Performance Analysis of Quantum Cryptography Protocols in Optical Earth-Satellite and Intersatellite Links

L. Moli-Sánchez, A. Rodríguez-Alonso, G. Seco-Granados

***Abstract*—In this paper we analyze the feasibility of performing Quantum Key Distribution (QKD), in earth-satellite up and downlinks and in intersatellite links, with two quantum cryptography protocols: BB84 and SARG04, and with two implementation options: with and without decoy states. As real measurements in these scenarios are not possible yet, the objective is to obtain results as realistic as possible to support the design of future satellite missions performing QKD. Therefore, we use realistic values for the optical hardware and take into account usual atmospheric conditions. In the same line, we assume specific types of attacks, namely the photon number splitting and the intercept-resend with unambiguous discrimination attacks, which could likely be the main threat to the first satellite-based QKD applications. A lower bound on the key generation rate of SARG04 with two decoy states is presented. The optimum signal- and decoy-states mean photon numbers for each protocol and each distance are also computed. The resulting values for the signal-state are larger than those often employed. We show that it may be possible to establish QKD with LEO (Low Earth Orbit) and, under certain circumstances, with MEO (Medium Earth Orbit) satellites, but not with GEO (Geostationary) ones. Furthermore, we obtain that the optimum signal-state mean photon number for SARG04 with two decoy states is almost independent of the link distance, which greatly facilitates its use in a real scenario.**

***Index Terms*—Quantum cryptography, satellite secure communications, decoy states, SARG04 protocol.**

I. Introduction

THE CAPABILITIES of satellite technology revolutionized communications, permitting easier and faster data transfers between arbitrarily distant parts of the world. Since the ancient civilizations, information privacy has been one of the main human challenges, and technology development has lead to the invention of several methods to preserve the security of the communications. Nowadays, the promise of quantum computers threatens the security of current methods of cryptography. The quantum theory can be applied to cover this loophole. In the last decades, the science community has focused its efforts in Quantum Cryptography, developing new quantum cryptography protocols, performing complex experiments and showing that Quantum Key Distribution (QKD) is the only physically secure way of sharing secret information between two partners [1]. The best known QKD protocol is the BB84, published by Bennett and Brassard in 1984 [2]. Its security is based on the existence of single photon sources. Although there are intense experimental efforts towards the design of single photon sources, they are not available yet. At the moment, the best alternative is an attenuated laser source, which provides pulses with a number of photons following a Poisson distribution. The existence of multiple-photon pulses can be exploited by an eavesdropper (Eve). One of the most powerful attacks against the BB84 protocol is the so-called Photon Number Splitting (PNS) attack. In a high-attenuation channel, Eve may extract full information about the key. In order to guarantee security in front of these attacks, new protocols have appeared: SARG04 [3], B92 [4] and 4+2 protocols [5]. The decoy-states method, first proposed by Hwang [6], has represented an important innovation in this area. This method proposes to introduce extra test states (denoted as decoy states) to evaluate the action of the eavesdropper. The decoy states method has been successfully applied to the BB84 protocol [7], [8], [9], [10], increasing the achievable distances and the key generation rates. Up to date the most relevant experiments in quantum cryptography have been performed using this method [11]. On the contrary, the application of the decoy-states method with protocols other than the BB84 is at best at an early stage. In this paper, we present a bound of the key generation rate for SARG04 protocol using a finite number of decoy states.

Due to the limitations of the propagation along optical fibers, QKD over fibers can only reach a few hundred of kilometers [12], [13]. Free-space links permit to increase this distance (see e.g. [11]) thanks to the low absorption of the atmosphere in certain wavelength ranges and to its nonbirefringent character, which guarantees the conservation of the polarization. However, terrestrial free-space links suffer from attenuation caused by the atmosphere and objects in the line of view. In order to fully exploit the potential of free-space communications, satellites should be used. Thus, significant improvements in the QKD range could be obtained since, in an earth-satellite link, only around 30 kilometers of the propagation path (the exact length depending on the satellite elevation) are inside the atmosphere.

The organization of the paper is as follows. In Section II, we describe the link characteristics and the assumptions applicable to the rest of the study. For the sake of completeness, brief analyses of BB84 and SARG04 are provided in Sections III and IV. In Section V, first we review the decoy-states method as applied to the BB84 with the vacuum and a weak decoy state. Next, we introduce and analyze our proposal of using

Manuscript received 16 January 2009; revised 15 May 2009. This work was supported by the Spanish Government under projects TEC2008-06305 and EXPLORA ESP2006-26372-E, the Catalan Government under grant 2009 SGR 298, and the Chair of Knowledge and Technology Transfer Parc de Recerca UAB - Santander.

The authors are with Telecommunications and System Engineering Department, Universitat Autònoma de Barcelona, 08193 Bellaterra, Barcelona, Spain, (e-mail: gonzalo.seco@uab.es).

Digital Object Identifier 10.1109/JSAC.2009.091208.

SARG04 with the vacuum and two weak decoy states. Section VI contains the numerical results. In the last section, the main results are summarized and conclusions are drawn.

II. Link characteristics

In this section we examine the link characteristics considered for the analysis of the quantum channel attenuation. Channel attenuation is mainly caused by beam diffraction, atmospheric attenuation and detector (in)efficiency. Furthermore, we assume that the dark counts of the detector are the only source of quantum bit errors, which are quantified by the quantum bit error ratio (QBER). On the one hand, this assumption implicitly implies that the transmitter (Alice) and receiver (Bob) have perfectly agreed on the measurement basis states. Carrying out this basis alignment with the accuracy required to cause negligible impairment is a technical challenge. Recent terrestrial implementations (see e.g. [11], [14]) have used a parallel tracking channel to stabilize the link, which could also be exploited to align the bases. Time synchronization between transmitter and receiver is also crucial [1], [15]. The parallel channel could also be used for this goal; however, in those recent implementations, the transmitter and receiver clocks have been synchronized be means of the Global Positioning System (GPS). As GPS can be used in satellites as well, this is probably the preferred solution for an eventual experiment in the near future. Further practical implementation aspects are beyond the scope of the paper but can be found in the references just provided. On the other hand, we have omitted the background radiation as another cause of bit errors. Although this radiation is always present, there are techniques to reduce its effect to a level ideally lower than that of the dark counts [16]. We have considered that it is realistic to take for granted that a potential QKD experiment in space will make use of those state-of-the-art techniques to achieve the best possible background noise mitigation.

A. Photon source and Receiver

Quantum cryptography protocols assume that single photon sources are available, but current technology only allows us to generate weak coherent states (usually represented as $\left|\sqrt{\mu}e^{i\theta}\right\rangle$; see [1] for an introduction on the *bracket* notation) using attenuated laser sources [17], [18]. Assuming that the phase of all signals is totally random, the probability distribution of the number of photons follows a Poisson distribution with mean μ, which is the mean number of photons per pulse. That is to say, the probability that the number of photons in a pulse sent by Alice be equal to n is $P_n(\mu) = e^{-\mu}\mu^n/n!$ [13]. The existence of multi-photon pulses may allow Eve to perform some attacks without being detected by Alice and Bob.

