PERFORMANCE COMPARISON OF BB84 AND B92 SATELLITE-BASED FREE SPACE QUANTUM OPTICAL COMMUNICATION SYSTEMS IN THE PRESENCE OF CHANNEL EFFECTS

Etengu, R.
Faculty of Engineering, Multimedia University, Cyberjaya 63100, Selangor, Malaysia
E-mail: *etengur@yahoo.com, etengurichard05@mmu.edu.my*
Abbou, F. M.
Alcatel-Lucent, 50450 Kuala Lumpur, Malaysia
Wong, H.Y.
Faculty of Engineering, Multimedia University, Cyberjaya 63100, Selangor, Malaysia
Abid, A.
Al-Madina International University, Malaysia
Nortiza, N.
Setharaman, A.
Faculty of Information Technology, Multimedia University, Cyberjaya, Selangor, Malaysia

ABSTRACT

The performance of single photon pulsed polarization based BB84 and B92 platforms against individual attacks for free space quantum optical communication links between a ground station and a satellite in the low earth orbit was compared. The comparison was attained by evaluating the quantum bit error rate and secure communication bit rate on secure optical link loss and the sensitivity of different parameters. Precisely, realistic experimental parameters were used and the results obtained were compared with those of other works. Quantum bit error rates as low as 3.5% have been regularly obtained. Moreover, with repetition rate of 10MHz at the low earth orbit standard orbital altitude of 100km and at zenith angle of 60 degrees, secure communication bit rates of ~280kHz and ~70kHz were received for the BB84 and B92 respectively. The obtained results show that the BB84 protocol exhibits better performance than B92 in the distribution of the secure communication key over long distance. Overall, these results reveal that it is possible to obtain secure key exchange in the low earth orbit, an idea which can be extended to other long distance laser links such as geostationary orbit.

Keywords: *Comparison, quantum key distribution performance, quantum bit error rate (QBER), secure communication rate, low earth orbit (LEO), geostationary orbit (GEO).*

INTRODUCTION

Quantum cryptography, better termed quantum key distribution (QKD) and employed to provide a perfectly secure coding method is currently the most mature application in the field of quantum communication. As a cryptographic technique, QKD uses the single-photon optical communication link to securely distribute one-time-use encryption keys between two or more remote legitimate parties in a way that guarantees the detection of any eavesdropper in order to obtain confidential quantum optical communication. The security of QKD is guaranteed by Heisenberg's uncertainty principle and the quantum no-cloning principle (Wootters and Zurek, 1982). Essentially, by using these physical properties of the information carrier to combat eavesdropping, a solution to the key distribution problem is deviced. Any information obtained by illegitimate third party about the exchanged key leads to a corresponding increase in the $QBER$ of the transmitted data.

The concept of QKD was first proposed in 1984 by Bennett and Brassard (1984). Moreover, free space QKD was first demonstrated in 1989 by Bennett and his co-workers over 30 cm optical link (Bennet, Bessette, Brassard, Salvail, and Smolin 1992). The first experimental implementation of QKD was proposed in 1992 (Ott, Grebogi and York, 1990), since then a lot of research effort has been devoted by communication scientists to develop the technology for use in future optical communication systems, to support security critical information flows. While the experimental setup was able to send quantum signal over distances of 100 km (Buttler et al, 1998) in optical fiber link, in free-space quantum signal was sent over a distance of 23.3 km (Hatcher, 2003). Recently, advances have led to demonstrations of QKD over point-to-point optical links (Buttler et al, 1998; Rarity, Gorman and Tapster 2001; Kurtsiefer et al, 2002; Hunghes et al, 2000). These rather promising transmission distances have stressed the high possibility of obtaining practical QKD systems. In order to implement QKD between any two locations on the globe, a satellite is needed to be used as a secure relay station. Researchers have shown that the ground-to-satellite, satellite-to-ground and satellite-to-satellite QKD demonstrations are feasible (Nordholt, Hunghes, Derkacs and Peterson 2002; Rarity, Tapster, Gorman and Knight 2002). Recently, Zhu and Zeng (2005) proposed a stratospheric quantum communication model based on the characteristics of the stratosphere. Besides, a study by Gabay and Arnon (2006) on the effect of turbulence on a quantum key distribution system can be found in Gabay, Arnon, Zhiu and Zeng, 2005). Moreover, to improve the transmission bit rate of free space systems, two authors conducted a study on quantum key distribution by free-space MIMO system (Gabay and Arnon, 2006).

Essentially, there are five steps to generate a secret key with QKD: authentication, single photon sources transmissions, sifting, error correction and privacy amplification (Nordholt, Hunghes, Derkacs and Peterson 2002; Rarity, Tapster, Gorman and Knight 2002). Primarily, to generate secret key information the randomly generated raw key is sent over the quantum channel. This is followed by key information exchange over the public channel which leads to the obtainment of the sifted key. Subsequently, the steps of error correction and privacy amplification are implemented. The purpose of error correction step is to correct the erroneously received information bits and to provide an estimate of the error rate. Besides, implementation of privacy amplification is to distill a shorter and much more secure final key as desired.

Moreover, to evaluate the performance of various QKD systems, the $QBER$ and secure communication rate are considered as important criterion (Butler et al 1998). The $QBER$ which is indicative of the security and post-error-correction communication key rate is taken in to account when evaluating the link performance. Any information learnt by an unauthorized third party about the exchanged key leads to an increase in the $QBER$. A high $QBER$ enables an unauthorised user or more correctly the eavesdropper to learn more information about the transmitted key at the expense of the legitimate recipient. Thus, it should be taken in to account that obtaining high $QBER$ values in QKD systems can resultantly lower the secure communication key rate during error correction stage of the protocol. It has been shown that, as long as the $QBER$ of the sifted key is below a certain threshold, Alice and Bob can still distill a secure key by means of classical error correction and privacy amplification. Besides, past studies have shown that any *QBERs* of the sifted key above 15 % give room for an eavesdropper to actually learn more information than the intended recipient. When the obtained $QBER$ is more than 15 %, no form of classical privacy amplification techniques can be used effectively (Kumavor, Beal, Yelin, Donkor, Wang (2005). Thus, any proper design a QKD link should ensure a baseline $QBER$ of below 15 % threshold if privacy amplification strategies are to be used to eliminate any knowledge gained by the eavesdropper. If the $QBER$ goes above 15% limit value, depending on the restrictions on the eavesdropper's abilities, it will no longer be possible to extract as secure communication bit rate. This baseline $QBER$ considers a QKD link in which a one-way classical processing by Alice and Bob is observed.

