Evaluations of Maximum Distance Achieved Using the Three Stage Multiphoton Protocol at 1550 nm, 1310 nm, and 850 nm

Majed Khodr
Electrical, Electronics and Communications Department
American University of Ras Al Khaimah
Ras Al Khaimah, UAE
e-mail: majed.khodr@aurak.ae

***Abstract*—This paper presents an initial investigation of practical realization of quantum secure communication using the three-stage multi-photon tolerant protocols. The secret raw key was optimized and used to calculate the maximum achievable distance at three different wavelengths, i.e., 1550 nm, 1310 nm, and 850 nm assuming lossless fiber optics channel length. The maximum achievable distances for the three wavelengths were around 200 km, 140 km, and 25 km, respectively.**

Keywords-quantum communication; fiber channel; three stage protocol; multi-photon.

I. INTRODUCTION

Quantum cryptography is an emerging field in network security that relies on quantum mechanics proofs [1, 2] rather than on the complexity of solving a mathematical problem as in the case of classical cryptography. It is mainly used for secret key distribution, called quantum key distribution (QKD). The BB'84 protocol is the first QKD distribution protocol [1] and it was proposed by Bennett and Brassard in 1984. BB'84 is based on encoding the bits of a random key using a single photon for each bit. The major drawbacks associated with the BB'84 protocol are due to the constraint of using a single photon per encoded bit to provide a provably secure QKD scheme. Therefore, this protocol is vulnerable to photon number splitting attacks (PNS) in cases where more than a single photon is generated per bit transmission.

The three stage multi-photon tolerant protocol investigated in this paper does not require any prior agreement between a sender Alice and a receiver Bob [3-5]. This protocol is based on the use of unitary transformation known only to the party applying them. The transformation applied to the message in transit is the key that provides it with quantum level security. As shown in Figure 1, for each transmission, Alice and Bob use a new set of transformations.

Coherent non-decoying quantum states are used in this paper in order to transfer the encoded bits from Alice to Bob. The studied multi-photon, multi-stage protocol is considered quantum secure as long as less than N photons are used for communication [5] [6]. Therefore, in this paper, it is assumed that a light source can be constructed such that its Poisson photon-number distribution is truncated to a maximum number of photons. Although, this type of light source does not exit practically at this time, current and future developments in this field can lead to such sources and hence validate this research in a practical setup. Based on this and the formulations obtained, the maximum achievable distance for the three wavelengths of interest were evaluated at: 1550 nm, 1310 nm, and 850 nm.

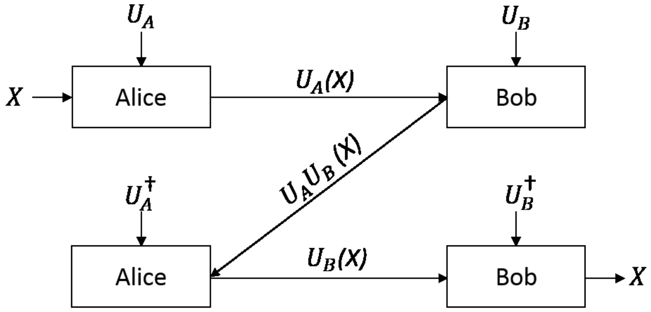

Figure 1. Schematic of the three-stage protocol [3].

Significantly, this is the first research that has ever been done on the three stage protocol that estimates key results such as maximum distance that can be achieved at three key communication wavelengths, and then compares the data to existing results. Moreover, the three stage multi-photon protocol eliminates the need for the sifting step that is needed in the BB'84 protocol. In section II, the BB'84 formulations were adopted to fit the three stage protocol under study. Section III include the theoretical data and results obtained, while section IV is the conclusion.

II. FORMULATION METHOD

A sender, Alice, has in her possession a list of symbols (called raw key); she wishes to share them with Bob using the three stage quantum protocol. To extract a short secret key from the raw key, one-way post-processing is required. The optimal one–way post processing consists of two steps. The first step is error correction (EC), also called information reconciliation, at the end of which the raw key becomes shorter and symbols perfectly correlated. The second step is privacy amplification (PA), and it is aimed at diminishing Eve's knowledge of the reference raw key. The length of the final secret key depends on Eve's information about the raw keys.

