Evaluations of Quantum Bit Error Rate Using the Three Stage Multiphoton Protocol

Majed Khodr
Electrical, Electronics and Communications Engineering
American University of Ras Al Khaimah
Ras Al Khaimah, UAE
Majed.khodr@aurak.ac.ae

Abstract—**This work investigates the quantum bit error rate as a function of the optical channel length for quantum communication using the three-stage multi-photon protocols. After optimizing the laser beam intensity that Alice uses to encode her quantum bits, the quantum bit error rates are calculated as a function of fiber optics channel length. The quantum bit error rate was found to increase with channel length. It was found that the bit error rate reaches a value of 7.3 per cent at the maximum achievable distance at the communication wavelength of 1550 nm. At 1310 and 850nm, this maximum value decreased to 6.1 and 5.6 per cent at the corresponding maximum achievable channel length, respectfully.**

Keywords—Quantum Key Distribution, Fiber Optics, QBER, Three stage protocol, Multi-photon

I. INTRODUCTION

Currently securing the information transferred is based on implementations of classical cryptography protocols and they are computationally secure. With the advances in quantum computers, computing power increases, and hence the classical key distribution (CKD) between parties becomes increasingly susceptible to brute force and cryptanalytic attacks. The merging field of quantum cryptography is based on quantum physics laws and is the only known means of providing secure communication regardless of computational power [1]. Most of the current implementations of quantum cryptography are based on the BB'84 protocol to secure quantum key distributions (QKD) between parties [2]. BB'84 was proposed by Bennett and Brassard in 1984 and is based on encoding the bits of a random key using a single photon for each bit.

In most of the used quantum key distribution protocols today, the polarization states of photons is utilized to realize the key distribution. Quantum physics provides these important points; 1) It is generally impossible to gain any precise information about the unknown polarization state of a single photon, 2) Once the polarization of the photon is measured, its polarization is irreversibly altered, and 3) due to the no-cloning theorem, an unknown quantum state of a single photon cannot be copied. Since the only way to emit a single photon per laser pulse is by attenuating the laser beam. Statistically and in practical setting, there is a probability that an emitted pulse can contain no photons, one single photon or more than one photon in an emitted laser pulse. Therefore, the constraint of using a single photon per encoded bit makes the BB84 protocol vulnerable to photon number splitting attacks (PNS) in case more than a single photon were generated per bit transmission in a practical setting. Due to this and other practical reasons, unfortunately, the BB84 was recently hacked [3] although patches were soon put in place by the manufacturers. At present, two companies - MagiQ 2 and IDQ - have successfully developed commercial and R&D products for quantum key distribution.

One of the alternative protocols to the BB84 was proposed by Kak in 2006 and is based on three stage multi-photons [4]. The multiphoton protocols loosen the limit on the number of photons imposed by currently used quantum key distribution protocols. Kak's proposal can be used in QKD based on the use of mathematical unitary transformations known only to the communicating party applying them i.e. either Alice or Bob. For each transmission Alice and Bob use a new set of transformations Fig. 1.

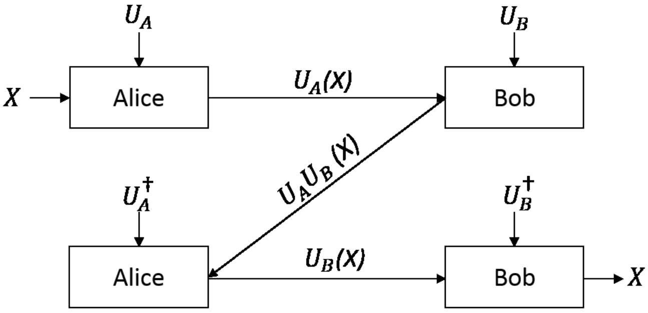

Fig. 1. Schematic of the three-stage protocol.