Over the years, different schemes have been proposed for quantum cryptography, including BB84 (Bennett and Brassard, 1984), B92 (Bennet, Bessette, Brassard, Salvail and Smolin 1992), BBM92 (Lo and Chau, 1999) and EPR (Inamori, Rallam and Vedral, 2000). Precisely, in this paper we consider the performance analysis of the well-known BB84 protocol and the B92 protocol counterpart in terms of secure communication bit rate. B92 is similar to BB84, and EPR takes advantage of quantum entanglement to ensure security. We perform security analysis of free space BB84 and B92 protocols, against individual attacks, let alone the most commonly considered intercept-resend and photon number splitting (PNS) attack. The system under consideration is based on the polarization coding of ideal single photon sources and single-photon sources with Poisson distribution as a photon source. So far, all known QKD realizations use three lines for communication including the quantum channel, the timing channel or trigger and the classical channel.

In Goggy, Yaun and Shields (2004) the quantum channel is pulsed attenuated laser at the operating wavelength, typically between 600-900 nm for free space links. The trigger is a pulsed bright laser at the desired wavelength, which is used to synchronise the whole apparatus. Lastly, the classical channel, which could be anything from an Ethernet connection to a telephone line, and optical communications link, which is employed to transfer the information about the bases and about error correction and privacy amplification. In this case we consider the BB84 and B92 QKD systems which are completed through quantum channel and conventional channel for communication between the transmitter and the receiver. Performance of the protocols is gauged by using the $QBER$ and the communication key exchange rate. Precisely, the legitimate users of the link can detect the presence of the eavesdropper by monitoring the $QBER$. Additionally, the sampled $QBER$ is compared with a baseline $QBER$. The analysis result shows that the performance of a QKD system, in terms of communication distance and secure communication rate is determined by the characteristics of the source of single photons and single photon detectors. To this end, we consider the commonly used InGaAs/ InP APDs as single photon detectors.

However, this work is designed to review the physical principals used for the simulations, and discuss the security analysis for the two protocols given the different link scenarios.

COMMUNICATION RATE EQUATIONS

The Standard BB84 Protocol: In this section we consider the most popular BB84 protocol, one of the first realizations of the idea of quantum physics in the context of cryptography. The BB84 protocol is the most studied and developed protocol (Bennett and Brassard 1984), implementing polarization mode encoding as a means of modulating the random bit sequence onto the polarization states of photon pulses commonly referred to as single qubit. Moreover, to operate the protocol, the sender (Alice) and the receiver (Bob) use two conjugate bases: computational (rectilinear) basis, + and the diagonal basis, x for the polarization of single photons. Each basis contains two nonorthogonal basis states to represent "0" and "1" binary digits. In an effort to perform the BB84 protocol, Alice sends Bob single photons randomly modulated in the two non-orthogonal bases using electro-optic modulator. At the receiving end, Bob measures the polarization states of the received single photons in a randomly chosen polarization basis, by using either computational or diagonal basis with equal probability for each qubit. This is done in an effort to learn the value of the bits.

We further consider a system in which Bob uses a passive modulation detection apparatus to randomly select and measure a qubit. In order to partition the photons into two different polarization analysers, a 50/50 beamsplitter is used. In the system set up, a passive electro-optic modulator is assumed as given in Lükenhaus (2000). To this end, the result of the system setup will then be used to calculate the communication rate of BB84 protocol. If Bob's measurement basis is compatible with Alice's, he learns the value of the bits with 100% probability. This outcome allows Bob to get full information. When the measurement is carried out in the wrong basis, he obtains no information because the measurement result is uncorrelated with Alice's transmission. After the quantum transmission has concluded, the sifting process which allows Bob to decode the bit values is brought into play. During sifting, Alice and Bob reveal the bases they have used without disclosing the measurement result. The bases are revealed via an authenticated classical channel that offers no protection against eavesdropping. In the absence of disturbance by the eavesdropper (Eve) and errors of various kinds, the sifted key should be identical between Alice and Bob. Alice and Bob then ignore and hence discard the bits that were measured in the wrong basis. Since Bob chooses the wrong basis with 50% probability, the sifting parameter in this case is $1/2$. Eventually, based on the desired threshold, Alice and Bob test a few bits to estimate the error rate. In the event that error rate is less than the same threshold, error correction and privacy amplification procedures are used to realize a secure communication bit rate.

At this point, we estimate the performance of the system by considering the transmission distance and the secure communication rate as important measurement factors. In order to analyse the performance of the system, the secure communication rate of the standard BB84 protocol is calculated as given in equation (1), following the original derivation by Lükenhaus (2000).

$$R_{BB84} = \frac{1}{2} \nu p_{click} \{1 - \tau(QBER, \beta) + f(QBER)\, h(QBER)\} \qquad (1)$$

The secure communication rate of the BB84 protocol R_{BB84} is a pure number and represents the fraction of distilled secure bits after the procedures of error correction and privacy amplification. The secure communication rate of the BB84 protocol is usually multiplied by the effective repetition rate of the source in order to determine the total secure communication rate of the system under consideration. The derivation of the secure communication rate R_{BB84} of the BB84 quantum coding protocol against an arbitrary individual attack, let alone the most commonly considered intercept-resend and photon number splitting (PNS) attack, in light of various experimental system parameters is as given in equation (1) from Lükenhaus (2000).

Equation (1) is applicable for free-space QKD links including the terrestrial point-to-point, ground-to-satellite, and satellite-to-satellite links. We perform the numerical simulation for free-space quantum key distribution experiments in which case we plot the communication rate as a fraction of total loss. In order to derive the communication rate R_{BB84} which is essential for use in the numerical simulations, various quantities must be derived first. First, we review and define various quantities which act as contributors to the communication key rate of the system. One of the important quantities of interest, assuming the use of the standard BB84 protocol is primarily the signal of the system under consideration, denoted as p_{click} . p_{click} is defined as the total expected probability that Bob detects a photon in a given pulse. Generally, p_{click} is computed from two independent sources which are assumed to trigger detection event. These sources can either include the propagated photon arriving from Alice or dark counts. As one of the figures of interest, p_{click} is formulated as

$$p_{click} = p_{\exp}^{signal} + p_{\exp}^{dark} - p_{\exp}^{signal} p_{\exp}^{dark} \qquad (2)$$

While $p_{\exp}^{signal}$ is the probability that Bob's detector fires because of a photon originally emitted by Alice's source, $p_{\exp}^{dark}$ is the probability that a dark count occurs in Bob's detector. Owing to the fact that each of Bob's detector is characterized by a dark count probability per time slot in the absence of real signal, the total dark count probability contribution to the detection event is given by the relation:

$$P_{\exp}^{dark} = 4d \qquad (3)$$

Essentially, the occurrence of dark count depends on the characteristics of the detectors. Usually, the occurrence of dark counts become significant when $p_{\exp}^{signal}$ is small. The dark counts occurrence emanate from thermal fluctuations in the detector and stray counts, among other contributors. As given in equation (3), coefficient 4 is due to the presence of four detectors in the passive module. This implies, the dark count is four times as large as D . Moreover, the dark counts per measurement time window are given by

$$d = Dt_w \qquad (4)$$

where D is the dark count rate of the detectors and t_w is the measurement time window of the system. It is noteworthy to say that in expression (Bennett and Brassard 1984), simultaneous occurrence of signal and dark count events are ignored when $p_{\exp}^{signal}$ and $p_{\exp}^{dark}$ are small.

