The Comparison of Secure Key Rate of BB84 Protocol Using Single Photon Detectors and Optical Homodyne Detectors

Peiyao Xiong
The University of Sheffield, Western Bank, Sheffield, S10 2TN, UK
Email: 1754442171@qq.com

Abstract. To increase the security and efficiency of information transmission, the technology of Quantum Key Distribution is developed. A simulation of secure key rate of BB84 protocol is done to give a visualized comparison of efficiency of the protocol using different light sources and detectors. The simulation shows that the Poisson light source is less efficient than single photon source and the secure key rate of using continuous variable detectors is lower than using discrete variable detectors.

1. Introduction
With the development of computer and internet, there are massive information transmitted online every second, this makes it important to improve the security of information. To avoid eavesdropping, public-key encryption is wildly used in today’s cryptographic algorithms [1]. The most secure algorithm in classical information theory is the symmetrical cryptosystems which requires the key has longer or at least the same length as the plain text [2]. However, the public-key cryptographic algorithms in classical theory is insecure against attacks from quantum computers, to keep the security of information. Quantum Key Distribution (QKD) is needed for secure transmission of keys for symmetrical encryptions. The protocols of QKD use the quantum physical features of photons to transmit the secret and random keys for classical symmetrical cryptographic systems, which enables unconditional information security between two communicators. Moreover, the characteristics of photon, such as no-cloning theorem [3], make eavesdropping impossible and can be detected, which makes it a possible carrier for unconditional secure communication.

The QKD is one of the most significant research fields for quantum information. The University of Oxford has a long history in this field where the famous E91 protocol was proposed. Recently, China launched a Quantum Space Satellite named Mozi on 16th of August 2016 which enables key distribution over 2000km. There were many protocols that improved the security and efficiency of QKD [4]. Meanwhile, many experimental demonstrations have been published to illustrate the practical potential of applying this technique in real-world. Generally, according to different types of quantum states employed, the QKD protocols can be categorized into two types: discrete variable (DV) and continuous variable (CV). The protocols of DV normally uses single photons (e.g. BB48) or entangled particles (e.g. E91) to do the key distribution, whose Hilbert space has a finite dimension. The protocols of continuous variable QKD (CVQKD) use different way to do the key distribution, they rely on uncertainty principle and use coherent states instead of single photons to transmit information [5]. The discrete variable QKD (DVQKD) protocols can provide high security communication with low noise, but the high cost and low rate make it not
suitable for public and high rate data communication. For today’s technology, it is hard to generate and receive single photons, which makes it vulnerable to a photon-number-splitting (PNS) attack [6]. On the other hand, although CVQKD does not cost much, it allows high key-rate and has lower difficulty on the generation and reception of photons. The incomplete security analysis and the high noise are still problems that need to be resolved [7]. To enhance the application of QKD technology in public lives, high security and key rate, low noise and cost are needed in the same time. As a result, it is natural to combine the advantages of DVQKD and CVQKD. To achieve this, we need to do the detection without using single photon detector. In 2020, Qi presented a way that can do the BB84 quantum key distribution by using optical homodyne detectors [8]. This showed that it is possible to apply CV detectors for DV protocols.

To figure out the safety and efficiency of different protocols, the security analysis is needed. It shows the secure key rate with different transmission distances. This paper will simulate and compare the secure key rate of BB84 protocol that using single photon detector and also that of using optical homodyne detectors. In Section 2, the theory of security analysis and equations of secure key rate are introduced. Section 3 shows the method of the simulation, the result and analysis will be included in Section 4. In Section 5, the outcomes are discussed with the final conclusion presented in section 6.