In this paper, the three stage multi photon protocol is studied and formulas were developed to calculate the secret key generation rate and quantum bit error rate (QBER) associate with the transmission of encoded bits between Alice and Bob in a secured quantum channel. In this paper coherent nondecoying quantum states are used to transfer the encoded bits from Alice to Bob. We assumed that a light source can be constructed such that its emitted pulse can contain a known and precise number of desired photons to encode Alice's bits. Although, this type of light source does not exit practically at this time, but the current and future developments in this field can lead to such source and hence validate this research in a practical setup. Based on this

978-1-5386-0872-2/17/$31.00 ©2017 IEEE

and the formulations obtained we were able to evaluate the secret key rate and quantum bit error rate as a function of the optical channel length for three important communication wavelengths 1550 nm, 1310 nm, and 850 nm.

II. Formulation Method

Alice she wishes to share a set of raw keys with Bob using the three stage protocol. To extract a short secret key K from the raw key, one-way post-processing is required. The optimal one –way post processing consists of two steps, error correction (EC) and privacy amplification (PA). For practical purposes, the raw-key rate R (the length of the raw key that can be produced per unit time) must be taken into account. It depends on the protocol used, the light source used, efficiency, detector type, and channel losses. The relationship between the final secret key K and the raw key rate R is given by the following relation [5]:

$$K = Rr \tag{1}$$

Where *r* can be written as [5]:

$$r = \left(1 - \frac{\mu}{2\eta_{det}\eta_{qc}}\right)\{1 - h(2Q)\} - h(Q), \tag{2}$$

And *h* is the binary entropy, *Q* is the quantum Bet Error Rate (QBER), and the remaining variables are defined below.

Based on the suggestions in [6] and [7] that the protocol is secure as long as the number of photons less than a threshold maximum value N_{max}, we express the raw key rate *R* by the following equation [8]:

$$R = v_s(P_{Bob} + P_d). \tag{3}$$

where the factor v_s is the repetition rate of the source used and $P_{Bob}(N)$ is Bob's detection probability given by:

$$P_{Bob}(N_{max}) = \sum_{n=1}^{N_{max}} p_A(n)\left[1 - \left(1 - \eta_{det}\eta_{qc}\right)^n\right] \tag{4}$$

Under the no-truncation assumption (i.e $N_{max} \to \infty$), Alice's photon-number distribution for a polarized-modulated pulse that she uses to send a single bit is according to the Poissonian statistics of mean $\mu = \langle n \rangle$, $p_A(n) = \frac{\mu^n}{n!}e^{-\mu}$. Because of the truncation assumption at N_{max}, $p_A(n)$ was properly normalized so that Alice's average photon number is represented correctly by $\mu = \langle n \rangle$. Then, Alice encodes her bit in one photon with normalized frequency $p_A(n = 1)$ in two photons with normalized frequency $p_A(n = 2)$ and so on, and does nothing with frequency $p_A(n = 0)$. η_{det} is the quantum efficiency of the detector (typically 10% at telecom wavelengths) and η_{qc} is the attenuation due to losses in the quantum channel. For fiber optics links with length D, η_{qc} is given by

$$\eta_{qc} = 10^{\frac{-\alpha D}{10}}, \tag{5}$$

where the attenuation coefficient α is in dB/km at the wavelength of interest. In this paper we consider three communication wavelengths λ=1550 nm, 1310 nm, and 850 nm with attenuation coefficient of 0.25, 0.35, and 2 dB/km respectively.

P_d is the dark count rate given by

$$P_d = 2p_d \sum_{n\geq 0}^{Nmax} p_A(n)[1 - \eta_{det}\eta_{qc}]^n, \tag{6}$$

Where $p_d = 10^{-5}$

is the dark counts per time slot. The expected error rate can be written as follows [8]

$$Q = \frac{\varepsilon P_{Bob} + \frac{1}{2}P_d}{P_{Bob} + P_d} \tag{7}$$

where the first term in the numerator represents the photon signal probability of an error per time slot which is due to alignment errors or fringe visibility and ε is a constant of value 0.005 [5]. The second term in numerator represents the dark count contribution to the same error probability. Since the dark count will result at random in one of the two measurement results for Bob, so that half of the cases an error is created. The number of photons *n* that Alice encodes her bit can vary as $n \geq 1$ for P_{Bob} (N_{max}) and $n \geq 0$ for P_d.