Besides the above, it is imperative to restate that QKD systems are based on either fiber optical links or free space. Here, we consider free space link as the channel of interest. Essentially, free space transmission links are based on the atmospheric channel which features various undesirable atmospheric transmission phenomenons such as atmospheric absorption, dispersion and turbulence. These undesirable phenomenons can lead to photon losses during propagation. This condition is commonly referred to as decoherence. The condition of decoherence constitute a major drawback in ensuring successful free space quantum key distribution. To this end, besides the p_{click} , the total transmission efficiency becomes yet another vital figure of interest. For free space channel with a relatively high link loss, the signal contribution to the detection event can greatly depend on the total transmission efficiency of the quantum channel between Alice and Bob setup. The total transmission efficiency is formulated as

$$\eta_{tot} = T_{chan} P_{acq} \eta_{\det} \tag{5}$$

where T_{chan} and P_{acq} are respectively the quantum channel transmission and the single photon acquisition probability. These values are introduced to respectively account for the optical coupling and losses between the transmitter and the receiver. Depending on the link scenario, T_{chan} can be $A_{atm}^{GS\_GS}$, $A_{atm}^{GS\_SL}$, $A_{atm}^{SL\_SL}$ as given in equations. (6), (8 and (9) below respectively.

Moreover, owing to the fact that the effect of turbulence affects different link scenarios to different degrees, such variability can lead to different attenuation values. It is thus imperative that the various link scenarios of interest be considered when analyzing system performance. Consequently, we take into account the different link scenarios in the investigation of the effects of the various attenuation contributors to decoherence in the considered satellite-based QKD link infrastructure. The considered link scenarios include point-to-point, ground-to-satellite, satellite-to-ground, and satellite-to-satellite.

Usually, in the satellite-to-ground link, the emitted light signal propagates through longer distance of the vacuum before entering the unpredictable and troubling atmosphere. Besides, for a ground-to-satellite link the beam spreading effect of turbulence occurs in the first part of the path. This occurrence can greatly enhance the receiver's spot diameter. Finally, for satellite-to-satellite link there is no occurrence of turbulence. Given the variations in the intensity of the phenomena of turbulence and others, it is prudent to define different attenuation values for the different links scenarios. As a result, the atmospheric losses in a point-to-point link can be accounted for by the following formulation (Kim, McArthur and Korevaar 2000; Gajhardi and Karp, 1995; Jinj, Zhang Guang-Yu, and Tan Li-Yin 2005).

$$A_{atm}^{GS\_GS} = \exp(-\alpha L), \tag{6}$$

Where α is used to denote the attenuation coefficient of light signal after passing through the atmosphere. Thus, after the propagation of light signal through the atmosphere, the atmospheric attenuation coefficient of the laser light signal is given by the following formulation

$$\alpha = \frac{3.91}{v}\left(\frac{5 \cdot 4545.10^{14}}{f}\right)^{-q} \tag{7}$$

Where v is the visibility of the atmosphere, f is the optical transmission frequency of the system and q is the size distribution of the scattering particles, which is given as $0.585v^{\frac{1}{3}}$. Putting aside the point-to-point transmission link, the quantum channel transmission of the ground-to-satellite (and the satellite-to-ground) link can be computed as Jinj, Zhang Guang-Yu, and Tan Li-Yin (2005); Waks, C. Santori, and Y. Yamamoto (2002).

$$A_{atm}^{GS\_SL} = T_0^{B_\theta} \tag{8}$$

where T_0 is the atmospheric transmission at zenith angle, and B_θ is the zenith angle in the ground-to-satellite direction. Finally, for the case of the satellite-to-satellite link, the atmosphere does not exist and the channel attenuation is given as

$$A_{atm}^{SL\_SL} = 1\,. \tag{9}$$

Thus, for space-to-ground links as well as satellite-to-satellite, also called intersatellite links, we set r_o to infinity. For ground-to-space links, we assume that r_o = 9cm at λ =800 nm, corresponding to weak turbulence.

Typically, for free-space QKD system which rely on the use of WCP laser sources, the transmission and reception of photon pulses is difficult to obtain with absolute certainty owing to the channel conditions. This state of affairs arises due to the dynamic bidirectional variations of transmitted photons in the transverse plane. In such a scenario, the acquisition of single photons can be computed as Jinj, Zhang Guang-Yu, and Tan Li-Yin (2005).

$$P_{acq} = \int_0^{2\pi}\int_0^{d/2} \frac{8}{\pi}\frac{1}{L^2\theta_0^2}\exp\left\{-\frac{8}{L^2\theta_0^2}\left[\left(r\cos\beta + LP_e\right)^2 + \left(r\sin\beta\right)^2\right]\right\} rd\, rd\beta \tag{10}$$

where P_e is the tracking pointing error of the transmitter, θ_0 is the far-field divergence angle, L is the transmission link distance between the transmitter and the receiver and d is the aperture diameter of the receiver.

Normally, as reported by many researches, current practical realization of free space QKD systems rely on the use of greatly attenuated laser sources as the signal source. With this requirement, photon detection can not be determined with certainty due to the unpredictable number of photon output per pulse. It is important to note that in such systems the number of photons per pulse may not necessarily be one – but may vary from none at all to one to many. Generally, such photon sources follow the Poisson probability distribution as the underlying principle. Using the fact that the laser pulse follows the Poisson number distribution, the distribution of photon pulses can be expressed as

$$P\left(n,\mu\right) = \frac{\mu^n}{n!}\exp(-\mu) \tag{11}$$

Where $P\left(n,\mu\right)$ is the Poisson probability distribution of photons for every weak laser pulse of the transmitter, taking into account the assumption that there are n photons in a pulse. Also, parameter μ is used to denote the average number of photons per weak laser pulse.