However, for practical setups, a practical parameter must also be taken into account as well: namely the raw key rate (R) rather than the raw key. This rate depends on the protocol used and on details of the implementation setup: the source used, losses in the channel, efficiency, and type of detectors. Hence, to assess the performance of practical single-stage protocol, a secret key rate is defined as [7]:

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

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

$$\mathrm{R}=\nu_s \mathrm{P}_{\mathrm{Bob}}(\mathrm{N}_{\max})=\nu_s \sum_{\mathrm{n}=1}^{\mathrm{N}_{\max}} \mathrm{p}_{\mathrm{A}}(\mathrm{n})\left[1-\left(1-\eta_{\det}\eta_{\mathrm{qc}}\right)^{\mathrm{n}}\right] \tag{2}$$

The factor ν_s is the repetition rate of the source used, and $P_{Bob}(N)$ is Bob's detection probability. Under the no-truncation assumption (i.e. $N_{max} \rightarrow \infty$), Alice's photon-number distribution for a polarized-modulated pulse that she uses to send a single bit is according to 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}, $p_A(n)$, it was properly normalized so that Alice's average photon number is represented correctly by $\mu = \langle n \rangle$. 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 link with length D, η_{qc} is given by

$$\eta_{\mathrm{qc}}=10^{\frac{-\alpha\mathrm{D}}{10}}, \tag{3}$$

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

The second parameter in (1) is defined as the secret fraction *r*, and can be written in terms of quantities that are known from calibration or from the parameter estimation of the protocol as [7]:

$$\mathrm{r}=\left(1-\frac{\mu}{2\eta_{\det}\eta_{\mathrm{qc}}}\right)\{1-\mathrm{h}(2\mathrm{Q})\}-\mathrm{h}(\mathrm{Q}), \tag{4}$$

Where Q is the expected error rate QBER and h is the binary entropy.

As a first step, set in (2) was an assumed maximum number of photons $N_{max} = 12$ that was encoded by Alice and sent to Bob at a fixed optics link length D to calculate the secret key rate K as a function of μ. A maximum K value will be obtained at an optimum value of μ referred to in this paper as μ_{opt}. Since the attenuation in (3) depends on the D and α, used, in this first step, is a laboratory short distance ($D \approx 0$) for the calculation of μ_{opt} where the attenuation is equal to 1.00 regardless of the wavelength used.

As a second step, using this optimum value of $\mu_{\mathrm{opt},}$ one can calculate the secret key rate K from (1) as a function of the optical length D for each of the three communication wavelengths under investigations. The maximum optical link length or distance that can be achieved at each wavelength can then be determined. Varying the optics link length will affect the attenuation in (3), and hence will reduce the value of the maximum secret key rate from its peak value at D≈ 0.

III. RESULTS

As shown in Figure 2, the secret key rate from (1) as a function of μ for $N_{max} = 12$. One notices that the maximum K value occurs at μ_{opt} = 7.22. This value can then be used to calculate the maximum secret key as a function of D. As we increase D, the maximum secret key rate starts to decrease linearly until we reach a maximum possible distance ($D_{max.}$). The maximum possible distances (D_{max}) that can be achieved at μ_{opt} can be found from Figure 3 at the fall off *K* values due to the effects of error correction and privacy amplifications for a no-decoy state at μ_{opt} = 7.22 as a function of distance. It can be noted from the linear relationship that these effects are small for short distances and small losses. However as we approach the maximum possible distance the channel losses increase; thus EC and PA have more severe effects on K. This leads to a sharp drop in the secret key rate at the distance of about 200 km for the 1550 nm wavelength. This distance is comparable and even better theoretically from the currently used protocols in the market where the maximum distance achieved is around 100 km. The influence of the wavelength through the attenuation coefficients on the secret key rate values for μ_{opt} = 7.22 at 1310 nm and 850 nm are also shown in Figure 3. The maximum distances that can be achieved at 1310 nm and 850 nm are 140 km and 25 km, respectively. The maximum achievable distance is higher at λ = 1550 nm that is due to the low attenuation of the medium at this wavelength.