2. Theory

In QKD protocols, two distant parties which normally referred as Alice and Bob are able to share a series of identical random numbers through quantum states. Specifically, Alice sends the quantum states, which are usually photons to Bob, and then they distillate the secure key using classical post-processing methods. The keys need to be identical and secret to ensure the communication is safe. In terms of security, there are mainly three methods of security proof for quantum key distribution. The first one is reduction to prepare-and-measure schemes, which transform the bit error and phase error to classical error and privacy amplification [9]. This method was used to do the security proof of BB84 and six-states protocols [10]. Secondly, Koashi’s complementarity approach can also be used to do the security proof, it is normally used for the protocols that used the feature of quantum entanglement such Twin-Field Quantum Key Distribution (TFQKD) protocol [11]. Moreover, Entropic approach based on the entanglement distillation has been proposed for both CVQKD and DVQKD [12]. In 2000, Shor and Preskill presented a proof of security of the BB84 protocol and showed that the secure key rate of BB84 protocol should be given by [9]:

\[ R = qQ_\mu[1 - H_2(\delta_b) - H_2(\delta_p)]. \]  

(1)

where \( q \) is the basis reconciliation factor which equal to 1/2 for BB84 protocol and can be close to 1 for efficient BB84 protocol [13], \( Q_\mu \) is the probability that the detector obtains a detection, \( \delta_b \) and \( \delta_p \) are the bit error and phase error respectively, \( H_2 \) is the binary entropy function which is given by:

\[ H_2(x) = -x \log_2(x) - (1-x) \log_2(1-x). \]  

(2)

In 2005, Lo et al. extended equation (1) to [14]:

\[ R \geq q\{-f(E_\mu)Q_\mu H_2(E_\mu) + Q_0[1 - H_2(e_\mu)]\}. \]  

(3)

Where \( f(x) \) is the error correction efficiency [15], \( E_\mu \) is the Quantum Bit Error Rate (QBER), \( Q_1 \) is the gain of one-photon state and \( e_\mu \) is the error rate of untagged qubits. When optical homodyne detectors are used in BB84 protocol, the cases that detectors receive a vacuum state, one photon and more than one photon should be considered. By combing these cases, the secure key rate can be given by [8]:

\[ R = Q_0 + Q_1[1 - H_2(E_\mu)] - QH_2(E). \]  

(4)

Where \( Q_0, Q_1 \) and \( Q \) are the states that represent the vacuum, one photon and more than one photon respectively, \( E_\mu \) is the expected value of QBER when single photon detectors are used and \( E \) is the overall QBER.
3. Method

In BB84 protocol, Alice will send single photons to Bob. However, it is hard to make single photons in reality, so weak coherent states are normally made to do the key distribution [16]. The set-up of the protocol is shown in Figure 1.

![Figure 1. The scheme of BB84 protocol, where LS is the light source, VOA is variable optical attenuator, PC is polarization controller, RNG is random number generator, PBS is polarization beam splitter, D0 and D1 are the single photon detectors that return 0 and 1 respectively.](image)

As shown in Figure 1, after the weak coherent states are generated by laser (light source), they will go through the variable optical attenuator to get classical or quantum regime, then the polarization controller which is driven by random number generators will generate one of the random eigenstates and sent them to Bob. After Bob receives those states, he will use the polarization controller to choose different basis for measuring the state. According to different basis that Bob choose, the light pulses will go to different detector and return different value after they go through the polarization beam splitter.

The weak coherent states make the photon number follows a Poisson distribution and the probability that Bob receives \( n \) photons can be given by [17]:

\[
P(n) = \frac{\mu^n}{n!} e^{-\mu},
\]

where \( \mu \) is the average photon number which normally equal to 0.1 in BB84 protocol. According to that, the probability that Bob obtain a detection when Alice sends out an \( n \)-photon state can be shown as:

\[
Q_n = Y_n \frac{\mu^n}{n!} e^{-\mu},
\]

where \( Y_n \) is the conditional probability of a detection event at Bob’s side and \( Y_0 \) is nearly \( 10^{-5} \). Then the \( Q_\mu \) in equation (3) can be determined:

\[
Q_\mu = \sum_{n=0}^{\infty} Y_n \frac{\mu^n}{n!} e^{-\mu}.
\]

