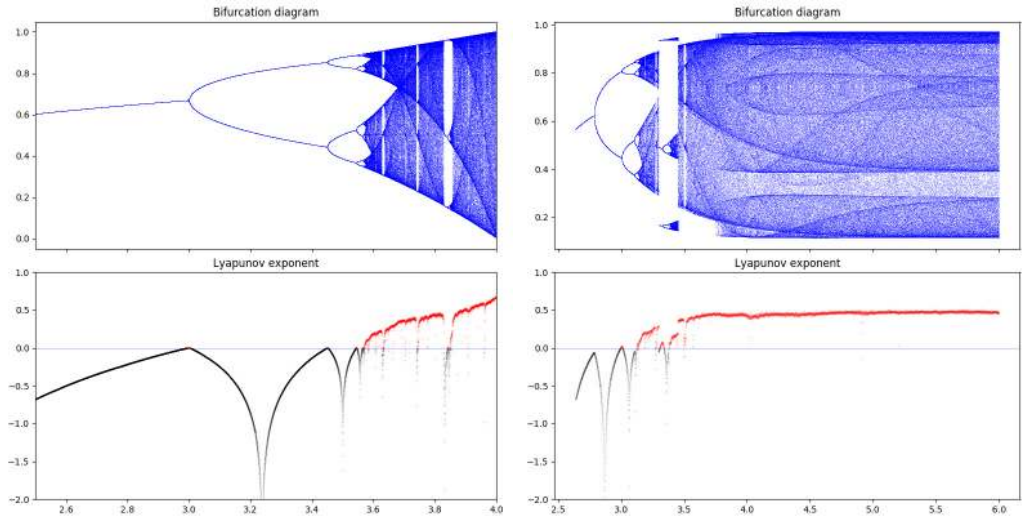
It follows that, photons probability distribution coincides with Poisson distribution showing that the produced photon pairs are independent each other. Similar equation has already been obtained by Ma *et al* [47], but with different photon mean number.

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

Usual QKD protocols mostly provide the condition of randomly choice of the bases in which quantum states are encoded, requiring the legitimate parties (Alice and Bob) to use true random number generator (TRNG). However, this cost sifting procedure and leads to loss of almost a half of the key raw. In order to avoid this drawback, new protocols that use PRNs instead of TRNs have been introduced [53–55]. QKD associated with PRNs for quantum state preparation and post-processing procedures might provide high secure encryption key. Limited number of PRNGs exist, among them chaotic systems have been found to be an efficient tool for the purpose. For this reason, the present subsection briefly describes the procedure of generating pseudo-random bit sequence (PRBS) associated to photon state polarization based on quantum logistic map (QLM) for QKD purpose. First introduced by Goggin *et al.* [46], QLM is a system where a quantum kick rotator is coupled to a bath of harmonic oscillator. It was demonstrated that, under quantum error corrections, the system may be treated as classical system, where its dynamics is described by [43]:

$$\begin{cases} x_{k+1} = r(x_k - |x_k|^2) - ry_k, \\ y_{k+1} = -y_k e^{-2s} + re^{-s}[(2 - x_k - x_k^*)y_k - x_k z_k^* - x_k^* z_k], \\ z_{k+1} = -z_k e^{-2s} + re^{-s}[2(1 - x_k)z_k - 2x_k y_k - x_k], \end{cases} \tag{22}$$

with $x = \overline{a}$, $y = \overline{\delta a^\dagger \delta a}$, $z = \overline{\delta a \delta a}$, x^*, z^* the complex conjugate of x and z, respectively. $a(a^\dagger)$ are the annihilation (creation) bosonic operators, $\delta a(\delta a^\dagger)$ the quantum fluctuation associated to the operators a and $a^\dagger$, respectively. The parameters r and s are the bifurcation parameters. Fig.1 depicts the bifurcation diagram of the QLM with respect to r (Fig.1a) and s (Fig.1b). It is



(a) (b)

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

observed that, all the values of x always fall in the interval $[0,1]$ and display period doubling showing that our system depicts chaotic behavior, with r and s kindly selected i.e. $4 \geq r > 3.85$ and $s \geq 3.5$. It is important to mention that, x_k belong to a set of real number given real initial conditions of system (22). Similar figures can be obtained for variables y and z, which also exhibit chaotic behavior and always fall in the interval $[0,1]$. We notice that, the variables x, y and z which help to define the set of Eq. (23) 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. (23), and thus cannot quietly perform the polarization state measurement. Therefore, system (22) provide an efficient and secure PRNG for quantum state encoded bases in the QKD protocols. The procedure to generate these pseudo-random bases 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 (22), the following sequence is obtained, $S = \{1111111\cdots0100011000111011111010111011\}$. Based on the NIST STP randomness test [56], we 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:

$$B_i = \left\{ |\phi_{s_k^i}\rangle, |\phi_{s_k^i} + \frac{\pi}{2}\rangle \right\}, \text{ with } \phi_{s_k^i} = \frac{s_k^i \pi}{2} 2^{-s_k^i}, \qquad i = A, B, \tag{23}$$

where $s_k^i = \{0,1\}_{k=1,2,\cdots,N}$. 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:

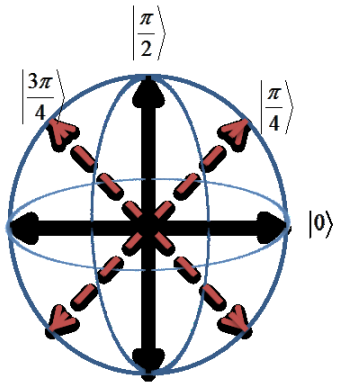


Fig. 2: Polarization state measurement pseudo-random rotation bases.

4 Decoy states based satellite-to-earth link QKD protocol

As previously mentioned, decoy states QKD is one of the most implementation quantum key sharing scheme, since it provides more security as compared to the protocol without decoy states. This is due to the fact that, additionally to the usual BB84 states that are used in standard QKD protocol, decoy states are also produced and shared between the QKD legitimate users (Alice and Bob), with an exclusive role of detecting the presence of any eavesdropper (Eve). However, in the existing QKD protocols with decoy states [22–24, 57], authors usually use single photon source at the transmitter's side, which is not easily implementable. In addition, both the transmitter and the receiver perform their photon polarization state measurement with true randomly selected bases, and by the way their outcome measurement are identical with $\frac{1}{2}$ probability. But in the new protocol that we wish to implement, one of the main objectives is to solve this issue by using PRNG for photon polarization measurement bases choice.