Imperfections in receivers, like low detector efficiency, additional losses and intrinsic dark counts, are some of the main limiting factors in QKD since these factors make the action of an eavesdropper possible. Detector efficiency is improving continuously. Recent developments have shown the possibility of having detectors with 95% efficiency in the near-infrared region [19]. However, the effective receiver efficiency (or attenuation), which we denote by δ_{rec}, is not only composed of the detector efficiency but also of the filtering and other transmission losses [15]. Although detector efficiency is becoming closer to one, the effective receiver efficiency is still well below one [14]. Dark counts do not impact the receiver attenuation, but can lead to false identification of signals, especially at low rates.

B. Channel attenuation

The total channel attenuation, represented by $\delta \in [0,1]$, can be obtained from the contributions of the three effects mentioned above: diffraction (also known as geometric losses), atmospheric propagation and receiver efficiency. Note that δ actually represents a gain (i.e. the reciprocal of an attenuation), but it is usually referred to as attenuation with some abuse of the language. The smaller the value of δ, the more attenuation is present between transmitter and receiver. For the sake of completeness, here we briefly present each effect but, for a more detailed analysis, readers are referred to [1], [20].

We assume that conventional telescope architectures, like the Cassegrain type, are used both in the transmitting and receiving sides, and that the laser beams are Gaussian as it is common practice [21], [22]. Cassegrain telescopes are of reflective type, in which the secondary mirror produces a central obscuration. Moreover, their finite dimensions and the distance between them are responsible for the beam diffraction. The attenuation due to beam diffraction and obscuration can be expressed as [23], [24]

$$\delta_{diff} = \left(e^{-2\gamma_t^2\alpha_t^2} - e^{-2\alpha_t^2}\right)\left(e^{-2\gamma_r^2\alpha_r^2} - e^{-2\alpha_r^2}\right), \quad (1)$$

$$\gamma_{t,r} = \frac{b_{t,r}}{R_{t,r}}, \quad \alpha_{t,r} = \frac{R_{t,r}}{\omega_{t,r}}, \quad \omega_t = R_t, \quad \omega_r = \frac{\sqrt{2}\lambda L}{\pi R_t},$$

where the subscript t refers to the transmit telescope and r to the receive one; R and b are the radii of the primary and secondary mirrors, respectively; λ is the wavelength; $\omega_{t,r}$ is the beam radius at the transmit or receive side, and L is the distance between the telescopes (i.e. the link distance). The telescopes can be also designed as refractors, which is realistic in particular for the transmitter. The formula above is still valid after setting the corresponding value of b to zero. The effect of pointing errors or misalignment of the optics can be readily taken into account by including an additional attenuation term in δ_{diff}.

Let as denote the atmospheric attenuation by δ_{atm}. It is produced by three phenomena: scattering, absorption and turbulence, and hence it can be written as $\delta_{atm} = \delta_{scatt}\,\delta_{abs}\,\delta_{turb}$, where each term represents the attenuation due to each of the phenomena. Excellent reviews of free-space optics can be found in [25], [26], [27], [28]. The light is absorbed and scattered by gas molecules and aerosols when it passes through the atmosphere. However, the most relevant contribution to the atmospheric attenuation is caused by turbulence, which is due to thermal fluctuations that produce refractive index variations. The turbulence depends basically on the atmospheric conditions and the position of the ground station [15]. Turbulence effects are usually taken into account by increasing the divergence angle of the beam. In the case of the uplink, the attenuation due to turbulence can be expressed as [20]

$$\delta_{turb} = \frac{\left(\frac{\lambda}{R_t}\right)^2}{\left(\frac{\lambda}{R_t}\right)^2 + \theta_{turb}^2}, \quad (2)$$

where θ_{turb} is the additional divergence, in radians, due to turbulence. Finally, recalling that the total channel attenuation is the result of three effects, it is given by

$$\delta = \delta_{diff}\, \delta_{atm}\, \delta_{rec}. \tag{3}$$

III. Analysis of the Secure Rates with Different Protocols

A. The BB84 protocol

The BB84 protocol was first proposed by Bennett and Brassard in 1984 [2]. The BB84 protocol consists of two phases: the quantum transmission phase and the classical communication phase [29], [30]. In the first phase, Alice *randomly* encodes each bit in a qubit using one basis taken out of two possible ones: σ_x or σ_z. The corresponding states can be expressed as: $|+\psi\rangle = 0$, $|-\psi\rangle = 1$, with $\psi = x$ or z. The qubit is sent to Bob, who measures the qubit using one of the bases, selected *randomly*. In the second phase, Alice announces through a classical channel the basis that has been used for each qubit. Finally, they use this information to construct the key; a process that involves error correction and privacy amplification.

Due to the fact that real sources generate a portion of pulses having several photons, one of the best possible attacks for Eve against BB84 protocol is the Photon Number Splitting attack (PNS). In the PNS attack, Eve first performs a photon number non-demolition measurement to identify Alice's multi-photon signals. Eve blocks all single photon pulses, while for multi-photon pulses she stores one photon in a quantum memory, and resends to Bob the remaining photons by a transparent quantum channel.

When Eve carries out the PNS attack, she introduces some attenuation. Intuitively, if this attenuation is lower than the channel attenuation, Alice and Bob can not notice the presence of Eve, and thus Eve can obtain full information. Note that Eve introduces no errors when performing the PNS attack.

The information shared by Alice and Bob, measured in bits/pulse, is denoted by $I(A:B)$. We can analogously define $I(B:E)$ as the information between Bob and Eve. $I(A:B)$ is the Shannon's mutual information between the Alice's and Bob's raw keys [1], [31] (similarly for $I(B:E)$). These keys are streams of classical binary logical symbols (i.e. bits). The relation between these symbols is the input-output relation of a memoryless binary erasure channel. The erasure probability, i.e. the fraction of lost symbols, depends on the number of photons that constitutes each input symbol. Given that a symbol is lost when none of its photons is detected, and the probability of not detecting a photon is $(1-\delta)$, the erasure probability of a symbol formed by n photons is $(1-\delta)^n$. It is well-know that the mutual information between input and output of a memoryless binary erasure channel is equal to one minus the erasure probability [31]; therefore $I(A:B)$ is simply derived by averaging this value over all possible states of the transmitter:

$$I(A:B) = \sum_{n=0}^{\infty} \left(1-(1-\delta)^n\right) P_n(\mu) \approx \mu\delta\ . \tag{4}$$