In 2008, Ma extended \( Q_\mu \) and QBER \( E_\mu \) to [17]:

\[
Q_\mu = Y_0 + 1 - e^{\eta \mu}
\]

\[
E_\mu Q_\mu = c_0 Y_0 + c_\beta (1 - e^{-\eta \mu}),
\]

Where \( \eta \) is the transmittance and can be given by:

\[
\eta = \eta_b 10^{\frac{\rho}{10}},
\]
Where $\eta_B$ is the transmittance on Bob’s side, $\beta$ is the loss coefficient (channel loss) and $l$ is the transmission distance.

According to Qi’s research, when the single photon detectors are replaced by optical homodyne detectors, the cases of vacuum, one photon and more than one photon should be considered. The three states in equation (4) can be extended to:

\[
Q_0 = 2(l - \eta)(1 - e^{-\beta l})e^{-\tau}
\]

\[
Q_1[l - H_2(E_X)] = \eta[(\tau + 2)e^{-\tau} - 2(\tau + 1)e^{-2\tau}][l - H_2(E_X)]
\]

\[
QH_2(E) \approx Q_0 H_2(E_0) + Q_1 H_2(E_1)
\]

Where $\tau$ is a pre-defined threshold value and $E_X$ is equal or smaller than a fixed value. By applying these to equation (4), the secure key rate of using CV detector with different distances can be determined. In the simulation, the threshold value is set as 5 and $E_X$ is smaller and equal than 0.001.

4. Simulation and results

As the factors in equation (3) was extended, the secure key rate with different transmission distance can be determined. As mentioned before, normally, $q$ equal to 1/2 and $\mu$ equal to 0.1 in BB84 protocol. According to Cascade protocol, $f(x)$, the error correction efficiency, is equal to 1.22 [15]. Moreover, the $Y_0$ is nearly $10^{-5}$, $\eta_B$ is 0.1, $\beta$ is 0.21dB/km, the error rate of a vacuum state ($e_0$) and erroneous detection probability ($e_d$) are equal to 0.5 and 0.03 respectively [18]. Finally, by applying these numbers in equation (3) with different values of distance, the secure key rate can be calculated and the graph of secure key rate with different transmission distances can be plotted.

When single photons are made and single photon detectors are used (i.e. the ideal situation of BB84 protocol), the QBER will equal to $e_1$ and $Q_i = Q_i = Y_1$ in equation (3). Plotting the ideal situation secure key rate with the normal situation will give a visualized comparison of ideal and real situation. In the BB84 protocol that using CV detector, an ideal source was assumed. By using equation (4), the secure key rate can be calculated. Then, by plotting the secure key rate of DV detector and CV detector, we can get the comparison of the efficiency of DV and CV detectors.

![Figure 2. The secure key rate with different transmission distances.](image-url)
5. Discussion

As shown in Figure 2, the line of ideal source dropped slower than the line of Poisson source, this means that the ideal source that can sent single photons performs better than the Poisson source. This showed that the lack of perfect single photon source limited the secure key rate of QKD and the development of single photon source might hugely improves the efficiency of QKD. In Figure 3, the secure key rate of using CV detectors is smaller than that of using DV detectors with same light source. According to this, if the single photon detectors in QKD protocols are replaced by optical homodyne detectors, the efficiency of the protocols will decrease [8].

To apply the QKD protocols in public lives, there are still some challenges to overcome. The high cost and limit key rate in long transmission distance of using single photon detectors makes it not sufficient for public lives. However, although CV detectors are more economic, the secure key rate dropped faster with the increasing of communication distance than using DV detectors. Moreover, Figure 3 showed the situation of using ideal single photon source, but in real situation, the light sources can only make coherent states, this will reduce efficiency of key distribution, the secure key rate might drop to zero in less than 10 km distance. To fix this, the decoy state witch can increase the secure key rate might be needed [17]. Furthermore, some new QKD protocols (e.g. TFQKD) have higher secure key rate than BB84 protocol [19], using CV detectors in these protocols might be able to have a communication with longer distance.