Here, the steps that Alice(transmitter) and Bob (receiver) need to perform in order to generate a full private encryption key via satellite based QKD are presented in detail. 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:

- **Step 1:** Alice and Bob first agree on the bifurcation parameters range (r and s), the initial conditions x_0, y_0 and z_0 describing the PRNG given by system (22). Also, they agree on the number of iterations N needed to run their PRNG.
- **Step 2:** Via a SPDC-photon source located in a LEO-type satellite with an automate commend on Alice's possession, Alice runs the SPDC module and produces a pair of entangled photons at each pulse, while at the same time she produces decoy sates using a multi-intensity laser source also located in the same satellite. Thus, those entangled photons pairs are shared through atmospheric propagation between her and Bob, additionally to the random-like selected decoy states intensity. The

latest will help them in detecting whether the entangled photon sent has been intercepted or not. Having done that, the following steps have to be performed:

(i) Upon receiving, both Alice and Bob measure the intensity level of the received decoy states, and thus they notify each to other the reception of the half entangled photon pair sent, using classical communication (telephone, fax, etc.) and the intensity of decoy states into their possession. Ubiquitously, if the signal has not been intercepted during the sending process by an untrusted parties (Eve), Alice and Bob should detect the decoy states sent with identical intensity level. In case those conditions are not simultaneously satisfied, Alice repeat **Step 2** until these conditions are fulfilled.

(ii) Under the condition that (i) is satisfied, Both Alice and Bob run their QLM systems N times to generate pseudo-random bases for photon polarization measurement, following the procedure fully described in Sec.3.

(iii) Alice and Bob perform a polarization state measurement on the half of entangled photon pair in their possession, in the bases they generated from (ii), and note the result somewhere.

(iv) Following the output of the state polarization measurement, Alice and Bob assign a bit "1" for horizontal polarization and the bit "0" for vertical polarization, if the selected basis is Z (i.e. $B_{A/B} = \{|0\rangle, |\frac{\pi}{2}\rangle\}$), while they assign a bit "1" for 45^0-polarization and the bit "0" for 135^0-polarization, if the selected basis is X (i.e. $B_{A/B} = \{|\frac{\pi}{4}\rangle, |\frac{3\pi}{4}\rangle\}$), as shown on Fig.2

(v) Alice and Bob keep the results of (iv) in two initially empty sequences S_A for Alice and S_B for Bob. In addition, Bob measures the bit error rate (BER) and notifies the result to Alice, if it is not significant, they abort the process and repeat again **Step 2**.

Step 3: They thus, increment the value of r by step of $\varepsilon = \frac{r_{max} - r_{min}}{N}$, if r is selected as the control parameter, or that of s by $\varepsilon = \frac{s_{max} - s_{min}}{N}$, if s is selected as the control parameter, and repeat **Step 2**.

Step 4: Alice and Bob repeat **Step 2** and **Step 3** N times, and at each times pair of entangled photons and decoy states should be produced and shared between them.

Step 5: Alice and Bob end up with two sequences S_A for Alice and S_B for Bob, which should be identical and extremely secret, that they can now use to encrypt a message. The procedure is summarized on Fig.3.

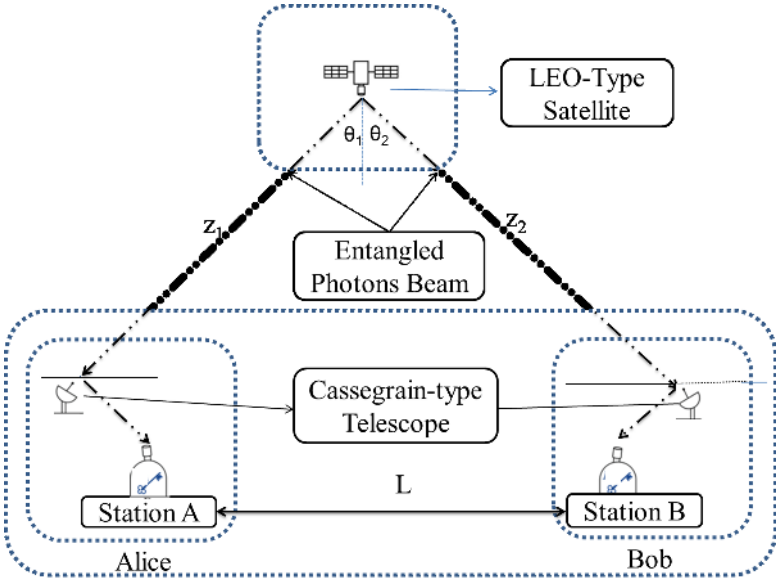


Fig. 3: LEO-type satellite based QKD scheme, with each station containing a photon detector device, a photon polarization state measurement device and a photon beam splitter as the procedure require single photon measurement.

In Fig. 3, 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.

5 Free-space key rate estimation results and discussion

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 [58–61],

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 as presented on Fig. 3. It is important to mention that, the almost non-birefringent character of the atmosphere guarantees the preservation of photon pairs polarization state [58,59,61]. 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:

$$\eta_{atm} = \eta_{abs}\eta_{scatt}\eta_{turb}, \tag{24}$$

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 [58,59, **?**]. 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 [59,62–64]. It causes divergence rate of the light beam, and is evaluated following the work of Moli-Sanchez *et al.* [59] by:

$$\eta_{turb} = \frac{1}{1+\frac{\theta_{turb}^2 R_t^2}{\lambda^2}}, \tag{25}$$

with $\theta_{turb} = \frac{\lambda}{\pi\omega_0}$ the additional divergence angle in radian due to 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 depend on the satellite-to-ground distance in additional to other telescope's parameters. Fig.4a depicts the Cassegrain-type telescope's principle to be 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 [27,65]. Under these assumptions, the attenuation rate due to diffraction can be calculated following refs. [27,65, 66] as:

$$\eta_{diff} = \left[\exp\left(-2\frac{r_t^2}{w_t^2}\right) - \exp\left(-2\frac{R_t^2}{w_t^2}\right)\right]\left[\exp\left(-2\frac{r_r^2}{w_r^2}\right) - \exp\left(-2\frac{R_r^2}{w_r^2}\right)\right] \tag{26}$$

where the subscript t refers to the transmit telescope and r to the receive one; R and r are the radii of the primary and secondary mirrors, respectively; λ is the light wavelength; $\omega_{t,r}$ is the beam radius at the transmit or 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 [67], 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 as presented on Fig.4b. 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,