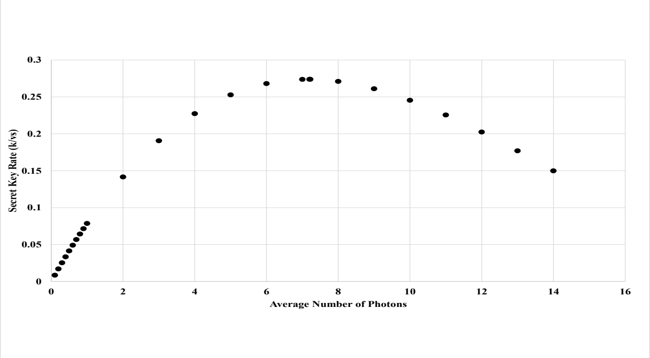

Figure 2. Plot of the secret key rate key rate as the function of average number of photons per pulse sent by Alice μ.The maximum secret key rate occurs at μ_{opt} = 7.22.

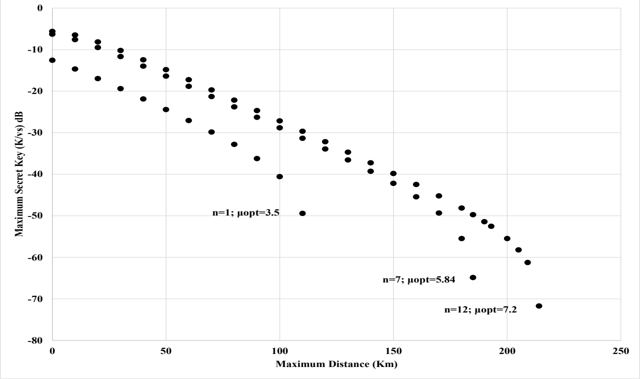

Figure 3. Plot of the secret key rate as a function of Optics Link length D for μ_{opt}=7.22

IV. CONCLUSION

This theoretical study was the first one toward determining key parameters and results to validate the use of the three stage multi-photon protocol in a practical setup. One of the key parameters that was determined is the maximum optical link length or maximum distance that the three stage multi-photon protocol can achieve to securely distribute a secret key between Alice and Bob at three communication wavelengths. Namely: 1550 nm, 1310 nm, and 850 nm. It is concluded that the maximum achievable distance using the three stage multi photon can reach 200 km at 1550 nm, theoretically, exceeding the single photon BB'84 protocol. This is an important result that needs to be proved in a practical setup. Operating at the other two wavelengths, where the fiber attenuation is higher, and decreases the maximum distance in a noticeable way.

Future work is required to validate this study. A starting point is to develop a laboratory setup were the fiber distance can be can considered zero and hence the maximum secret key rate can be determined and compared with the findings in this paper. Potential future research includes the use of fiber link lengths and wavelengths as parameters to determine the maximum distance that can be achieved practically with the use of this protocol. In addition, it can include developing a light source that can be truncated to a maximum number of photons per pulse.

ACKNOWLEDGMENT

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

REFERENCES

[1] C. Kollmitzer and M. Pivk, Applied Quantum Cryptography. Springer 2010.

[2] C. H. Bennett and G. Brassard, "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] S. Kak,"Three-stage Quantum Cryptography Protocol," Foundations of Physics Letters 2006, 19, pp. 293-296

[4] S. Mandal, et al., "Implementation of Secure Quantum Protocol using Multiple Photons for Communication," arXiv preprint arXiv:1208.6198, 2012.

[5] Y. Chen, et al.,"Multi-photon tolerant secure quantum communication—From theory to practice," IEEE International Conference on Communications (ICC) 2013, pp. 2111-2116.

[6] K. W. Chan, M. El Rifai, P. K. Verma, S. Kak. and Y. Chen, "Multi-Photon Quantum Key Distribution Based on Double-Lock Encryption," arXiv: 1503. 05793 [quant-ph] 2015.

[7] V. Scarani, et al, "The security of practical quantum key distribution," Rev. Mod. Phys.2009, 81, pp. 1301-1350.