As shown in Figure 4, the structure of the TFQKD protocol for CV states is similar with the original design of TFQKD. In this situation, the light sources will make coherent states and the single photon detectors are replaces by balanced optical homodyne detectors. By measuring the field quadratures of the coherent states, we might be able to do the key distribution. However, unlike BB84 protocol, the TFQKD used the entanglement of quantum states, it might take more works to decrypt the information.
6. Conclusion
The goal of this paper was to compare the secure key rate of BB84 protocol using ideal light source, Poisson source, single photon detectors and optical homodyne detectors. The Poisson source is less efficient than the ideal source. When the single photon detectors are replaced by optical homodyne detectors, the secure key rate decreases but the cost of CV detector is lower. Using the decoy state might be a way to increase the secure key rate.

7. References
[1] Paar, C., & Pelzl, J. (2009). Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media.
[2] Delfs, H., & Knebl, H. (2007). Symmetric-key encryption. In Introduction to Cryptography (pp. 11-31). Springer, Berlin, Heidelberg.
[3] Park, J. L. (1970). The concept of transition in quantum mechanics. Foundations of Physics, 1(1), 23-33.
[4] Xu, F., Ma, X., Zhang, Q., Lo, H. K., & Pan, J. W. (2020). Secure quantum key distribution with realistic devices. Reviews of Modern Physics, 92(2), 025002.
[5] Leverrier, A., & Grangier, P. (2011). Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation. Physical Review A, 83(4), 042312.
[6] Brassard, G., Lütkenhaus, N., Mor, T., & Sanders, B. C. (2000). Limitations on practical quantum cryptography. Physical Review Letters, 85(6), 1330.

[7] Braunstein, S. L., & Van Loock, P. (2005). Quantum information with continuous variables. Reviews of modern physics, 77(2), 513.

[8] Qi, B. (2020). The BB84 quantum key distribution using conjugate homodyne detection. arXiv preprint arXiv:2008.04142.

[9] Shor, P. W., & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. Physical review letters, 85(2), 441.

[10] Gottesman, D., & Lo, H. K. (2003). Proof of security of quantum key distribution with two-way classical communications. IEEE Transactions on Information Theory, 49(2), 457-475.

[11] Curty, M., Azuma, K., & Lo, H. K. (2019). Simple security proof of twin-field type quantum key distribution protocol. npj Quantum Information, 5(1), 1-6.

[12] Devetak, I., & Winter, A. (2005). Distillation of secret key and entanglement from quantum states. Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences, 461(2053), 207-235.

[13] Lo, H. K., Chau, H. F., & Ardehali, M. (2005). Efficient quantum key distribution scheme and a proof of its unconditional security. Journal of Cryptology, 18(2), 133-165.

[14] Lo, H. K., Ma, X., & Chen, K. (2005). Decoy state quantum key distribution. Physical review letters, 94(23), 230504.

[15] Brassard, G., & Salvail, L. (1993, May). Secret-key reconciliation by public discussion. In Workshop on the Theory and Application of of Cryptographic Techniques (pp. 410-423). Springer, Berlin, Heidelberg.

[16] Wang, S., He, D. Y., Yin, Z. Q., Lu, F. Y., Cui, C. H., Chen, W., ... & Han, Z. F. (2019). Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system. Physical Review X, 9(2), 021046.

[17] Ma, X. (2008). Quantum cryptography: theory and practice. arXiv preprint arXiv:0808.1385.

[18] Gobby, C., Yuan, Z. L., & Shields, A. J. (2004). Quantum key distribution over 122 km of standard telecom fiber. Applied Physics Letters, 84(19), 3762-3764.

[19] Liu, H., Wang, W., Wei, K., Fang, X. T., Li, L., Liu, N. L., ... & You, L. (2019). Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels. Physical review letters, 122(16), 160501.