As a first step, we set an assumed maximum photons $N_{max} = 12$ that was encoded by Alice and sent to Bob in (1) at a fixed optics links length D to calculate the secret key as a function of μ. A maximum value will be obtained at an optimum value of μ referred to in this paper as μ_{opt}. Since the attenuation in (5) depends on D and α, we shall use a laboratory short distance ($D \approx 0$) for the calculation of μ_{opt}. The optimum value obtained will be independent on the wavelength under investigation. As a second step, using this optimum value of $\mu_{opt,}$ one can calculate the quantum bit error rate (QBER) from (7) as a function of the optical length D for each of the three communication wavelengths.

III. Data and Results

Fig. 2 demonstrates the secret key from (1) as a function of μ for $N_{max} = 12$. One notice that the maximum *K* value occurs at $\mu_{opt} = 7.22$. This value can then be used to calculate the maximum secret key K Quantum Bit Error Rate (QBER) as a function of optics link length at the communication wavelength of interest. As we increase the distance D, the maximum secret key starts to decrease linearly until we reach a maximum possible distance D_{max} at the fall off *K* values due to the effects of EC and PA.

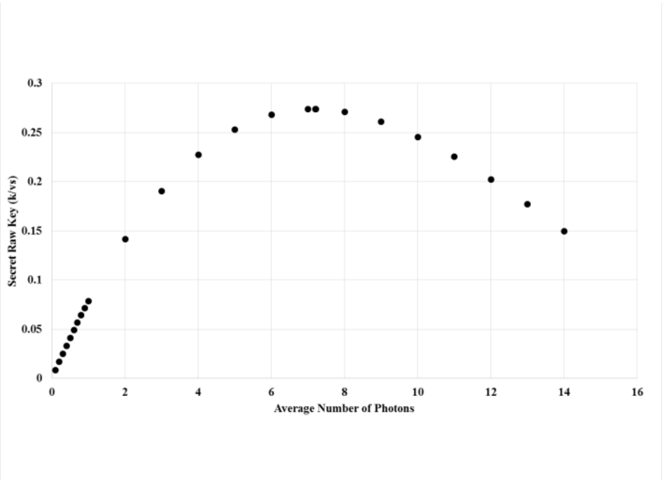

Fig. 2. **T**he secret raw key as a function of the function of μ sent by Alice. The maximum secret data rate occurs at $\mu_{opt} = 7.22$.

Table 1 lists three values of N_{max} and the corresponding μ_{opt} and D_{max} at wavelength of 1550 nm. Using (4) and (6), the error rate in (7) can be calculated as a function of distance. Fig. 3 shows the values of error rate as a function of optical link channel for $\mu_{opt} = 3.5$, 5.84, and 7.2 at wavelength of 1550 nm. The QBER increases sharply as a function of distance for each value, however at the maximum achievable distance that corresponds to μ_{opt} value is almost the same in the range between 6.7 and 7.3%.

Table 1: The maximum number of photons in each pulse and the corresponding optimum average and the maximum distance that can be achieved.

N_{max}	μ_{opt}	D_{max} (km)
1	3.5	100
7	5.84	180
12	7.22	210

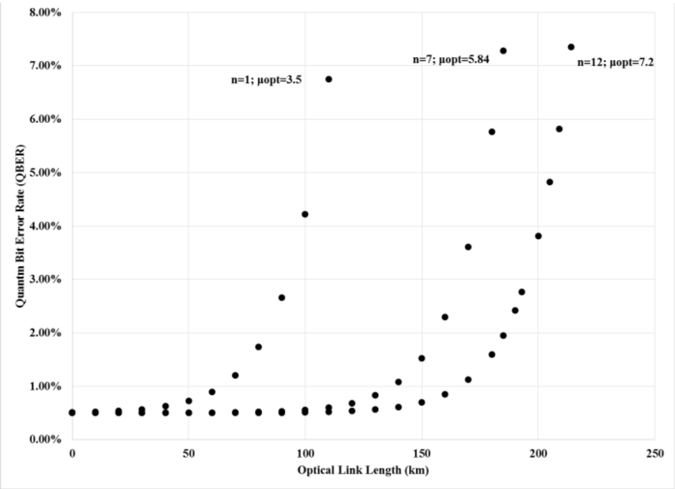

Fig. 3. The quantum bit error rate percent a function of distance for three optimum values.