The usual approximation above is obtained by considering that $(1-\delta)^n \approx 1-n\delta$. In order to formulate $I(B:E)$, it is assumed that Eve is not affected by the channel attenuation. It is a conservative supposition, but it is needed to guarantee security for any possible situation, and also reflects that Eve may have extraordinary abilities. Then, under the conditions of the PNS attack, Eve obtains full information (i.e. a value equal to one) when the pulse contains two or more photons, and zero information otherwise. Therefore, we can write

$$I(B:E) = \sum_{n\geq 2}^{\infty} P_n(\mu) \tag{5}$$

Let us define Eve's information as

$$I_{Eve} \triangleq \frac{I(B:E)}{I(A:B)}. \tag{6}$$

A lower bound of the key generation rate (in bits/pulse) is given in [7]:

$$R \geq q\left(-Q_\mu f(E_\mu) H_2(E_\mu) + \Omega\, Q_\mu \left(1 - H_2\left(\frac{E_\mu}{\Omega}\right)\right)\right), \tag{7}$$

where $\Omega = 1 - I_{Eve}$ is the fraction of "untagged" photons[1] and q is the efficiency of the protocol (1/2 for BB84). Q_μ is the expected raw rate (i.e. the rate before error correction and security amplification) at Bob's side, $f(x)$ is the bi-directional error correction efficiency (1.22 for the Cascade protocol [32]), $H_2(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ is the binary Shannon's entropy function [31]. The expected raw rate can be expressed as [33]

$$Q_\mu = \sum_{n=0}^{\infty} Y_n P_n(\mu)\ , \tag{8}$$

where Y_n is the yield of the *n*-photon pulses. This is defined as the probability that Bob's measurement is conclusive when Alice emits a *n*-photon pulse, and it is given by $Y_n = \delta_n + Y_0 - Y_0\delta_n \approx Y_0 + \delta_n$ [7], where Y_0 is the rate of dark counts and the attenuation for *n*-photon signal is $\delta_n = 1-(1-\delta)^n$. E_μ is the QBER and it is equal to

$$E_\mu = \frac{\sum_{n=0}^{\infty} Y_n P_n(\mu)\, e_n}{Q_\mu} = \frac{Y_0}{2Q_\mu}. \tag{9}$$

The last equality in (9) comes from the fact the bit error ratio of the n-photon signals is $e_n = \frac{Y_0}{2Y_n}$ given that the dark counts, Y_0, are the only effect causing the QBER.

B. The SARG04 Protocol

In 2004 Scarani et al. presented a new protocol, named SARG04, which is more robust than BB84 against the PNS attack [3]. This protocol is equivalent to the BB84 in the quantum communication phase, while the difference lies in the encoding and decoding of the classical information [1]. Instead of communicating the bases, Alice announces publicly one out of the four pairs of nonorthogonal states $A_{\omega,\omega'} = \{|\omega x\rangle, |\omega' z\rangle\}$, with $\omega, \omega' \in \{+,-\}$, and with the convention that $|\pm x\rangle = 0,\ |\pm z\rangle = 1$.

[1]"Untagged" refers to the photons from which Eve can not extract information [7].

Due to the fact that the information is encoded in four nonorthogonal states, when a generalized measure is performed, it is necessary to have at least three copies of the state to obtain a conclusive result with probability $P_{ok}(n)$ [34]. Therefore, in order to obtain full information, Eve must carry out an IRUD attack (Intercept-Resend with Unambiguous Discrimination). The attack starts with a photon number nondemolition quantum measurement; if the pulse contains one or two photons, Eve blocks it, otherwise she conducts a generalized quantum measurement. When the measurement is conclusive, she sends to Bob a copy of the state through a transparent quantum channel.

Eve introduces some attenuation when performing the previous attack. If the channel attenuation is smaller than that introduced by the IRUD attack, Eve should adopt a different strategy, otherwise her presence would be immediately detected. In such a case, she blocks a fraction t of the single-photon pulses, keeps one photon from each two-photon pulse, and she performs the IRUD attack on the rest of the multiphoton pulses. Then, the attenuation can be expressed as

$$\delta = \frac{(1-t)\,P_1 + P_2(\mu) + \chi}{\mu}, \quad t \in [0,1] \tag{10}$$

where χ is defined as

$$\chi \triangleq \sum_{n\geq 3}^{\infty} P_n(\mu) P_{ok}(n)\,. \tag{11}$$

The attenuation introduced by Eve (10) is simply obtained as the ratio between the mean number of photons that are received and the mean number that would be received in the absence of attenuation (i.e. μ). According to the Eve's strategy described above, the mean number of photons received can be computed as the sum of a fraction $(1-t)$ of the single-photon pulses, plus one photon for each two-photon pulse, plus one photon for the pulses with three or more photons that lead to conclusive measurements. This last term is represented by χ.

When a value of attenuation higher than that possible with (10) is allowed, all single-photon pulses (i.e. $t = 1$) and a fraction s of the two-photon pulses can be blocked. The expression of the attenuation is then

$$\delta = \frac{(1-s)\,P_2(\mu) + \chi}{\mu}, \quad s \in [0,1]\,. \tag{12}$$

This expression is obtained following the same reasoning as for (10). Conversely, it is also possible to use (10)-(12) to obtain the values of t and s given a value of the allowed attenuation.

We can formulate the information shared by Alice and Bob, and that shared by Bob and Eve. The same reasoning as in the previous section can be used, that is to say, the keys at both sides are related by a memoryless binary erasure channel. The erasure probability is different in general for each transmitter state (i.e. for each value of the number of photons per transmitted pulse) and can be readily obtained from the preceding discussion on Eve's actions. Therefore, these informations can be expressed in bits/pulse as (13) and (14) where I_2 is the maximum information that Eve can extract from one copy of the state; its value is 0.4 bits/pulse [3]. The value of P_{ok} depends on the number (n) of photons of the state and the overlap of the basis, but it is not less than $1/2$ [34], [35]. Obviously, using this attack, Eve does not obtain information from single-photon pulses.

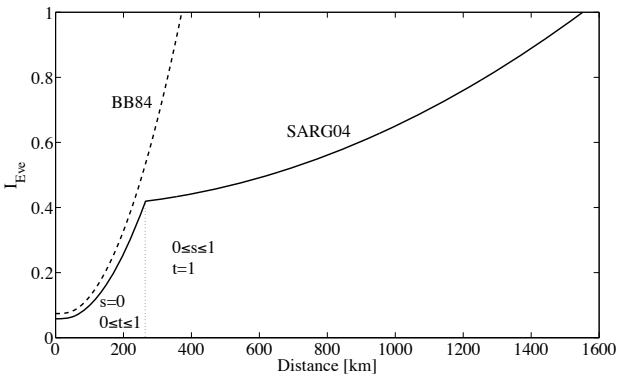

Fig. 1. Eve's information in bits/pulse for the BB84 with $\mu = 0.1$ and for the SARG04 protocol with $\mu = 0.2$. The parameters defined in Section IV for the uplink and 1 hour before sunset have been used. The vertex corresponds to the transition between blocking only single-photon pulses or also two-photon pulses. For any distance, Eve obtains less information with SARG04 than with BB84.