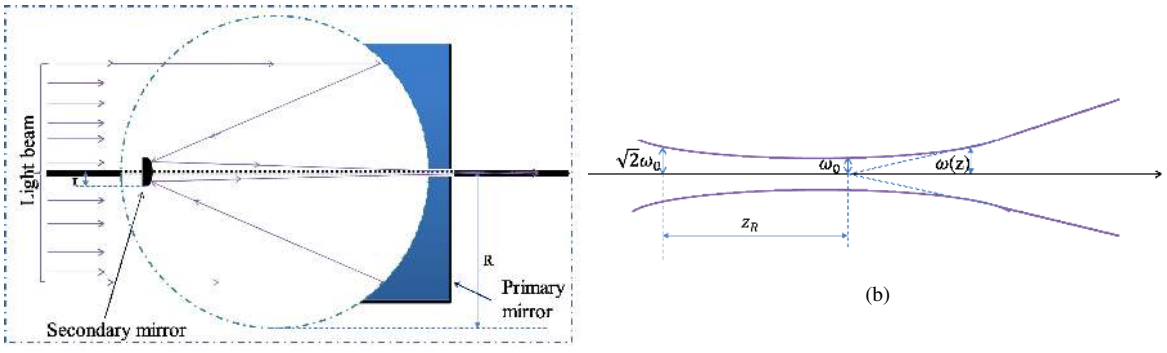


Fig. 4: Cassegrain-type telescope (Fig.4a) and Gaussian beam width $\omega(z) = \omega_r$ in terms of the axial distance z, the Rayleigh length z_R and ω_0 the beam waist (Fig.4b).

which is realistic in particular for the transmitter. Eq. (26) 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:

$$\begin{cases} T_A = \eta_{err}\eta_{atm}\varepsilon_A\eta_{diff}^A, \\ T_B = \eta_{err}\eta_{atm}\varepsilon_B\eta_{diff}^B, \end{cases} \tag{27}$$

where ε_A and ε_B define respectively the detector efficiencies of Alice's and Bob's detectors. From Fig.3 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:

$$L = \sqrt{z_1^2 + z_2^2 + 2z_1z_2\cos(\theta)}. \tag{28}$$

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

$$\begin{cases} z_1 = \frac{1}{\cos(\theta_1)}\frac{L}{\tan(\theta_1)+\tan(\theta_2)}, \\ z_2 = \frac{1}{\cos(\theta_2)}\frac{L}{\tan(\theta_1)+\tan(\theta_2)}, \end{cases} \tag{29}$$

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 assumptions, the overall transmittance of i-photon pairs between Alice and Bob can be defined as follows:

$$T_i = \left[1-(1-T_A)^i\right]\left[1-(1-T_B)^i\right]. \tag{30}$$

Given that, dark count may occur (i.e. detection occurring on Alice's and Bob's sides given zero photon), the probability that a quantum state is transmitted given a quantum state is a conditional probability also known as the yield, and given by:

$$\begin{aligned} \Upsilon_n &= [T_n + \Upsilon_{0A} - \Upsilon_{0A}T_n][T_n + \Upsilon_{0B} - \Upsilon_{0B}T_n] \\ &= [1-(1-\Upsilon_{0A})(1-T_A)^n][1-(1-\Upsilon_{0B})(1-T_B)^n], \end{aligned} \tag{31}$$

where, Υ_{0A} and Υ_{0B} introduces the dark count probability on Alice's and Bob's side, respectively. Moreover, we must recall that for each photon pulse, a set of decoy states should be also produced and exchange between Alice and Bob. Thus, the probability that Alice's and Bob's detectors indicate a detection of j-photons coming out of the SPDC photon source can be derived as:

$$P_j = \sum_{i=1}^{\infty}(i+1)\frac{\lambda^i}{(1+\lambda)^{i+2}}p_{j/i}, \tag{32}$$

where $p_{j/i}$ represents the conditional probability for Alice's and Bob's detector to indicate simultaneously j-photon states given an incoming i-photon states. In this case, only two options are to be considered: (i) the case of triggered (i.e. $j=1$) and (ii) that of non-triggered events (i.e. $j=0$). For non-triggered event, $p_{0/i} = (1-T_A)^i(1-T_B)^i$ and for triggered events, $p_{1/i} = 1-(1-T_A)^i(1-T_B)^i$. Considering these assumptions we have two different situations to be considered during the key rate estimation: the case of non-decoy states with threshold detector and that of infinite number decoy states with threshold detector.

5.1 Key rate estimation in case of non-decoy states with threshold detector

Let Q_j^λ and E_j^λ be the overall photon gain and the quantum bit error rate (QBER), respectively. Then, one has:

$$\begin{cases} Q_j^\lambda = \sum_{i=0}^{\infty} Q_{i,j}^\lambda = \sum_{i=0}^{\infty} P_i(\lambda)p_{j/i}\Upsilon_i \\ E_j^\lambda Q_{i,j}^\lambda = Q_{i,j}e_i \end{cases} \tag{33}$$

where $P_i(\lambda)$ is given by Eq. (21), Υ_i by Eq. (31), and e_i defining the error rate given by [68]:

$$e_i = q_0 - 2\frac{q_0-q_d}{(i+1)\Upsilon_i}\left[\frac{1-(1-T_A)^{i+1}(1-T_B)^{i+1}}{1-(1-T_A)(1-T_B)} - \frac{(1-T_A)^{i+1}-(1-T_B)^{i+1}}{T_B-T_A}\right], \tag{34}$$

with q_0 the background count error rate, and q_d the intrinsic detector error rate. After some computations, we get:

$$Q_0^\lambda = \frac{1}{[1+\lambda T_A+\lambda T_B-\lambda T_A T_B]^2} - \frac{1-\Upsilon_{0A}}{[1+\lambda T_B+\lambda T_A(2-T_A)(1-T_B)]^2} - \frac{1-\Upsilon_{0B}}{[1+\lambda T_A+\lambda T_B(2-T_B)(1-T_A)]^2} + \frac{(1-\Upsilon_{0A})(1-\Upsilon_{0B})}{[1+\lambda+\lambda(1-T_A)^2(1-T_B)^2]^2}, \tag{35}$$

and

$$Q_1^\lambda = 1 - \frac{1-\Upsilon_{0A}}{[1+\lambda T_A]^2} - \frac{1-\Upsilon_{0B}}{[1+\lambda T_B]^2} + \frac{(1-\Upsilon_{0A})(1-\Upsilon_{0B})}{[1+\lambda T_A+\lambda T_B-\lambda T_A T_B]^2} - Q_0^\lambda, \tag{36}$$

$$\begin{cases} E_0^\lambda Q_0^\lambda = Q_{1,0} e_1, \\ E_1^\lambda Q_1^\lambda = Q_{1,1} e_1, \end{cases} \tag{37}$$