During communication, the transmitted photons undergo a lot of disturbances and changes in the channel. Such changes include reflection, absorption and scattering.

In order to describe the effects of these undesirable channel characteristics on the transmitted photon pulses, binomial probability distribution rule is used. As such, during photon propagation, if at least one photon is registered at the receiver, then this is expressed in probability as

$$P_n \geq 1 = \sum_{k=1}^{n} C_n^k \left(\eta_{tot}\right)^k \cdot \left(1-\eta_{tot}\right)^{n-k} \quad = 1-\left(1-\eta_{tot}\right)^n \tag{12}$$

Moreover, by getting the product of equations. (11) and (12), the quantum channel efficiency η_{Qchan} can be determined. The quantum channel efficiency η_{Qchan} is given as

$$\begin{aligned} \eta_{Qchan} &= \sum_{n=1}^{\infty} P\left(n,\mu\right) P_n \geq 1 \\ &= \exp\left(-\mu\right) \sum_{n=1}^{\infty} \frac{\mu^n}{n\,!} \cdot \left[1-\left(1-\eta_{tot}\right)^n\right] \\ &= 1-\exp\left(1-\eta_{tot}\right)^n \end{aligned} \tag{13}$$

Having determined the quantum channel efficiency η_{Qchan} of the system built on WCP sources, the link budget for such systems can be discussed. This is covered in the next section. Essentially, it is important to note that the probability of p_{click} diminishes with the increasing distance between the remotely communicating parties, this being according to the expression

$$p_{\exp}^{signal} = 1-\exp(-\mu\eta_{tot}) \tag{14}$$

In expression (14), μ is the average number of photons per pulse. For an ideal single-photon source, μ=1, while for a Poisson source, it becomes a free variable which needs to be optimized. Generally, due to the effect of losses in the quantum channel, single-photon signals will arrive at Bob's detector site with a probability η_{tot} where they will lead to detection. Precisely, as given above, η_{tot} is the total transmission efficiency of the quantum channel (which is defined based on whether one is using fiber optic or free space channel).

Additionally, having computed the $p_{\exp}^{signal}$, the quantum bit rate by sifting is considered next. The sifted key rate shows the number of sifted keys received in a unit time. The sifted key rate may also be used to characterize the performance of QKD systems. The sifted key rate can be expressed as:

$$\begin{aligned} R_{sifted} &= \frac{1}{2} R_{raw} \\ &= \frac{1}{2} f_{rep} P_{click} \end{aligned} \tag{15}$$

where f_{rep} is repetition frequency of the source. Here, R_{sifted} depends on the QKD protocol and system parameters. Moreover, P_{click} is given by equation (2).

Like previously mentioned, the overall bit rate or more precisely quantum bit error rate ($QBER$) is another important figure useful in the distillation phase, that is, during error correction and privacy amplification procedures, in the analysis and simulation of QKD systems. The $QBER$ is generally defined as a measure of the ratio of the wrong bit counts to the total number of received bit counts. Precisely, the $QBER$ is equivalent to the probability of getting a false detection to the total probability of detection per pulse. The major contributions to the $QBER$ are the signal and the dark count components. Using the above definition we can write the $QBER$ as

$$QBER = \frac{\frac{1}{2} p_{\exp}^{dark} + bp_{\exp}^{signal}}{p_{click}} \tag{16}$$

where b is the defined baseline system error rate, which cannot be distinguished from interference. Like previously mention in section I, the baseline system error rate b should be defined to account for the various errors that occur during execution of the system. Such signal based errors may arise because of imperfection in the state preparation, channel decoherence, and imperfect polarization optics at Bob's detection unit. As accounted for in equation (3), another error component comes from the dark count of Bob's detectors. Each dark count is completely uncorrelated with Alice's signal and thus causes a 50% error rate.

Additionally, the last term in equation (1) corresponds to further shrinking of the sifted key due to the leakage of information to Eve during the classical error correction. The function $f\,(QBER)$ depends on the error correction algorithm For the bi-directional algorithm, the Shannon limit gives $f\,(QBER)$ =1 for any $QBER$. Moreover, for the best known performing algorithm, $f\,(QBER)$ =1.16 for $f\,(QBER) \leq 5$ (Waks, C. Santori, and Y. Yamamoto, 2002). Additionally, the function $h(QBER)$ is the conditional binary entropy function. If we introduce the probability of an error $QBER$ on the channel, this conditional entropy follows the result from the a binary symmetrical channel and can be written as

$$h(QBER) = \left[QBER \log_2 QBER + (1 - QBER)\log_2 (1 - QBER)\right] \tag{17}$$

Lastly, factor τ is the main shrinking factor in the privacy amplification step. Precisely, it represents the fraction of the error corrected key which has to be discarded during privacy amplification when only single-photon pulses are taken into account. It is related to the average collision probability, p_c through the expression:

$$\tau = -\log_2 Pc \tag{18}$$

The collision probability p_c is a measure of Eve's information with Alice and Bob. As given in Lo and Chau (1999), the following result is derived for τ:

$$\tau(QBER, \beta) = -\beta \log_2 \left[\frac{1}{2} + 2\frac{QBER}{\beta} - 2\left(\frac{QBER}{\beta}\right)^2\right] \tag{19}$$

Moreover, as provided in equation (19), parameter β is a sort of security parameter which is the fraction of single-photon states emitted by the source. Until the β parameter is positive the protocol is secure against the so called PNS attacks (Lükenhaus 2000). It is formulated as:

$$\beta = \frac{P_{click} + P_{mult}}{P_{click}} \tag{20}$$

Parameter β is defined in order to account for the photon splitting attacks due to multiplication states emitted by the source. Typically, in QKD systems, the need to characterize the quality of single photon sources is imperative. This is done by assessing the emission efficiency and the sub-Poissonian statistics of the source. Such a requirement involves measuring the emission rate and reduction in probability of multiphotonic emissions, which is then compared with an equivalent weak coherent source (WCS) having the same number of photons per pulse. In order to account for this, the amount of reduction of multiphotonic emission probability by the source should be measured with respect to photon statistics of equivalent WCP.