Eve's information in the SARG04 protocol is obtained by substituting (13) and(14) into (6). Note that the efficiency (q) of the protocol is $1/4$ in this case. The key generation rate for SARG04 protocol can be computed by introducing this value of Eve's information in (7). As a representative example, Figure 1 draws a comparison between I_{Eve} under BB84 and SARG04. It has been obtained using the realistic link parameters defined later in Section IV. SARG04 shows two different behaviors. The vertex corresponds to $t = 1$ and $s = 0$. In all cases SARG04 is better than BB84 since, with SARG04, Eve is able to obtain less information for any distance[2].

C. Improvement using the decoy-states method

The decoy-states method was first proposed by Hwang [6], and it has been further studied in [8], [37], [38]. The key point underlying the decoy-states idea is that, using extra test states, the so-called decoy states, a better analysis of the quantum channel or of the eavesdropping activity is possible. To make the difference clear, the signal states refer to those specifically used for the key generation.

The steps constituting the decoy-states method are as follows:

i. Alice can use two different kinds of sources: a signal source S with fix a mean photon number (μ) and one from a set decoy-state sources with different mean photon numbers $(\nu_1, \nu_2, \dots)$.
ii. Alice *randomly* chooses the bit values and the sources to encode them.
iii. Bob performs the polarization measurement.
iv. Alice announces the source used and Bob evaluates the gain of each source. If the gains are different to the expected ones they abort the protocol, otherwise they continue the protocol using signal states.

[2]This result is valid for the attacks considered in this paper. It has been show that under other more generic attacks BB84 may outperform SARG04 when both methods employ decoy states (see e.g. [33], [36]).

$$I(A:B) = P_1(\mu)\,(1-t) + P_2(\mu)\,(1-s) + \sum_{n\geq 3}^{\infty} P_n(\mu) P_{ok}(n)\,, \tag{13}$$

$$I(B:E) = P_2(\mu)\,(1-s)\,I_2 + \sum_{n\geq 3}^{\infty} P_n(\mu) P_{ok}(n)\,, \tag{14}$$

Next, we discuss the security of the BB84 and the SARG04 protocols with decoy states by analyzing the lower bounds of the key generation rates.

1) BB84: Vacuum + weak decoy state: Combining the idea of the entanglement distillation approach in GLLP [39] with the decoy-states method, a lower bound of key generation rate was already obtained in [7]:

$$R_{\mathrm{BB84}} \geq q\Big(-Q_\mu f\,(E_\mu)\,H_2\,(E_\mu) + Q_1\Big(1 - H_2\,(e_1)\Big)\Big), \tag{15}$$

where Q_μ is the gain (or rate) of the signal state, E_μ is the QBER, Q_1 is the gain of single-photon states, e_1 is the error rate of single-photon states, and $q = 1/2$. All parameters have been already defined in Section III-A, except for Q_1, which can be expressed as [33]

$$Q_1 = Y_1 e^{-\mu}\mu\,. \tag{16}$$

The values of Q_μ and E_μ, being average values for all states of the signal source, can be measured directly from the experiment, whereas Q_1 and e_1 need to be bounded based on other other variables that can be measured. Q_1 and e_1 can not be measured directly because Alice and Bob know the source used to transmit a given pulse, but not the number of photons generated by the source. The lower bound of Q_1 and the upper bound of e_1, obtained using the vacuum plus a weak decoy state (ν), are given by [8]

$$Y_1^L = \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2-\nu^2}{\mu^2} Y_0\right) \leq Y_1, \tag{17}$$

$$Q_1^L = \mu e^{-\mu} Y_1^L \leq Q_1, \tag{18}$$

$$e_1^U = \frac{e_0 Y_0}{Y_1^L} \geq e_1. \tag{19}$$

The background yield Y_0 can be measured as the gain of the vacuum decoy state. The background error rate e_0 is $1/2$ due to the fact that dark counts occur randomly, so half of the photons click on the correct detector.

2) SARG04: Vacuum + two weak decoy states: In the BB84 protocol, only single-photon states contribute to the key generation rate. However, in the SARG04 protocol, the key can be generated with both single-photon and two-photon states. Combining this idea with the GLLP [39], the lower bound of the key generation rate (in bits/pulse) for SARG04 is (20) [33] where X_n and Z_n represent the bit error and the phase error events, respectively, for n-photon pulses. The gain of the two-photon pulses is [33]

$$Q_2 = Y_2 e^{-\mu}\frac{\mu^2}{2}\,. \tag{21}$$

Note that the rest of parameters have already defined in the previous sections. X_n and Z_n are binary random variables. They take a value equal to one when there is a bit or phase error, and zero othersiwe. $H\,(\cdot)$ is the Shannon's entropy of a random variable [31]. Given that the specific class of Eve's attacks we are considering (i.e. IRUD attack) does not introduce phase error or bit errors, and that the only source of errors, i.e. the dark counts, is independent of the signal, phase and bit errors are independent from each other and have the same distribution. Therefore, we can replace $H\,(Z_1 \mid X_1)$ with $H_2\,(e_1)$, and $H\,(Z_2)$ with $H_2\,(e_2)$.

We present a method to compute the lower bound of the key generation rate in SARG04. It uses three decoy states: ν_0, ν_1 and ν_2. Without loss of generality, we assume that ν_0 is the vacuum (i.e. $\nu_0 = 0$), and ν_1 and ν_2 are weak decoy states (the meaning of weak is made explicit in the second term of (24)). The gains and the QBERs associated to these decoy states are defined as

$$Q_{\nu_i} = \sum_{n=0}^{\infty} Y_n P_n\,(\nu_i)\,, \tag{22}$$

$$E_{\nu_i} = \frac{\sum_{n=0}^{\infty} Y_n P_n\,(\nu_i)\,e_n}{Q_{\nu_i}}. \tag{23}$$

The values of Q_{ν_i} and E_{ν_i} can be measured directly from the experiment, whereas Q_1, Q_2, e_1 and e_2 can only be estimated approximately by indirect means due to the same reasons explained previously. The formulas for Y_n and e_n are the same ones as described in Section III-A. The bounds of Q_1 and e_1 are obtained as in the BB84 protocol, using (18) and (19) with the vacuum and the ν_1 state. We propose here an approach to bound Q_2 and e_2 using the decoy states ν_1 and ν_2.