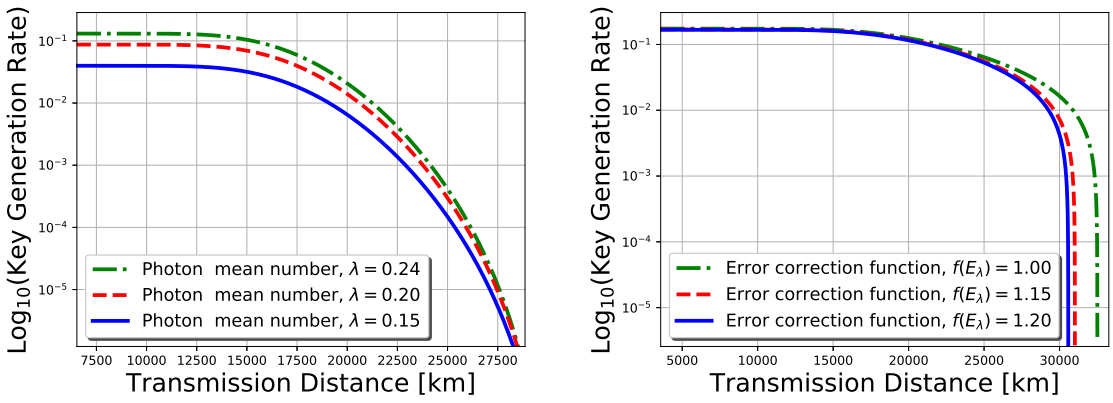
where

$$\begin{cases} Q_{1,0} = P_1(\lambda) p_{0/1} \Upsilon_1 = 2\frac{\lambda}{(1+\lambda)^3}(1-T_A)(1-T_B)\Upsilon_1, \\ Q_{1,1} = P_1(\lambda) p_{1/1} \Upsilon_1 = 2\frac{\lambda}{(1+\lambda)^3}\Upsilon_1 - Q_{1,0}. \end{cases} \tag{38}$$

By applying the Gottesman-Lo-Lutkenhaus-Preskill's (GLLP) relationship giving the upper bound of the secure key rate, one has [18,68,69]:

$$R \geq R^{lim} = \sum_{j=0}^{1} \left[-f(E_j^\lambda) Q_j^\lambda H_2(E_j^\lambda) + Q_{1,j}\,(1-H_2(e_1)) \right], \tag{39}$$

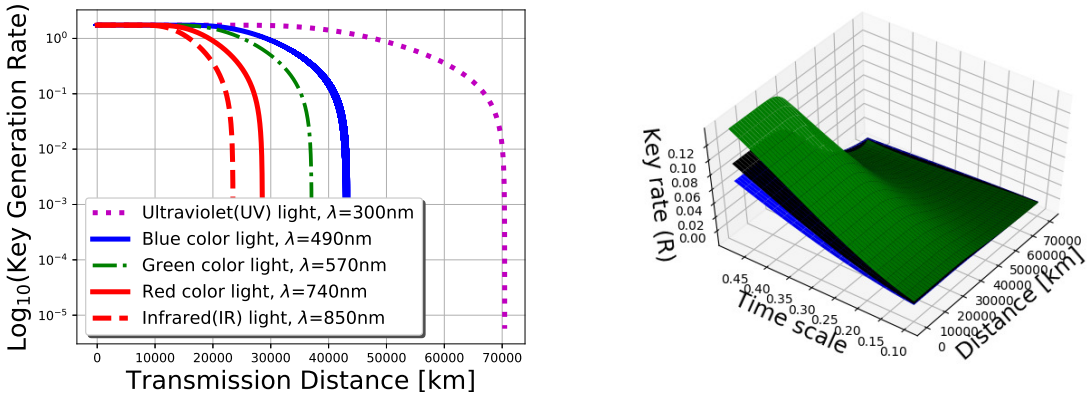
where $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ introduces the usual Shanon binary entropy function, $f(E_j^\lambda)$, $j = 0,1$, the error correction cost function, which is lower in our protocol as compared to that of the usual BB84 protocols, provided that this protocol avoids public discussion for bases reconciliation, source of errors in the existing protocols. Fig.5 depicts the secure key rate with respect to the communication distance.



(a) (b)

Fig. 5: Non decoy states based PRB-EPQKD protocol secure key rate simulation as function of λ, the maximum photon mean number (Fig.5a) and the error correction function, $f(E_\lambda)$ (Fig.5b), both with respect to the communication distance (L) separating Alice's and Bob's stations, considering the background error $q_0 = 0.5$, the detectors' error $q_d = 1.5\%$, and the dark count error rate $\Upsilon_{0A} = \Upsilon_{0B} = 1.5 \times 10^{-3}$. The light used for entangled photons pairs production being the orange color light with wavelength $\mu = 650nm$, with the telescopes' radii, $r_t = 10mm$, $R_t = 20mm$, $r_r = 0.01mm$, $R_r = 2m$, and $\omega_0 = 2mm$.

From Fig.5a representing the secure key rate with respect to the communication distance, it can be observed an increasing in the secure key size when the photon mean number λ increases. This observation is due to the fact that, when the number of exchanged entangled photons pairs between Alice and Bob is high enough, the protocol becomes more robust against photon number splitting attack. Moreover, the secure key rate of the protocol goes to 1 as the photon mean number increases, which implies that, when the number of exchanged photon during the process is very large, the effects of noise due turbulence-induced atmospheric propagation become negligible such that the entire photons pairs produced by the SPDC reach the recipients (Alice and Bob). Ma *et al.* [70,71] demonstrated that in the entanglement based QKD protocols, the optimal photon mean number is 0.24, and that is the reason we choose this value and its neighborhood in our simulations, with its maximum set to 0.24. In addition, Fig.5b plots the secure key rate as function of different error correction functions. As discussed in several existing



(a) (b)

Fig. 6: Non decoy states based PRB-EPQKD protocol secure key rate simulation for different wavelengths (i.e. type of light used for entangled photons pairs production), with respect to the communication distance (L) between Alice's and Bob's stations (Fig.6a) and the three dimensional simulation of the secure key rate with respect to both the pulse time scale ($\chi = \kappa t$, $\kappa = 0.5$ for blue/bottom panel, $\kappa = 0.6$ for black/middle panel and $\kappa = 0.7$ for green/top panel), and the communication distance (L) separation Alice's and Bob's stations (Fig.6b), considering the error correction function, $f(E_\lambda) = 1.1$, the background error $q_0 = 0.5$, the detectors' error $q_d = 1.5\%$, and the dark count error rate $\Upsilon_{0A} = \Upsilon_{0B} = 1.5 \times 10^{-3}$, with the telescopes' radii, $r_t = 10mm$, $R_t = 20mm$, $r_r = 0.01mm$, $R_r = 2m$, and $\omega_0 = 2mm$.