Thus, for security analysis and numerical simulation, we consider a sub-Poissonian multiphotonic reduction factor of 6.7 as given in Alleaume, Treussart-Tualle, Poizat and Grangier (2004). Moreover, in the operation of a typical QKD system, the information leakage towards potential eavesdropper is directly linked to P_{mult} , which is the probability per excitation pulse that a multiphotonic pulse will leaves on Alice's side. As a result, contained in the equation below is P_{mult} , which is the probability that the source emits a multi-photon state. For the case of an ideal single photon source, the probability of multiphotonic emission is evaluated as Alleaume, Treussart-Tualle, Poizat and Grangier (2004).

$$P_{mult} = \frac{1}{R}\left[1-(1+\mu)QBER^{-\mu}\right] \tag{21}$$

where parameter R is the multiphotonic reduction factor. Besides, for a practical photon light source (Trifonor, Sabacius, Berzanskis and Zavriver 2004), it is evaluated as

$$P_{mult} = 1-(1+\mu)QBER^{-\mu} \tag{22}$$

In some situations, Eve may perform quantum non-demolition (QND) measurement of the photon number in each pulse, keeping one photon on her quantum memory when she detects multiple photons, and thus applying delayed measurement of on her photon after the public announcement of the bases by Bob. Basically, in an effort to account for such PNS attacks, parameter β is used. This kind of attack is a major restricting factor in the performance analysis of the BB84 protocol implementing weak laser pulses.

Moreover, with the above security analysis, the assumption that Eve has quantum memory with an infinitely long coherence time is held, owing to the fact that Alice and Bob can holdup the public announcement for an arbitrary long time. Also, by holding the assumption that Eve is not equipped with such a quantum memory, she must perform the polarization measurement with a randomly chosen basis. In this practical case, equation (19) has to be modified to:

$$\tau(QBER,\beta) = \frac{1+\beta}{2}\log_2\left[\frac{1}{2}+4\frac{QBER}{1+\beta}-8\left(\frac{QBER}{1+\beta}\right)^2\right] \tag{23}$$

The B92 protocol: An account of the BB84 quantum coding protocol, a protocol based on two non-orthogonal bases as been given. Going beyond the BB84 protocol is the simpler and cost effective B92 protocol, one which is similar to the BB84. The B92 protocol according to Bennet, Bessette, Brassard, Salvail and Smolin (1992) was developed in an attempt to simplify the BB84 protocol. This is reflected in the fact that it is built based on only one quantum alphabet or more correctly basis states, instead of two in the case of BB84. Precisely, B92 protocol uses only two out of the four BB84 non-orthogonal states to represent a 0 or 1 on Alice’s side of the transmission system.

The B92 protocol is commonly described in terms of the polarization states of the photons rotated by angle θ, where the following polarization coding can be used to represent the quantum alphabet (Samuel and Lomonaco, 2001).

$$\begin{cases} "1" =|\,\theta_+\rangle \\ "0" =|\,\theta_-\rangle \end{cases} \qquad (24)$$

As given in equation (24), the state $|\,\theta_+\rangle$ is used to represent a 1 and $|\,\theta_-\rangle$ is used to represent a 0. Moreover, these states are used to denote the polarization states of a photon linearly polarized at angles of θ and θ_- with respect to the vertical where the values of $0\langle\theta\langle\frac{\pi}{4}$. In the B92 protocol, encoding of classical information over the quantum channel is usually implemented by the transmission of photons in some polarization states. Moreover, two non-orthogonal BB84 states are used to encode the randomly generated classical bits. Precisely, the direction of polarization encodes a classical bit. The classical bit 0 is encoded by a photon with horizontal polarization and the classical bit 1 is encoded by a photon with polarization angle of 45 degrees. So, Alice prepares photons by randomly picking one of the two non-orthogonal coherent states for each bit she wants to send. The following photon polarization description may be used to represent the coding

$$\begin{cases} "1" = 0\deg \\ "0" = +45\deg \end{cases} \qquad (25)$$

After polarization encoding, the randomly encoded classical bit information is then passed over the quantum channel. At the receiver end, Bob randomly selects one of the two bases for polarization measurement. By using the two non-orthogonal polarization measurements to receive and measure the state information, a decision of whether the received bit was a 1 or 0 is arrived at. Generally, the following polarization representation is used to decode the transmission.

$$\begin{cases} "1" = -45\deg \\ "0" = 90\deg \end{cases} \qquad (26)$$

As a result, Bob informs Alice of the detected events without the information on the measurement basis, this being done through the classical channel. Using this information, Alice processes her raw key to establish the sifted key. In reality, it is the detected events which collectively form the sifted key which is the key information. Whenever compatibility occurs in the bit selection between Alice and Bob, the probability that Bob measures a photon is 0.5. This means that only 25% of the bits transmitted will be detected by Bob. Additional decrease occurs due to the fact that the probability per light pulse is smaller than 1. The transmission efficiency of the B92 protocol based on any two non-orthogonal states, therefore, is 25% in the absence of losses and any other imperfection. This means that when sifted, 25% of the raw quantum bits should be kept and thus the sifting factor.

Finally, to test the quality of the QKD link and to see whether the sifted key obtained could be generated by performing error correction and privacy amplification (Bennett, Brassard, Crepeau and Maurer (1915), the QBER is calculated. With the above probabilities, the secure communication rate of the B92 protocol against an arbitrary individual attack, including the most commonly considered intercept-resend and photon number splitting (PNS) attack (Lütkenhaus 2001) can be formulated as:

$$R_{B92} = \frac{1}{4} v p_{click} \left\{ 1 - \tau \left(QBER, \beta \right) + f \left(QBER \right) h(QBER) \right\} \quad (27)$$

NUMERICAL RESULTS AND DISCUSSION

The communication rates for the BB84 and B92 protocols were numerically estimated using carefully selected experimental parameters. Provided in this section is a quantitative comparison of the BB84 and B92 protocols. Here, the numerical simulation of a free space quantum communication link is performed and the obtained results presented. Moreover, as previously mentioned, in the system under consideration, we progressively recognise the simulation of the quantum channel and photon transfer, implementation of error estimation, error correction and privacy amplification in the system under consideration. Moreover, Eve's eavesdropping activity is simulated in the security evaluation of the two protocols. As previously mentioned, for the numerical simulation, three free space quantum communications link scenarios in the low earth orbit (LEO) are considered.

Additionally, owing to the phenomena of atmospheric turbulence and other losses, a typical QKD system operated in the visible wavelengths range of 600-900 nm is assumed. As reported in previous studies, such systems are commonly operated at near the 770 nm where atmospheric transmission in the ground to space link is as high as 80%. At this wavelengths range, the detection efficiency is high and the atmosphere tends to be weakly dispersive. Choice of this wavelengths range is due to the readily available high performance single photon detectors with quantum efficiencies as high as 65% (Hunghes et al, 2000). Unlike the case with fiber optical links, in free space communications, the channel loss is not any more an exponential function of distance but is rather a complicated function which is formulated from atmospheric effects, beam diffraction and beam steering problems. By taking into account these causes it becomes obvious to represent the communication rate of such links as a function of total link loss instead of distance which is the case with fiber optical links.