Let us suppose Alice and Bob choose values of ν_1 and ν_2 that satisfy

$$0 < \nu_1 < \nu_2, \qquad \nu_1 + \nu_2 < \mu. \tag{24}$$

Combining Q_{ν_1} and Q_{ν_2} under the condition (24) we have

$$\begin{aligned}
&\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1} = Y_0\,(\nu_1 - \nu_2) + Y_2 \nu_1 \nu_2 \left(\frac{\nu_2 - \nu_1}{2}\right) \\
&\quad + \nu_1\nu_2 \sum_{n=3}^{\infty} \frac{Y_n\left(\nu_2^{n-1} - \nu_1^{n-1}\right)}{n!} \\
&\leq Y_0\,(\nu_1 - \nu_2) + Y_2 \nu_1 \nu_2 \left(\frac{\nu_2 - \nu_1}{2}\right) \\
&\quad + \nu_1\nu_2 \left(\frac{\nu_2^2 - \nu_1^2}{\mu^3}\right)\left(Q_\mu e^\mu - Y_0 - Y_1\mu - \frac{Y_2\mu^2}{2}\right).
\end{aligned} \tag{25}$$

In order to derive the inequality in (25), we have used that $a^k - b^k \leq a^2 - b^2$, which is valid for any a, b such that $0 < a + b < 1$ and $k \geq 2$.

$$R_{\mathrm{SARG04}} \geq q\Bigg(-Q_\mu f\left(E_\mu\right) H_2\left(E_\mu\right) + Q_1\Big(1 - H\left(Z_1 \mid X_1\right)\Big) + Q_2\Big(1 - H\left(Z_2\right)\Big)\Bigg), \tag{20}$$

$$Y_2^L = \frac{2\mu\left(\left(\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1}\right) - Y_0\left(\nu_1 - \nu_2\right) + \nu_1\nu_2\left(\frac{\nu_2^2 - \nu_1^2}{\mu^3}\right)\left(Y_0 + Y_1^L\mu - Q_\mu e^\mu\right)\right)}{\nu_1\nu_2\Big(\mu\left(\nu_2 - \nu_1\right) - \left(\nu_2^2 - \nu_1^2\right)\Big)} \leq Y_2. \tag{26}$$

TABLE I
LINK PARAMETERS USED FOR THE NUMERICAL RESULTS. THE RADII CAN CORRESPOND TO THE TRANSMITTER OR TO THE RECEIVER DEPENDING ON WHETHER THE UPLINK, DOWNLINK OR AN INTERSATELLITE LINK IS CONSIDERED.

Parameter	Notation	Value
Wavelength	λ	650 nm
Detector efficiency	δ_{rec}	65 %
Dark counts	Y_0	$50 \cdot 10^{-6}$ counts/pulse
Satellite telescope radius	$R_{t,r}$	15 cm
Ground telescope radius	$R_{t,r}$	50 cm
Satellite secondary mirror radius	$b_{t,r}$	1 cm
Ground secondary mirror radius	$b_{t,r}$	5 cm

By solving for Y_2 in (25) and substituting Y_1^L for Y_1, the lower bound of Y_2 is obtained, which is shown in (26). Then, the lower bound of the two photon gain is

$$Q_2^L = \frac{Y_2^L \mu^2 e^{-\mu}}{2} \leq Q_2. \tag{27}$$

The upper bound of e_2 can be estimated using the QBER of the weak decoy states. From (23),

$$E_{\nu_i} Q_{\nu_i} e^{\nu_i} = e_0 Y_0 + e_1 \nu_i Y_1 + e_2 \frac{\nu_i^2}{2} Y_2 + \sum_{n=3}^{\infty} e_n Y_n \frac{\nu_i^n}{n!}. \tag{28}$$

Particularizing (28) for the two weak decoy states and combining the results, we obtain under the condition (24)

$$\begin{aligned} &\nu_1 E_{\nu_2} Q_{\nu_2} e^{\nu_2} - \nu_2 E_{\nu_1} Q_{\nu_1} e^{\nu_1} \\ &= e_0 Y_0\left(\nu_1 - \nu_2\right) + e_2 Y_2 \nu_1\nu_2\left(\frac{\nu_2 - \nu_1}{2}\right) \\ &\quad + \nu_1\nu_2 \sum_{n=3}^{\infty} e_n Y_n \left(\frac{\nu_2^{n-1} - \nu_1^{n-1}}{n!}\right) \\ &\geq e_0 Y_0\left(\nu_1 - \nu_2\right) + e_2 Y_2 \nu_1\nu_2\left(\frac{\nu_2 - \nu_1}{2}\right). \end{aligned} \tag{29}$$

Solving for e_2 and substituting Y_2^L for Y_2, the upper bound of e_2 can be expressed as:

$$e_2^U = \frac{\nu_1 E_{\nu_2} Q_{\nu_2} e^{\nu_2} - \nu_2 E_{\nu_1} Q_{\nu_1} e^{\nu_1} - e_0 Y_0\left(\nu_1 - \nu_2\right)}{Y_2^L \nu_1\nu_2\left(\frac{\nu_2 - \nu_1}{2}\right)} \geq e_2. \tag{30}$$

Finally, replacing Q_1^L, Q_2^L, e_1^U and e_2^U in (20) we obtain the lower bound of the key generation rate for the SARG04 protocol with two decoy states.

IV. NUMERICAL RESULTS

We have considered three different scenarios: a ground-satellite uplink, a ground-satellite downlink and an intersatellite link. The assumed link parameters are listed in Table I. The wavelength $\lambda = 650$ nm corresponds to an absorption window and to an efficiency peak of the chosen detector (an SPCM-AQR-15 commercial silicon avalanche photodiode detector). The values of the telescopes radii have been obtained from the SILEX Experiment [40] and the Tenerife telescope [14], which are similar to those considered in other studies, such as [15]. Without loss of generality, we have assumed no additional attenuation due to pointing errors or misalignment of the optics. As already said, these effects could be readily included, and essentially they would only affect by slightly shifting to the right the distance axis of the following figures.

The uplink attenuation due to turbulence has been computed considering the Tenerife telescope ($\backsim$3 km above sea level) for two conditions: 1 hour before sunset ($\delta_{turb} = 5$ dB) and a typical clear summer day ($\delta_{turb} = 11$ dB) [41]. The turbulence effect on the downlink is negligible given that the additional divergence of the beam occurs when the beam is already very wide [15]. The scattering plus absorption attenuation is evaluated using the Clear Standard Atmosphere model [42], which results in $\delta_{scatt} = 1$ dB. These values are also in line with those reported in [15], [20]. Figure 1 can be used to calibrate the scenario, that is to say, to relate the distance to the attenuation for the system parameters that we have considered. This can be achieved by noting that the condition $I_{Eve} = 1$ is achieved when the attenuation is equal to 13 dB for BB84 and 25.6 dB for SARG04, with $\mu = 0.1$ and $\mu = 0.2$ respectively [3].