QKD protocols [26,28,58,60,62], upon receiving half of entangled photons pairs, and measuring their polarization, Alice and Bob must communicate each to other the measurement bases selected through untrusted classical channel and cancel the bits that photons measurement bases do not coincide. This procedure leads to sifting and may cost up to half of the key raw. Thus, an efficient algorithm was proposed to minimize the error occurring during this procedure. That is, it was then proved that this error is function of the QBER and may be constant despite the QKD protocol used, with an optimal value of 1.22 [70,71]. However, in our protocol (PRB-EPQKD protocol), as we already mentioned, public discussion between Alice and Bob as regard to the measurement bases reconciliation is avoided, since they are certain to perform their measurement in identical bases provided the bases generation process developed in Sec.3. The only public discussions that do not even reveal any useful information to Eve concern the photon reception. Given the above considerations, it comes that the error-induced bases reconciliation is negligible, and thus the error correction function should be less than that of the existing protocols. For this reason, we have simulated our secure key rate under this consideration, and the results proved that this protocol is far better as regard to both the maximum communication distance between legitimate users and the secure key size. Furthermore, we have looked forward to observe the effects of different color light that can be used for entangled photons pairs production on the secure key, by simulating the secure key rate with respect to different wavelength selected in the ultraviolet light, visible light or infrared light wavelength range. It turns out that, entangled photons pairs produced via an ultraviolet light source will be more robust against noise-induced atmospheric attenuation, and thus cover more distance as compared to others. This observation is corroborated by Fig. 6a. From Fig.6b plotting the secure key rate simultaneously with respect to the communication distance and the pulse time scale, we realize that the secure key rate strongly depends on the nature of crystal that is being used for entangled photons pairs production during the process, since it can be observed that as the value of κ, which reveals the crystal's properties increases, the secure key rate increases significantly. However, although this protocol, namely non-decoy states based PRB-EPQKD significantly improves the communication distance, as it reaches up to a maximum of 70000 km, providing the quality of light used (UV), the error correction function, the nature of the crystal kindly selected, it provides less security as compared to the case with infinite active decoy states, developed in the following subsection.

5.2 Key rate estimation in the case of infinite decoy states with threshold detector

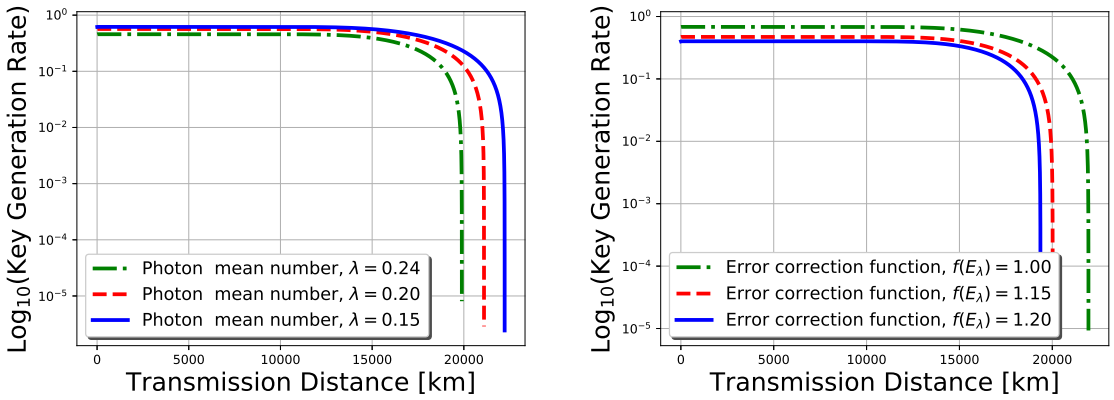
Analogically to the case of non-decoy states with threshold detector based QKD, the secure key rate in the present case can still be evaluated using Eq. (39). However the overall QBER E_j^λ, j=0,1 are evaluated as follows:

$$\begin{aligned} E_0^\lambda Q_0^\lambda &= \sum_{i=0}^{\infty} P_i(\lambda) p_{0/i} \Upsilon_i e_i \\ &= q_0 Q_0^\lambda - 2\frac{q_0 - q_d}{1+\lambda}\left[\frac{\frac{1}{1-(1-T_A)(1-T_B)}}{1+\lambda T_A+\lambda T_B-\lambda T_A T_B} - \frac{\frac{1-T_A}{T_B-T_A}}{1+\lambda T_B+\lambda T_A(2-T_A)(1-T_B)}\right] \\ &\quad - 2\frac{q_0 - q_d}{1+\lambda}\left[\frac{\frac{1-T_B}{T_B-T_A}}{1+\lambda T_A+\lambda T_B(2-T_B)(1-T_A)} - \frac{\frac{(1-T_A)(1-T_B)}{1-(1-T_A)(1-T_B)}}{1+\lambda-\lambda(1-T_A)^2(1-T_B)^2}\right], \end{aligned} \tag{40}$$

and

$$
\begin{aligned}
E_1^{\lambda}Q_1^{\lambda} &= \sum_{i=0}^{\infty} P_i(\lambda)p_{1/i}\Upsilon_i e_i \\
&= q_0(Q_0^{\lambda}+Q_1^{\lambda}) - E_0^{\lambda}Q_0^{\lambda} - 2\frac{q_0-q_d}{1+\lambda}\left[\frac{1}{1-(1-T_A)(1-T_B)} - \frac{\frac{1-T_A}{T_B-T_A}}{1+\lambda T_A} + \frac{\frac{1-T_B}{T_B-T_A}}{1+\lambda T_B}\right] \\
&- 2\frac{q_0-q_d}{1+\lambda}\left[-\frac{(1-T_A)(1-T_B)}{1-(1-T_A)(1-T_B)}\frac{1}{1+\lambda T_A+\lambda T_B-\lambda T_A T_B}\right],
\end{aligned} \tag{41}
$$

The quantum gain of non-triggered and that of triggered events Q_0^{λ} and Q_1^{λ}, respectively are evaluated analogically to those of eqs.(35) and (36). The parameters of these equations are defined in the previous section, but the main difference resides in the evaluation of the QBER, which takes into consideration, the infinite number of decoy states exchanged between Alice and Bob. Fig. 7 depicts the secure key rate with respect to the communication distance.