In this paper we consider three communication wavelengths λ=1550 nm, 1310 nm, and 850 nm with α of 0.25, 0.35, and 2 dB/km, respectively. The influence of the wavelength through the attenuation coefficients on the secret key rate values and QBER for N_{max}=12 or $\mu_{opt} = 7.22$ at 1550 nm, 1310 nm and 850 nm are shown in Fig. 4. One notice that the QBER values increase as function of optical link length to reach a maximum value. This maximum value increases with wavelength from 5.56 % for the 850 nm to 7.3% for the 1550 nm wavelength.

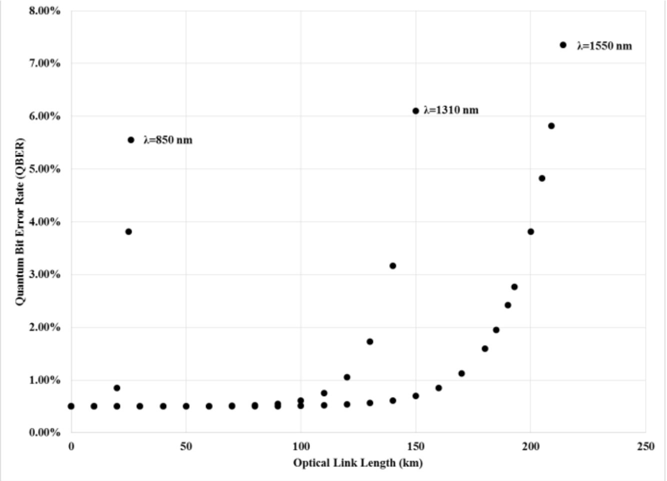

Fig. 4. QBER percent as a function of channel length for the three communication wavelengths 850 nm, 1310 nm, and 1550 nm at $\mu_{opt} = 7.22$.

IV. CONCLUSION

This work calculates the optimum average number of photons per pulse that corresponds to three values of $N_{\max}$; 1,7, and 12 that Alice can use to obtain the maximum secret raw key. The maximum achievable distances for these three values were calculated at a fixed wavelength of 1550 nm. It was found out that the QBER increases as a function of optical link length to a maximum value in the range between 6.7 and 7.3 per cent for the three values. For the most common communication wavelengths namely 1550 nm, 1310 nm, and 850 nm the QBER at the maximum achievable distance increased slightly as the wavelength increased.

ACKNOWLEDGMENT

The author would like to extend his gratitude to the support of this research by Oklahoma University Quantum Communications group.

REFERENCES

[1] H.K. Lo, H.F. Chau, Unconditional security of quantum key distribution over arbitrary long distances. *Science* 1999; 283(5410): 2050-2056.

[2] Bennett C.H.; Brassard G., Quantum Cryptography: Public Key Distribution and Coin Tossing, in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), p. 175.

[3] L. Lydersen, Wiechers, C., Wittman, C., Elser, D., Skaar, J. and Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* 4, 686, 2010.

[4] Kak, S. A Three-stage Quantum Cryptography Protocol. Foundations of Physics Letters 2006, 19, 293.

[5] Scarani V.; Bechmann-Pasquinucci H.; Cerf N.J.; Dušek M.; Lütkenhaus N.; Peev M. The security of practical quantum key distribution. Rev. Mod. Phys. 2009, 81, 1301.

[6] Chen, Y.; Kak S.; Verma P.K.; Macdonald G.; El Rifai M.; Punekar N. Multi-photon tolerant secure quantum communication—From theory to practice. IEEE International Conference on Communications (ICC) 2013, 2111-2116.

[7] Chan, K.W.C., El Rifai, M.,Verma, P.K., Kak, S.,Chen,Y., “Multi-Photon Quantum Key Distribution Based on Double-Lock Encryption”, arXiv:1503.05793 [quant-ph] 2015.