Figure 2 shows the bounds of the key generation rates for the studied protocols as a function of the distance. The bits-per-pulse values can be translated into bits per second by scaling them with the pulse repetition rate of the laser. Values of the repetition rates achievable today can be found in [11]. For all protocols, the mean photon numbers (both for the signal and decoy states) have been optimized to achieve the maximum key generation rate at each distance (see Figure 3). The optimization was carried out by doing an exhaustive search for all values of μ and ν_i's for each distance. A threshold on the minimum values of ν_i was set. The resulting optimal values of ν_i are the lowest allowed values. However, these values can not be arbitrarily low since the gains must

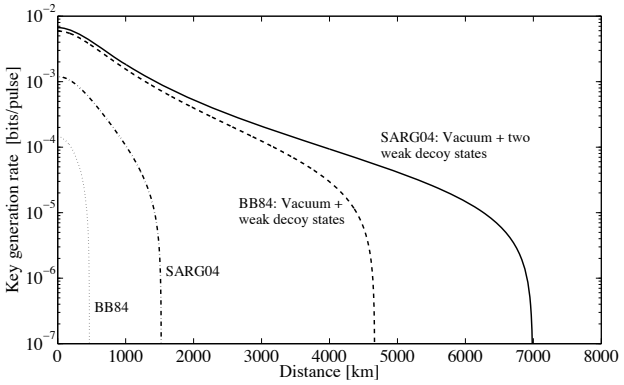

Fig. 2. Maximum secure rates achievable in the uplink and 1 hour before sunset with the four protocols under consideration. Rates can be expressed in bits per second by scaling them with the pulse repetition rate of the laser. For all protocols and for each distance, the mean photon numbers of the signal and decoy states have been numerically optimized to maximize the corresponding rate.

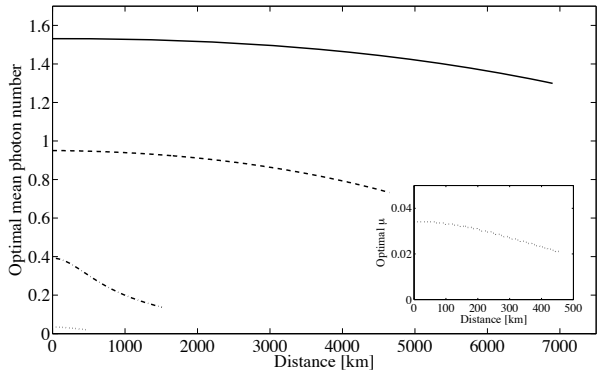

Fig. 3. Value of mean photon number of the signal state, μ, for which the maximum secure rates in Figure 2 are attained (conditions: uplink, 1 hour before sunset.). The small plot shows a zoom for BB84. In general, when the attenuation grows the value of μ and, hence, the probability of multiphoton pulses should be decreased. When decoy states are used, the optimum value of μ is approximately constant, whereas in the rest of methods the value is reduced approximately by a factor of 2 at large distances with respect to short ones.

be quantifiable in a relative short period of time, because the period of time employed to measure the gains is subtracted from the period of time available for the transmission of the key. This means that in the former period of time the decoy-states counts must be large enough to estimate the gains with small uncertainty.

Referring again to Figure 2, we observe that the critical distance[3] for SARG04 is larger than for BB84. This is due to the fact that SARG04 is more robust than BB84 against eavesdropping (see Figure 1), and it permits to use a greater optimal mean photon number. On the other hand, the BB84 critical distance increases significantly when the decoy-states method is used. It is worth recalling that the benefits of the decoy-states method are not limited to non-entanglement based protocols, which is the subject of this paper, but it is also a very powerful method to increase the critical distances and key generation rates of entanglement based protocols [43]. The most drastic improvement occurs when the decoy states method is applied to the SARG04 protocol, since it achieves the maximum critical distance among all the evaluated protocols. Note that this method is secure when the BB84 with decoy states fails, while for short distances the behaviors are similar. It is important to remark that these results do not always coincide with some security analyses in the literature [1], [33], [36]. The reason is that these other works present theoretical results about the security of the protocols under the assumption of some Eve's generic capabilities, whereas here we are using very specific attacks and scenarios, close to what might be implementable in the short term.

When the attenuation grows, Eve's attacks are more difficult to be detected, and hence the number of multiphoton pulses must be reduced (i.e. μ must be decreased). This behavior is corroborated by Figure 3. It can also be seen there that the more robust the protocol, the higher the value of μ that can be used. When the decoy-states method is applied, the optimum value of μ remains approximately constant with distance, whereas in the protocols without decoy states it is reduced by a factor of 2 at large distances compared

[3]Maximum link distance that can be achieved.

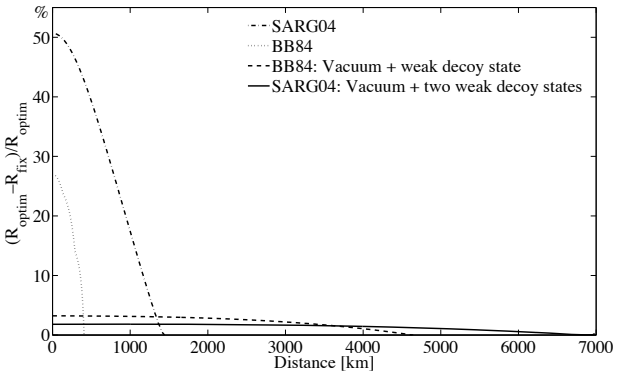

Fig. 4. Relative decrease in the secure rate when a constant value of μ, independent of the distance, is used for each protocol (conditions: uplink, 1 hour before sunset.). This value is the optimum one at the maximum possible distance for each protocol. For decoy-states protocols, the decrease is smaller than 3%, which actually means that the adaptation of μ as a function of the distance is not necessary. For the other two protocols, rate losses of 25% and 50% with respect to their maxima can occur at short distances if the mean photon number is kept fixed.

to short distances. The satellite movement along its orbit implies that the distance between itself and the ground station or the intersatellite distance varies. In order to achieve the maximal rate at each instant, the value of μ must be modified accordingly, but this is not easy with current technology and complex from an operational point of view. In Figure 4, we compare the maximum rates with the rates obtained when we fix the value of μ to the one that is optimal, for each protocol, at the maximum distance. The relative reduction is shown. We observe that for decoy-states based protocols the rate decrease is below 3%, which means that the adaptation of the value of μ as a function of the distance is not really necessary. On the contrary, the non-decoy-states based protocols present significant rate degradation, which implies that μ should be adapted according to the distance variation.

The analysis of the other three scenarios (uplink on a clear day, downlink and intersatellite link) follows similar steps.

TABLE II
CRITICAL DISTANCE FOR EACH PROTOCOL [KM].