QBER Performance: In order to measure the quality of the QKD link and to see whether the generated sifted key can produce secure key by performing error correction and privacy amplification (Bennett, Brassard, Crepeau and Maurer 1915), the $QBER$ is calculated. The use of $QBER$ is owed to the fact that it is an important criterion for the analysis and evaluation of different quantum key distribution systems (Buttler et al, 1998). Moreover, based on the expression of the $QBER$ for a QKD link implementing the ideal single photon source and single photon source with Poisson distribution, we present numerical simulation results for laser links between ground station and satellite in the low earth orbit. Our results show that at 800 nm operating wavelength, for μ =0.1 and with a fixed transmission distance, if the maximum tolerable $QBER$ is set at 15%, the link QBER is 2 % for BB84 and about 3.5% for B92 protocols. This performance is with respect to link loss. It is noteworthy to mention that these $QBER$ values include a baseline error rate owing to imperfection of the optical components used in the link. Obviously as expected, the $QBER$ values increase with additional losses in the quantum channel. This can be accomplished by varying the propagation distance. From the obtained $QBER$ values, it becomes clear that BB84 protocol is more stable to channel loss compared to B92. Overall all the $QBER$ values are far much below the defined threshold of 15%, meaning that the system is suitable for secure quantum key distribution in the LEO domain and perhaps in the GEO as an extension with modification.

Communication Bit Rate Performance: In addition to the $QBER$, it is pertinent to test the quality of the system using the secure communication bit rate on channel loss. In a general QKD system, optimisation of system performance is usually based on the generation of an improved private and hence secure communication bit rate as a figure of merit. Such optimisation is usually done in the presence of additional channel losses. Thus, in order to realise better performance, it is essential to ensure that the final secure communication bit rate as a performance measure is enhanced. For this requirement to be met, the average number of photons per pulse μ is usually exploited by system designers. This implies that an appropriate choice of the expected value of μ should be set. Moreover, choice of an appropriate value of μ should be done in light of the error correction and privacy amplification protocol being implemented.

As observed in early discussions, in this paper attention is principally directed to generation of an enhanced final secure communication bit rate. By considering the propagation of single photons for generation of the desired final secure communication bit rate, the optimisation of single photon source and single photon detection at the receiver end becomes the main concern. Such concern can be realised by carefully setting the transmission efficiency. Since we are dealing with attenuated single photon sources, the Poisson distribution of photon number is assumed. Essentially, with this assumption, the transmission of a single photon based system, in terms of secure communication bit rate is optimised when the value of μ is 0.1.

Obviously however, when implementing systems with Poisson distribution of photons, the possibility of generating and transmitting multiple photons arises. In line with this, one important limitation is noted, that is, the processing of multiple photons can sometimes be performed to the security disadvantage of the system. As a recap from, the problem of multiple photon transmission is a security disadvantage to users of similar systems, an issue which must be dealt with. Specifically, the limitation of multi photon transmission is owed to the fact that it increases the probability of successful photon splitting attacks by Eve. So, in an attempt to put to rest the multiple photon transmission problem, the value of μ should be kept as low as $\mu \leq 1$. Generally, the implementation of QKD systems with $\mu \leq 1$ has the benefit of improving system performance as opposed to implementations where $\mu \succ 1$. When the value of $\mu \succ 1$, this will result in undesirable performance. With the above examination, it is observed that the cutoff point between the two performance limits is when $\mu = 1$.

Moreover, in order to test the quality of our QKD link and to see whether it is capable of producing a secure communication key, we evaluate the sifted bit rate and secure communication bit rate for different orbital attitudes or transmission distance for both the standard BB84 and B92 QKD. We illustrate this by presenting two tables showing the analytical results for the two protocols taking into account the sifted bit rate and the secure communication bit rate at various link propagation distances.

Table 1: Analytical results for the BB84 and B92 QKD simulation at different orbital altitudes for the ground-to-satellite link when zenith angle is 60 degrees.

Distance (km)	R_{sift}^{B92}	R_{sift}^{BB84}	R_{B92}	R_{BB84}
100	$306.68x10^3$	$613.35x10^3$	$70.080x10^3$	$280.32x10^3$
300	$54.184x10^3$	$108.37x10^3$	$12.382x10^3$	$49.527x10^3$
500	$20.487x10^3$	$40.974x10^3$	$4.6816x10^3$	$18.726x10^3$
700	$10.594x10^3$	$21.187x10^3$	$2.4208x10^3$	$9.6831x10^3$
1100	$4.3267x10^3$	$8.6530x10^3$	988.7238	$3.9547x10^3$

Source: The data set given below is derived from several simulation runs. While R_{sift}^{BB84} and R_{sift}^{B92} are the sifted bit rate values for the BB84 and B92 protocols, R_{BB84} and R_{B92} are the secure communication bit rates for the BB84 and B92 protocols respectively.

Table 2: Analytical results for the BB84 and B92 QKD simulation at different orbital altitudes for the ground-to-satellite link at zenith angle of 0.

Distance (km)	R_{sift}^{B92}	R_{sift}^{BB84}	R_{B92}	R_{BB84}
100	$383.34x10^3$	$766.69x10^3$	$87.600x10^3$	$350.40x10^3$
300	$67.730x10^3$	$135.46x10^3$	$15.477x10^3$	$61.909x10^3$
500	$25.609x10^3$	$51.218x10^3$	$5.8520x10^3$	$23.408x10^3$
700	$13.242x10^3$	$26.684x10^3$	$3.0260x10^3$	$12.104x10^3$
1100	$5.4083x10^3$	$10.817x10^3$	$1.2359x10^3$	$4.9435x10^3$

Source: The presented data set is derived from a set of simulation runs. In addition, while R_{sift}^{BB84} and R_{sift}^{B92} are the sifted bit rate values for the BB84 and B92 protocols, R_{BB84} and R_{B92} are the secure communication bit rates for the BB84 and B92 protocols respectively.

As observed in Table I, for transmissions at Zenith angle of 60 degrees, the communication bit rates range from ~989 Hz to 280 kHz. Besides, as given in Table II, for transmissions at Zenith angle of 0, the communication bit rates range from ~1 kHz to 350 kHz. These transmission bit rates depend on the parameter values used for the numerical analysis. Overall, the highest achievable communication rate is 350 kHz, meaning that the link can support transmission at a maximum of 350,000 bps. This level of performance is better compared to what was reported by different research groups including Jinj, Zhang Guang-Yu, and Tan Li-Yin (2005). From the data sets presented, it is noteworthy to point out that for similar link parameters values the communication rates halve for B92 as compared the BB84 protocol. Moreover, as reported in recent studies, present day free space optical QKD systems can withstand links losses of up to 23 dB (Hatcher, 2003), but our result suggests an improvement in this value up to a link loss of 35 dB.