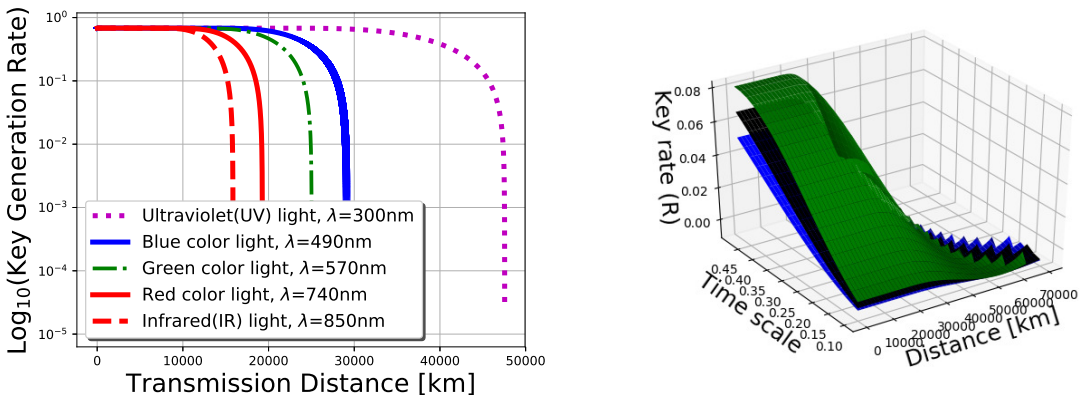


(a) (b)

Fig. 7: Infinite active decoy states based PRB-EPQKD protocol secure key rate simulation as function of λ, the maximum photon mean number (Fig.7a) and the error correction function, $f(E_\lambda)$ (Fig.7b), both with respect to the communication distance (L) separating Alice's and Bob's stations, considering the background error $q_0 = 0.5$, the detectors' error $q_d = 1.5\%$, and the dark count error rate $\Upsilon_{0A} = \Upsilon_{0B} = 1.5\times10^{-3}$. The light used for entangled photons pairs production being the orange color light with wavelength $\mu = 650nm$, with the telescopes' radii, $r_t = 10mm$, $R_t = 20mm$, $r_r = 0.01mm$, $R_r = 2m$, and $\omega_0 = 2mm$.

In Fig.7 plotting the secure key rate with respect to the communication distance for different values of the photon mean number (Fig.7a) and for different values of the error correction function (Fig.7b), for the case of infinite active decoy states, similar observations as in the case of non-decoy states can be made, as regard to the maximum communication distance as well as the secure key size, since these quantities are improved significantly compared to those of existing protocols. Although the communication distance does not reach that of non-decoy states protocol as shown on Fig. 5, the security is quietly enhanced here due to the use of decoy states, since as we previously mentioned, Alice and Bob share additionally to their photon states some set of decoy states with random intensity, the goal being to detect the presence of Eve intending to intercept their communication. However, it can be observed that the maximum communication distance is significantly improved in the case of infinite active decoy states as compared to that of one or two decoy states as developed by several authors (see for example refs. [58,59]).

It is worth noticing that these results may not always coincide with security analyses found in the literature, for example refs. [72–74], since these works present their security analyses under the assumption of some Eve's generic capabilities. But here, we consider Eve being able to listen to all the communication taking place between Alice and Bob during the process, and can even be able to intercept their entangled photons pairs. Under this consideration, she is not able to extract any useful information as regard to the secret key, since the legitimate users do not communicate their measurement bases. This point is one of the most important results of this protocol and contributes to its strong security. We recall that this fact is due to the use of PRNG instead of TRGN for photon state polarization measurement bases choice. In addition, when attenuation due to atmospheric turbulence increases, Eve's action becomes very difficult to detect. In this situation, Alice and Bob must modulate the photon mean number as presented on Figs. 5a and 7a, so to make the photons, travelling throughout atmosphere more robust against noises. Thus, the robustness of the protocol includes large value of photon mean number too, which remains constant in the case of non-decoy states protocol as well as in the case of infinite active decoy states protocol. This result is in agreement with that of ref.[59]. From Fig. 8 depicting the secure key rate in terms of the transmission distance between Alice and Bob for different nature of the light source used for photon pairs creation (Fig. 8a), and in terms of simultaneously the time scale and the transmission distance for different type of crystal used for photon pairs creation (Fig.8b), similar conclusion as in the case of non-decoy state can be drawn (shown on Fig.6). It is also important to mention that these results are achieved under daylight and downlink satellite conditions, and the main effects that influence the communication distance are due to turbulence-induced attenuation. Nevertheless, the



(a) (b)

Fig. 8: Infinite active decoy states based PRB-EPQKD protocol secure key rate simulation for different wavelengths (i.e. nature of light used for entangled photons pairs production), with respect to the communication distance (L) between Alice's and Bob's stations (Fig.8a) and the three dimensional simulation of the secure key rate with respect to both the pulse time scale ($\chi = \kappa t$, $\kappa = 0.5$ for blue/bottom panel, $\kappa = 0.6$ for black/middle panel and $\kappa = 0.7$ for green/top panel), and the communication distance (L) separation Alice's and Bob's stations (Fig.8b), considering the error correction function, $f(E_\lambda) = 1.1$, the background error $q_0 = 0.5$, the detectors' error $q_d = 1.5\%$, and the dark count error rate $\Upsilon_{0A} = \Upsilon_{0B} = 1.5 \times 10^{-3}$, with the telescopes' radii, $r_t = 10mm$, $R_t = 20mm$, $r_r = 0.01mm$, $R_r = 2m$, and $\omega_0 = 2mm$.

attenuation due to absorption and scattering is evaluated considering the model of standard atmosphere [27,75], which results in $\eta_{scatt} = 1dB$ and $\eta_{abs} = 8dB$. Furthermore, we have considered the background noise caused by daylight, and which present significant impact on the QBER and consequently on the secure key. Similar observations were made by Er-long *et al.* in [76].