Scenarios	BB84	SARG04	BB84: Vacuum + weak decoy state	SARG04: Vacumm + two weak decoy states
Uplink ($\delta_{turb} = 5$ dB)	460	1520	4650	6980
Uplink ($\delta_{turb} = 11$ dB)	-	500	2200	3460
Downlink	1540	3290	9450	14100
Intersatellite	430	920	2660	3900

Although the values are different, the curves have similar shapes. Therefore, we only provide the values of the critical distances (Table II) and the maximum rates (Table III). With these two sets of values, the corresponding curves can be approximately reproduced. The distances in the downlink are significantly larger compared to the ones in the uplink thanks to the lack of turbulence-induced attenuation. In fact, cryptography in MEO satellite downlinks using SARG04 with decoy states is possible. This increase in distance can not be achieved in the intersatellite link due to the reduced telescope dimensions. The most relevant parameters that influence the critical distance are the turbulence-induced attenuation and the telescopes dimensions. Furthermore, performance is severely impaired by daylight. Although the main effect taken into account herein has been the turbulence-induced attenuation, the additional background noise caused by daylight would make things even worse by increasing QBER [16].

An interesting result is the comparison of how much time we need to share a key of 10 bits between the European Space Station (at 400 km altitude approximately) and a ground station. Considering a 10 MHz source, SARG04 needs 1 ms while SARG04 with decoy states needs only 0.1 ms. It is worth remarking that SARG04 with decoy states always achieves the maximum rate and link distance. The improvement comes basically from the increase of the signal mean photon number and the contribution of the two-photon pulses to the key generation rate.

V. CONCLUSIONS

We have presented lower and upper bounds of the key generation rate and the error rate, respectively, for the SARG04 protocol combined with the vacuum and two weak decoy states. The results have been used to numerically compare the rate with those of other three protocols in realistically modelled ground-satellite and intersatellite links. Namely, the other protocols considered here are BB84, SARG04, and BB84 using the vacuum and one decoy state. It has been shown that SARG04 with decoy states outperforms all other protocols under the photon-number splitting and the intercept-resend with unambiguous discrimination attacks. Therefore, SARG04 with two decoy states is a good candidate for a satellite-based QKD mission. Moreover, we have presented results on the optimum value of the mean photon number for any distance. It has been noticed that an additional advantage of using decoy states is that a unique value of the signal-state mean photon number is almost optimum in practical terms for all distances.

REFERENCES

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev. (2008, Sep) The security of practical quantum key distribution. [Online]. Available: http://arxiv.org/abs/0802.4155v2

[2] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE International Conference Computers, Systems and Signal Processing*, Bangalore, India, 1984, pp. 175–179.

[3] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Phys. Rev. Lett.*, vol. 92, no. 5, p. 057901, Feb 2004.

[4] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992.

[5] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Phys. Rev. A*, vol. 51, no. 3, pp. 1863–1869, Mar 1995.

[6] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, p. 057901, Aug 2003.

[7] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230504, 2005. [Online]. Available: http://link.aps.org/abstract/PRL/v94/e230504

[8] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Review A (Atomic, Molecular, and Optical Physics)*, vol. 72, no. 1, p. 012326, 2005. [Online]. Available: http://link.aps.org/abstract/PRA/v72/e012326

[9] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental quantum key distribution with decoy states," *Phys. Rev. Lett.*, vol. 96, no. 7, p. 070502, 2006. [Online]. Available: http://link.aps.org/abstract/PRL/v96/e070502

[10] ——, "Simulation and implementation of decoy state quantum key distribution over 60km telecom fiber," in *Proc. IEEE International Symposium on Information Theory*, July 2006, pp. 2094–2098.

[11] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, no. 1, p. 010504, 2007. [Online]. Available: http://link.aps.org/abstract/PRL/v98/e010504

[12] E. Waks, A. Zeevi, and Y. Yamamoto, "Security of quantum key distribution with entangled photons against individual attacks," *Phys. Rev. A*, vol. 65, no. 5, p. 052310, Apr 2002.

[13] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar 2002.

[14] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Omer, M. Furst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," *Nat Phys*, vol. 3, no. 7, pp. 481–486, 2007. [Online]. Available: http://dx.doi.org/10.1038/nphys629

[15] J. Rarity, P. Tapster, P. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New J. Physics*, vol. 4, no. 1, 2002.

[16] M. Er-long, H. Zheng-fu, G. Shun-sheng, Z. Tao, D. Da-sheng, and G. Guang-can, "Background noise of satellite-to-ground quantum key distribution," *New J. Physics*, vol. 7, no. 215, 2005.

[17] G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden, "Long-distance entanglement-based quantum key distribution," *Phys. Rev. A*, vol. 63, no. 1, p. 012309, Dec 2000.

[18] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson, "Daylight quantum key distribution over 1.6 km," *Phys. Rev. Lett.*, vol. 84, no. 24, pp. 5652–5655, Jun 2000.

[19] A. E. Lita, A. J. Miller, and S. W. Nam, "Counting near-infrared single-photons with 95% efficiency," *Opt. Express*, vol. 16, no. 5, pp. 3032–3040, 2008. [Online]. Available: http://www.opticsexpress.org/abstract.cfm?URI=oe-16-5-3032

TABLE III
MAXIMUM SECURE RATE FOR EACH PROTOCOL [BITS/PULSE].

Scenarios	BB84	SARG04	BB84: Vacuum + weak decoy state	SARG04: Vacumm + two weak decoy states
Uplink ($\delta_{turb} = 5$ dB)	$1.4 \cdot 10^{-4}$	$1.2 \cdot 10^{-3}$	$5.8 \cdot 10^{-3}$	$6.5 \cdot 10^{-3}$
Uplink ($\delta_{turb} = 11$ dB)	-	$7.5 \cdot 10^{-5}$	$1.4 \cdot 10^{-3}$	$1.6 \cdot 10^{-3}$
Downlink	$1.7 \cdot 10^{-2}$	$2.4 \cdot 10^{-2}$	$4.4 \cdot 10^{-2}$	$4.6 \cdot 10^{-2}$
Intersatellite	$2.0 \cdot 10^{-2}$	$2.6 \cdot 10^{-2}$	$4.8 \cdot 10^{-2}$	$5.0 \cdot 10^{-2}$

[20] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. Leeb, and A. Zeilinger, "Long-distance quantum communication with entangled photons using satellites," *IEEE J. Sel. Topics Quantum Electronics*, vol. 9, no. 6, pp. 1541–1551, Nov.-Dec. 2003.

[21] B. E. A. Saleh and M. C. Teich, *Fundamentals of Photonics*. John Wiley & Sons, 1991, ch. Beam Optics.

[22] J. Alda, *Encyclopedia of Optical Engineering*. Marcel Dekker Inc., 2003, ch. Laser and Gaussian Beam Propagation and Transformation. [Online]. Available: http://www.informaworld.com/10.1081/E-EOE-120009751

[23] B. J. Klein and J. J. Degnan, "Optical antenna gain. 1: Transmitting antennas," *Appl. Opt.*, vol. 13, no. 9, pp. 2134–2141, 1974. [Online]. Available: http://ao.osa.org/abstract.cfm?URI=ao-13-9-2134

[24] J. J. Degnan and B. J. Klein, "Optical antenna gain. 2: Receiving antennas," *Appl. Opt.*, vol. 13, no. 10, pp. 2397–2401, 1974. [Online]. Available: http://ao.osa.org/abstract.cfm?URI=ao-13-10-2397

[25] S. Bloom, E. Korevaar, J. Schuster, and H. Willebrand, "Understanding the performance of free-space optics [invited]," *J.Optical Networking*, vol. 2, no. 6, pp. 178–200, Jun 2003.