In addition to the analytical data set provided in the above two tables, figure 1 is further presented based on equation I to better illustrate the quality of our QKD link. In figure I we give the theoretical results of the communication rate for the two protocols of interest, taking in to account ideal and Poisson sources. Moreover, we plot the secure communication rate against link loss. We consider a ground-to-satellite free space transmission link scenario, in the LEO. Generally, the results attainable with free space QKD system for two different source designs in the phase of the considered link scenario was calculated.

As presented below, figure 1 shows calculations for ground-to-satellite free space QKD link. Just like mentioned above, the communication rate is plotted as a function of total link loss in both arms, moreover taking in to account quantum efficiency of the detectors. In the numerical analysis, different parameters are carefully considered, among which are the dark counts of the detector which is set to $5 \cdot 10^{-8}$, the baseline system error rate which is set to 0.01, the repetition rate of the system which is set to μ=10 MHz. Moreover, as previously stated, this repetition rate is chosen because it is the maximum achievable with existing APDs detectors today (Yoshizawa, Kaji and Tsuchida 2004). Also, as given in figure 1, all curves are observed to portray a cut-off distance at which point the communication bit rate sharply falls to zero. This distance is one beyond which secure communication can no longer be possible.

With the plotted curves in figure 1, it is observed that free space quantum communication links which are based on ideal single photon sources can out perform those based on realistic photon sources when the secure communication key generation rate is evaluated against total link loss. For Poisson source, we observe a notable decrease in both the rate and total link loss. However, the two curves for B92 feature a much shorter cut-off distance as compared to their BB84 counterparts.

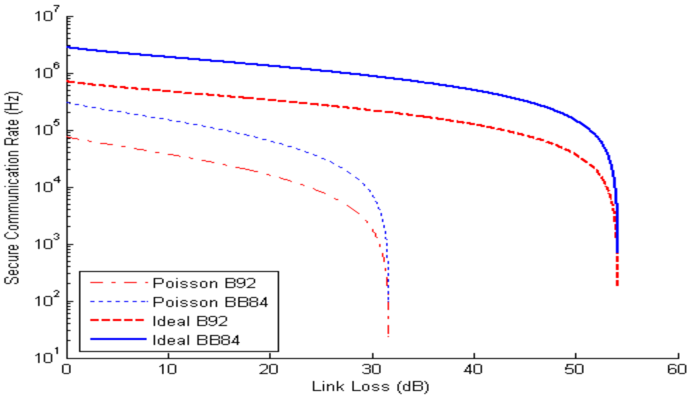

Figure 1: *Comparison of the secure communication bit rate as a function of channel loss for the standard BB84 protocol, and the B92 protocol within the visible wavelength range for a ground-to-satellite QKD link. In this case the communication bit rate is plotted as a function of link loss based on the carefully selected parameters.*

Overall, the calculated results show that free space QKD links based the BB84 protocol implementation offer the best performance as compared to B92 protocol for both ideal and Poisson photon source implementations in terms secure communication bit rate. In addition to the above set of results, figure 2 shows a plot of the secure communication bit rate as a function of channel loss with varying μ for BB84 and B92 protocols using equations (1). By taking in to consideration the curves for BB84 and

B92 protocols, for a system implementing Poisson light source, the average photon number μ becomes a free adjustable parameter which can be chosen to ensure numerical optimization of the communication rate for a given value of channel loss. It is noteworthy to say that if the value of μ is too small, the communication key rate will suffer but if the μ value is high, the system becomes more vulnerable to PNS attack. This means that there is a tradeoff between ensuring high secure communication key rate and providing security. We analysed our free space QKD links for the average photon number per pulse μ =0.01-0.03. Essentially, as revealed in the plotted curves (a) and (b) of figure 2, the BB84 protocol is observed to out perform the B92 counterpart in terms of secure communication bit rate. In other words, from the observations, the performance of the B92 protocol is only slightly worse than that of the BB84 given the varying mean number of photons per pulse, μ . In reality, the reflected curves in figure 2 have been obtained by varying the value of parameter μ for a fixed channel loss (or orbital altitude). Moreover, with further analysis, it is possible to determine the value of μ that maximises the secure communication bit rate of the system for both the two protocols.

Generally, it is imperative to make mention of the fact that the B92 QKD protocol is usually weak against eavesdropping attacks using Bob's measurement basis, which is assumed to be known to Eve (Huttner, Imoto, Gisin and Mor, 1995). Also, owing to the fact that eavesdropping attacks based on intercept resend strategies add additional channel loss to B92 QKD systems without considerably affecting QBER, monitoring the sifted key generation rate becomes a necessary requirement for Alice and Bob at all times. So, with the estimated value, each time a drop occurs in the sifted key generation rate, Alice and Bob should discard that portion of the sifted keys as there is a high possibility of Eve having the same set of sifted keys.

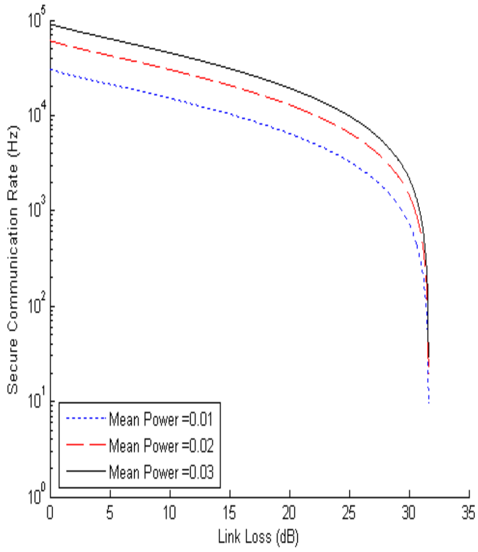

Figure 2 (a)

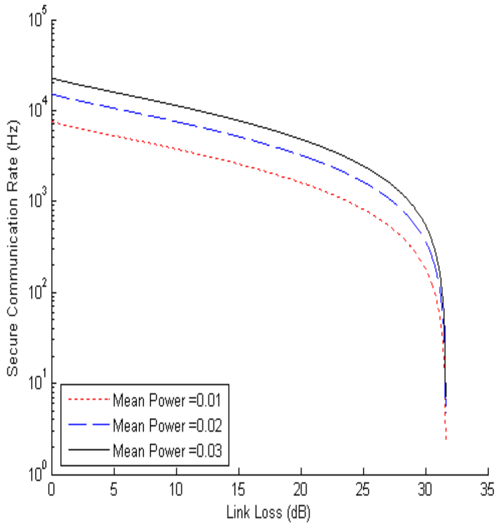

Figure 2 (b)

Figure 2 shows the key generation rate as a function of link loss with varying μ for the standard BB84 protocol and the B92 protocol. While plot (a) gives the calculated result of a ground-to-satellite QKD link for BB842 protocol, plot (b) gives the calculated result for a ground-to-satellite free space QKD link scenario for B92. In all cases the communication rate is plotted as a function of link loss using carefully selected parameters.