6 Concluding remarks

This paper's purpose was to theoretically develop a new QKD protocol, namely the pseudo-random bases entangled photon based quantum key distribution (PRB-EPQKD) protocol. The main goal of the latest being to improve not only the security as regards to the key sharing process, but also to improve the communication distance between legitimate users and the secure key size as well. For this reason, we first assumed a SPDC photon source capable of producing and distributing entangled photons pairs to Alice and Bob, and located in a LEO-type satellite. Secondly, we ensured that Alice's and Bob's photons state measurement bases are identically generated via a PRNG, namely the QLM. Thirdly, we have also assumed that in addition to their photons state, Alice and Bob intentionally share a set of decoy states at each pulse with randomly selected intensity, and with the goal to detect the presence of the eavesdropper (Eve), intending to listen to their communication. Under the above considerations, the secure key rate upper bound has been evaluated applying the GLLP relationship, for two different implementations, namely the non-decoy states and the infinite active decoy states based QKD. Four (04) main points was observed from simulations:

(i) The secure key size was strongly improved with the increasing of the photon mean number, which traduces the robustness of the protocol against photon number splitting attack, and additionally its robustness against attenuation-induced atmospheric propagation of photons.

(ii) The communication distance between legitimate users significantly improved, with decreasing in the error correction function, which shows the efficiency of the protocol, as it minimize the errors due to absence of public discussion between Alice and Bob usually performed in existing QKD protocols.

(iii) The secure key rate was found to decrease very weakly with the communication distance, and strongly impacted by the nature of light used for entangled photons pairs production, since for ultraviolet light source, we observed that the maximum communication distance achieved can reach up to 70 000 km, against a maximum of 40 000 km for visible light source, while for infrared light source it can reach only a maximum of 25000 km.

(iv) The crystal's properties that is used for entangled photons pairs production strongly impact the secure key size and the communication distance as well.

Therefore, as recommendation for any practical implementation, one should make sure to kindly select the light source nature and an appropriate crystal that will be used in the SPDC for entangled photons pairs production. These aspects, even important as we realized in this work, are neglected to best of our knowledge in existing protocols. In addition, daylight and downlink satellite conditions were found to minimize the attenuation-induced atmospheric turbulence effects, which are the most cause of errors in the protocol, and thus can be recommended.

Conflict of interest

The authors declare that they have no conflict of interest.

References

1. Charles H Bennett and Gilles Brassard. Proceedings of the IEEE international conference on computers, systems and signal processing, 1984.
2. Fu-Guo Deng and Gui Lu Long. Bidirectional quantum key distribution protocol with practical faint laser pulses. *Phys. Rev. A*, 70(1):012311, 2004.
3. Michel Boyer, Dan Kenigsberg, and Tal Mor. Quantum key distribution with classical Bob. In *2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07)*, pages 10–10. IEEE, 2007.
4. Xi-Han Li, Fu-Guo Deng, and Hong-Yu Zhou. Efficient quantum key distribution over a collective noise channel. *Phys. Rev. A*, 78(2):022321, 2008.
5. Gan Gao. Quantum key distribution by comparing Bell states. *Opt. Commun.*, 281(4):876–879, 2008.
6. Gao Gan. Quantum key distribution scheme with high efficiency. *Commun. Theor. Phys.*, 51(5):820, 2009.
7. Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108(13):130503, 2012.
8. Li-Hua Gong, Han-Chong Song, Chao-Sheng He, Ye Liu, and Nan-Run Zhou. A continuous variable quantum deterministic key distribution based on two-mode squeezed states. *Physica Scripta*, 89(3):035101, 2014.
9. Xiuqing Yang, Kejin Wei, Haiqiang Ma, Shihai Sun, Hongwei Liu, Zhenqiang Yin, Zuohan Li, Shibin Lian, Yungang Du, and Lingan Wu. Measurement-device-independent entanglement-based quantum key distribution. *Phys. Rev. A*, 93(5):052303, 2016.
10. Artur K Ekert. Quantum cryptography based on Bells theorem. *Phys. Rev. Lett.*, 67(6):661, 1991.
11. Momtchil Peev, Christoph Pacher, Romain Alléaume, Claudio Barreiro, Jan Bouda, W Boxleitner, Thierry Debuisschert, Eleni Diamanti, M Dianati, JF Dynes, et al. The SECOQC quantum key distribution network in vienna. *New J. Phys.*, 11(7):075001, 2009.
12. Masahide Sasaki, M Fujiwara, H Ishizuka, W Klaus, K Wakui, M Takeoka, S Miki, T Yamashita, Z Wang, A Tanaka, et al. Field test of quantum key distribution in the Tokyo QKD network. *Optics express*, 19(11):10387–10409, 2011.
13. Jian Li, Hong-Fu Zhou, Lu Jia, and Ting-Ting Zhang. An efficient protocol for the private comparison of equal information based on four-particle entangled W state and Bell entangled states swapping. *International Journal of Theoretical Physics*, 53(7):2167–2176, 2014.
14. Charles H Bennett, Gilles Brassard, and N David Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68(5):557, 1992.
15. Charles H Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *J. Cryptol.*, 5(1):3–28, 1992.
16. 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.
17. Li Jun-Lin and Wang Chuan. Six-state quantum key distribution using photons with orbital angular momentum. *Chin. Phys. Lett.*, 27(11):110303, 2010.
18. Xiongfeng Ma and Hoi-Kwong Lo. Quantum key distribution with triggering parametric down-conversion sources. *New J. Phys.*, 10(7):073018, 2008.
19. Qiang Zhang, Feihu Xu, Yu-Ao Chen, Cheng-Zhi Peng, and Jian-Wei Pan. Large scale quantum key distribution: challenges and solutions. *Optics Express*, 26(18):24260–24273, 2018.
20. Qinyu Xue and Rongzhen Jiao. The performance of reference-frame-independent measurement-device-independent quantum key distribution. *Quantum Inf. Process.*, 18(10):313, 2019.
21. Robert Bedington, Juan Miguel Arrazola, and Alexander Ling. Progress in satellite quantum key distribution. *Npj Quantum Inf.*, 3(1):1–13, 2017.
22. Won-Young Hwang. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.*, 91(5):057901, 2003.
23. Stéphane Félix, Nicolas Gisin, André Stefanov, and Hugo Zbinden. Faint laser quantum key distribution: eavesdropping exploiting multiphoton pulses. *J. Mod. Opt*, 48(13):2009–2021, 2001.
24. M Ferrero, TW Marshall, and E Santos. Bells theorem: Local realism versus quantum mechanics. *Am. J. Phys*, 58(7):683–688, 1990.
25. Wiley J Larson and James Richard Wertz. Space mission analysis and design. Technical report, Torrance, CA (United States); Microcosm, Inc., 1992.
26. Juan Yin, Yuan Cao, Yu-Huai Li, et al. Satellite-to-ground entanglement-based quantum key distribution. *Phys. Rev. Lett.*, 119(20):200501, 2017.
27. Vishal Sharma and Subhashish Banerjee. Analysis of atmospheric effects on satellite-based quantum communication: a comparative study. *Quantum Inf. Process.*, 18(3):67, 2019.
28. Imran Khan, Bettina Heim, Andreas Neuzner, and Christoph Marquardt. Satellite-based QKD. *Optics and Photonics News*, 29(2):26–33, 2018.
29. Giuseppe Vallone, Davide Bacco, Daniele Dequal, et al. Experimental satellite quantum communications. *Phys. Rev. Lett.*, 115(4):040502, 2015.
30. Wei Zhao, Qin Liao, Duan Huang, and Ying Guo. Performance analysis of the satellite-to-ground continuous-variable quantum key distribution with orthogonal frequency division multiplexed modulation. *Quantum Inf. Process.*, 18(1):39, 2019.
31. Vishal Sharma and Subhashish Banerjee. Analysis of quantum key distribution based satellite communication. In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–5. IEEE, 2018.
32. 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.
33. Sheng-Kai Liao, Jin Lin, Ji-Gang Ren, et al. Space-to-ground quantum key distribution using a small-sized payload on Tiangong-2 Space Lab. *Chin. Phys. Lett.*, 34(9):090302, 2017.
34. 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.
35. Pan Jianwei. Quantum science satellite. *Chinese Journal of Space Science*, 34:547, 2014.
36. 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.
37. Sebastian Nauerth, Florian Moll, Markus Rau, et al. Air-to-ground quantum communication. *Nat. Photonics*, 7(5):382, 2013.
38. 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.
39. 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.
40. 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.
41. 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.
42. 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.
43. 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.
44. 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. *Chaos Soliton Fract.*, 98:88–100, 2017.
45. 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.
46. ME Goggin, B Sundaram, and PW Milonni. Quantum logistic map. *Phys. Rev. A*, 41(10):5705, 1990.