[26] S. Arnon, "Effects of atmospheric turbulence and building sway on optical wireless-communication systems," *Opt. Lett.*, vol. 28, no. 2, pp. 129–131, 2003. [Online]. Available: http://ol.osa.org/abstract.cfm?URI=ol-28-2-129

[27] D. L. Shealy and J. A. Hoffnagle, *Encyclopedia of Optical Engineering*. Marcel Dekker Inc., 2006, ch. Atmospheric Optics for Laser Beam Shaping. [Online]. Available: http://www.informaworld.com/10.1081/E-EOE-120029768

[28] M. Gabay and S. Arnon, "Quantum key distribution by a free-space MIMO system," *J. Lightwave Technology*, vol. 24, no. 8, pp. 3114–3120, Aug. 2006.

[29] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, "Optimal eavesdropping in quantum cryptography. i. information bound and optimal strategy," *Phys. Rev. A*, vol. 56, no. 2, pp. 1163–1172, Aug 1997.

[30] D. Bruß and N. Lütkenhaus, "Quantum key distribution: from principles to practicalities," *Applicable Algebra in Engineering, Communication and Computing*, vol. 10, no. 4, pp. 383–399, 05 2000/05/18/. [Online]. Available: http://dx.doi.org/10.1007/s002000050137

[31] T. M. Cover and J. A. Thomas, *Elements of Information Theory 2nd Edition (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, July 2006.

[32] G. Brassard and L. Salvail, *Encyclopedia of Optical Engineering*. Springer Verlag, Berlin, 1993, ch. EUROCRYPT '93, Lecture Notes in Computer Science, pp. 410–423.

[33] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance of two quantum-key-distribution protocols," *Physical Review A (Atomic, Molecular, and Optical Physics)*, vol. 73, no. 1, p. 012337, 2006. [Online]. Available: http://link.aps.org/abstract/PRA/v73/e012337

[34] A. Chefles, "Unambiguous discrimination between linearly independent quantum states," *Phys. Lett. A*, vol. 239, pp. 339–347, 1998.

[35] A. Acín, N. Gisin, and V. Scarani, "Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks," *Phys. Rev. A*, vol. 69, no. 1, p. 012309, Jan 2004.

[36] B. Kraus, C. Branciard, and R. Renner, "Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses," *Physical Review A (Atomic, Molecular, and Optical Physics)*, vol. 75, no. 1, p. 012316, 2007. [Online]. Available: http://link.aps.org/abstract/PRA/v75/e012316

[37] T. Horikiri and T. Kobayashi, "Decoy state quantum key distribution with a photon number resolved heralded single photon source," *Physical Review A (Atomic, Molecular, and Optical Physics)*, vol. 73, no. 3, p. 032331, 2006. [Online]. Available: http://link.aps.org/abstract/PRA/v73/e032331

[38] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230503, 2005. [Online]. Available: http://link.aps.org/abstract/PRL/v94/e230503

[39] D. Gottesman, H.-K. LO, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Information Computing*, vol. 5, p. 325, 2004. [Online]. Available: http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/0212066

[40] P. Gatenby and M. Grant, "Optical intersatellite links," *Electronics and Communication Engineering J.*, vol. 3, no. 6, pp. 280–288, Dec 1991.

[41] D. G. Aviv, *Laser Space Communications*. Artech House, 2006.

[42] L. Elterman, "Parameters for attenuation in the atmospheric windows for fifteen wavelengths," *Appl. Opt.*, vol. 3, no. 6, pp. 745–749, 1964. [Online]. Available: http://ao.osa.org/abstract.cfm?URI=ao-3-6-745

[43] X. Ma, C.-H. F. Fung, and H.-K. Lo, "Quantum key distribution with entangled photon sources," *Phys. Rev. A (Atomic, Molecular, and Optical Physics)*, vol. 76, no. 1, p. 012307, 2007. [Online]. Available: http://link.aps.org/abstract/PRA/v76/e012307

Laura Moli-Sánchez was born in Barcelona, Spain, in September 1983. She received the B.Sc. and M.Sc. Degrees in Physics in 2005 and 2008, respectively, from the Universitat Autònoma de Barcelona (UAB). In 2007 and 2008, she was research assistant at the Signal Processing for Communications and Navigation Group of the Dept. of Telecommunications and Systems Engineering, UAB. She has worked in the R&D Department of ArcelorMittal. She is currently workings towards a Ph.D. degree in the area of hydrogen embrittlement at the Université d'Evry and the Commissariat à l'Energie Atomique (CEA), France.

Ana Rodríguez-Alonso was born in Barcelona, Spain, in September 1983. She received the B.Sc. and M.Sc. Degrees in Physics in 2004 and 2006, respectively, from the Universitat Autònoma de Barcelona (UAB). She also obtained the M.Sc. Degree in Materials Engineering in 2008 from UAB. In 2007, she was researcher assistant at the Signal Processing for Communications and Navigation Group of the Dept. of Telecommunications and Systems Engineering, UAB, working on the EXPLORA project "Quantum Satellite Communications", funded by Spanish Ministry of Science and Innovation. She has worked in the R&D Department of ArcelorMittal.

Gonzalo Seco-Granados (S'97-M'2002-SM'2008) received the Ph.D. degree in telecommunication engineering from Universitat Politècnica de Catalunya (UPC), Barcelona, Spain, in 2000, and the M.B.A. degree from IESE - University of Navarra, Barcelona, Spain, in 2002. Until 2005, he was member of the technical staff with the RF Payload Division, European Space Research and Technology Center (ESTEC), European Space Agency, Noordwijk, The Netherlands, where he was involved in the Galileo project. He led the activities concerning indoor positioning for GPS and Galileo. Since 2006, he has been an Associate Professor in the Department of Telecommunications and Systems Engineering, Universitat Autònoma de Barcelona, Barcelona, Spain. Dr. Seco-Granados received two best Ph.D. thesis awards from UPC and the Spanish Association of Telecommunication Engineers, as well as the best presentation award at the ION-GPS'2003 conference. He was co-guest editor for a special issue of the IEEE Signal Processing Magazine, and he is associate editor of the Hindawi International Journal of Navigation and Observation. He is coordinator of the Telecommunications Engineering degree and, since March 2008, he is Chair of Knowledge and Technology Transfer Parc de Recerca UAB - Santander.. His research interests include signal processing for wireless communications and navigation, location-based communications, estimation theory, resource allocation, and array processing.