CONCLUSION

This paper has compared the performance of the BB84 and B92 protocols implementing a point-to-point free space QKD in the LEO, against individual eavesdropping attacks. Inline with this, the expressions for the quantum communication bit rate are given based on the ideal single-photon sources and single-photon sources with Poisson distribution for the BB84 QKD protocol which can be used for B92 protocol with some modifications. On the basis of these equations, an evaluation of the quantum communication bit rate on channel loss for the laser links between a ground station and a satellite in the low earth orbit is performed. The presented theoretical analysis results show that the BB84 protocol can ensure the distribution of high secure communication bit rate for a given channel loss in comparison to the B92. However, the B92 is advantageous in that it is easy to implement. Overall, these results indicate that it is feasible to implement single photon QKD between a ground station and a satellite in the LEO. Moreover, from the obtained results, we can suggest that single photon QKD is a suitable candidate for long distance quantum cryptography, such as surface to LEO satellite QKD. Finally, in a more broad perspective, the obtained results can be applied as the theoretical basis in the coming ground-to-satellite, satellite-to-ground and satellite-to-satellite QKD demonstrations in order to achieve regional and global coverage.

REFERENCES

Alleaume R., Treussart-Tualle F., Poizat J. P. and **Grangier P.** (2004). Experimental open-air quantum key distribution with a single-photon source. *New Journal of Physics*, 6, 92.

Bennett C. H., Brassard G., Crepeau C. and **Maurer U. M.** (1915). Generalised privacy amplification. IEEE Transactions on Information Theory, IT- 41, 6, November 1995.

Bennett C. H. and **Brassard G.** (1984). Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing Bangalore, India, pp. 175-179.

Bennet C. H., Bessette F., Brassard G., Salvail L. and **Smolin J.** (1992). Experimental quantum cryptography. Journal of Cryptology 5, 3-38.

Buttler W. T., Hunhes R. J., Kwiat P. G., Lamoreaux S. K., Luther G. G., et al (1998). Practical free-space quantum key distribution over 1 km. Physical Rev. Lett., 81 (15), 3283-3286.

Gabay M., Arnon S., Zhiu S. J. and **Zeng G.** (2005). Effect of turbulence on a quantum-key distribution scheme based on transformation from the polarization to the time domain: laboratory experiment. *Optical Engineering* 44 (4), 045002.

Gabay, M. *and* Arnon, S. (2006). Quantum Key Distribution by a Free-Space MIMO System. *Journal of Light Technology*, 24, 8.

Gajhardi, R. M. and **Karp, S.** (1995). *Optical telecommunications.* New York: Wiley

Goggy C., Yaun Z. L. and **Shields A. J.** (2004). Applied Physics Lett. 84, 3762.

Hatcher M. (2003 June 5). Cryptography beats 100 km barrier [online]. *Available at http://optics.org/articles/news/9/6/3/1.*

Hunghes R. J., Buttler W. T., Kwiat P. G., Lamoreux S. K., Morgan G. L., et al (2000). Proceedings of SPIE 3932 117.

Huttner B., Imoto N., Gisin N. and **Mor T.** (1995). Quantum cryptography with coherent states. *Physical Review, A,* 51, (3), 1863-1869.

Inamori H., Rallam L. and **Vedral V.** (2000). Security of EPR-based quantum cryptography against incoherent symmetrical attacks. *Journal of Physics: A Mathematical and General* 34, 6913-6918.

Jinj M. A, Zhang Guang-Yu and **Tan Li-Yin** (2006). Theoretical study of quantum bit rate in free-space quantum cryptography. *Chinese Physical Letter,* 23 (6), 1379, December.

Kim I. I., McArthur B. and **Korevaar E.** (2000). Comparison of Laser Beam Propagation at 785nm and 1550nm in Fog and Haze for OWC. Optical Access Incorporated.

Kumavor P. D., Beal A. C., Yelin S., Donkor E. and **Wang B. C**. (2005). Comparison of Four Multi-User Quantum Key Distribuion Schemes Over Passive Optical Networks. *Journal of Light wave Technology,* 23, 1.

Kurtsiefer C., Zarda P., Halder M., Weinfurter H., Gorman P. M., et al (2002). *Nature*, 419, 450.

Lo, H. K. and **Chau, H. F.** (1999). Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283, 2050-2056.

Lütkenhaus N. (2001). Physical Review, A 61, 052304.

Lükenhaus, N. (2000). Security against individual attacks for realistic quantum key distribution. *Physical Review,* A 61, 052304.

Nordholt J. E., Hunghes J. E., Derkacs D. and **Peterson C. G.** (2002). *New Journal of Physics,* 4 43.1.

Ott E., Grebogi C. and **York J. A.** (1990). Controlling chaos. *Physical Review Lett.* 64, 1996-1199.

Rarity J. G., Tapster P. R., Gorman P. M. and **Knight P.** (2002). *New Journal of Physics,* 4 82.1.

Rarity J. G., Gorman P. M. and **Tapster P. R.** (2001). *Electronics Letter,* 37 512.

Samuel J. and **Lomonaco J. R.** (2001). A Talk on quantum cryptography or how Alice outwits Eve. Version 1.6, January.

Trifonor A., Sabacius D., Berzanskis A. and **Zavriver A.** (2004). Single photon counting at telecom wavelength and quantum key distribution. *Journal of Modern Optics,* 06.

Waks E., Santori C. and **Yamamoto Y.** (2002). Security aspects of quantum key distribution with sub-Poisson light. *Physical review,* A 66, 042315.

Wootters W. K. and **Zurek W.** (1982). A single photon cannot be cloned. Nature, 299, 802-803.

Yoshizawa A., Kaji R., and **Tsuchida H.** (2004). 10.5km Fiber-Optic Quantum Key Distribution at 1550 nm with a key rate of 45kHz. *Japanese Journal of Applied Physics,* 43, L735-L737.

Zhiu, J. and **Zeng G.** (2005). Attenuation of quantum optical signal in stratospheric quantum communication IEEE.