47. Xiongfeng Ma, Chi-Hang Fred Fung, and Hoi-Kwong Lo. Quantum key distribution with entangled photon sources. *Phys. Rev. A*, 76(1):012307, 2007.
48. Ruo Peng Wang and Hui Rong Zhang. Theory for quantum state of photon pairs generated from spontaneous parametric down-conversion nonlinear process. *Opt. Spectrosc.*, 103(1):148–152, 2007.
49. Yong-Chun Liu, Yun-Feng Xiao, You-Ling Chen, et al. Parametric down-conversion and polariton pair generation in optomechanical systems. *Phys. Rev. Lett.*, 111(8):083601, 2013.
50. Martin Tchoffo and Alain Giresse Tene. Privacy amplification of entanglement parametric-down conversion based quantum key distribution via quantum logistic map for photon bases choice. *Chaos Soliton Fract.*, 140:110110, 2020.
51. D Rodney Truax. Baker-Campbell-Hausdorff relations and unitarity of SU(2) and SU(1, 1) squeeze operators. *Phys. Rev. D*, 31(8):1988, 1985.
52. 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.
53. AS Trushechkin, PA Tregubov, EO Kiktenko, et al. Quantum-key-distribution protocol with pseudorandom bases. *Phys. Rev. A*, 97(1):012311, 2018.
54. Hoi-Kwong Lo, Hoi Fung Chau, and Mohammed Ardehali. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.*, 18(2):133–165, 2005.
55. 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.
56. 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.
57. 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.
58. 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.
59. 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.
60. Markus Aspelmeyer, Thomas Jennewein, Martin Pfennigbauer, Walter R Leeb, and Anton Zeilinger. Long-distance quantum communication with entangled photons using satellites. *IEEE J. Sel. Top. Quantum Electron*, 9(6):1541–1551, 2003.
61. Ahmed Ismael Khaleel and Shelan Khasro Tawfeeq. Key rate estimation of measurement-device-independent quantum key distribution protocol in satellite-earth and intersatellite links. *Int. J. Quantum Inf.*, 16(03):1850027, 2018.
62. John G Rarity, PR Tapster, PM Gorman, and Peter Knight. Ground to satellite secure key exchange using quantum cryptography. *New J. Phys.*, 4(1):82, 2002.
63. Scott Bloom, Eric Korevaar, John Schuster, and Heinz Willebrand. Understanding the performance of free-space optics. *Journal of Optical Networking*, 2(6):178–200, 2003.
64. Shlomi Arnon. Effects of atmospheric turbulence and building sway on optical wireless-communication systems. *Optics Letters*, 28(2):129–131, 2003.
65. Bernard J Klein and John J Degnan. Optical antenna gain. 1: Transmitting antennas. *Applied Optics*, 13(9):2134–2141, 1974.
66. 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.
67. Pavel Penchev, Stefan Dimov, and Debajyoti Bhaduri. Experimental investigation of 3D scanheads for laser micro-processing. *Optics & Laser Technology*, 81:55–59, 2016.
68. Hoi-Kwong Lo and Norbert Lütkenhaus. Quantum cryptography: from theory to practice. *arXiv preprint quant-ph/0702202*, 2007.
69. Daniel Gottesman, H-K Lo, Norbert Lutkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. In *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings.*, page 136. IEEE, 2004.
70. Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72(1):012326, 2005.
71. Xiongfeng Ma, Chi-Hang Fred Fung, Frédéric Dupuis, Kai Chen, Kiyoshi Tamaki, and Hoi-Kwong Lo. Decoy-state quantum key distribution with two-way classical postprocessing. *Phys. Rev. A*, 74(3):032330, 2006.
72. Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys*, 81(3):1301, 2009.
73. Chi-Hang Fred Fung, Kiyoshi Tamaki, and Hoi-Kwong Lo. Performance of two quantum-key-distribution protocols. *Phys. Rev. A*, 73(1):012337, 2006.
74. Barbara Kraus, Cyril Branciard, and Renato Renner. Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses. *Phys. Rev. A*, 75(1):012316, 2007.
75. Louis Elterman. Parameters for attenuation in the atmospheric windows for fifteen wavelengths. *Applied optics*, 3(6):745–749, 1964.
76. Miao Er-long, Han Zheng-fu, Gong Shun-sheng, Zhang Tao, Diao Da-Sheng, and Guo Guang-Can. Background noise of satellite-to-ground quantum key distribution. *New J. Phys.*, 7(1):215, 2005.