Journal of Information Security and Applications 38 (2018) 1–7

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Modeling optimized decoy state protocol for enhanced quantum key distribution

Minal Lopes[a,*], Nisha Sarwade[b]

[a] Electronics Engineering Department, Veermata Jijabai Technological Institute, Mumbai, India
[b] Electronics Engineering Department, Veermata Jijabai Technological Institute, Mumbai, India

ARTICLE INFO

Article history:

Keywords:
Decoy state QKD
Free space QKD
Modeling QKD
QC
QKD
Quantum cryptography
Quantum key distribution

ABSTRACT

Quantum key distribution (QKD) has been proved superior over classical encryption techniques due to its unconditional security. Yet it remains vulnerable due to imperfect real system implementations. It is observed that decoy state method overcome the photon number splitting attack and additionally improves performance of QKD. This paper investigates a model for Decoy state QKD protocol, which ensures enhanced secret key rates and secure distance. Typically a two-state (vacuum + very weak coherent state) decoy QKD protocol with global lower bound equation for privacy amplification is analyzed. The model is tested with sets of experimental parameters and verified for its optimum performance. It is observed that global lower bound equation for privacy amplification improves secret key rates significantly.

1. Introduction

With the evolution of quantum computers, conventional cryptography is predicted to become obsolete. Quantum Cryptography (QC) on other hand provides an unconditionally secure means of information transfer through the fundamental laws of quantum mechanics. Quantum key distribution is one of the most developed applications of QC. It was first proposed by Bennett and Brassard in 1984, thus named as BB84 [1]. The most interesting part of QKD is that it allows two users to communicate with absolute security even in presence of an eavesdropper.

1.1. Quantum key distribution

The aim of QKD protocols is to share a common set of bits (key), using photons over quantum channel and post processing over classical channel. In a standard BB84 QKD protocol, Alice and Bob share a time-ordered sequence of single photons. Each photon is polarized in one of the four polarizations- horizontal, vertical, 45° and 135° chosen randomly by Alice. Bob measures each received photon in either diagonal or rectilinear basis. He then notes his basis and measurement results and shares them with Alice publicly. Both parties retain the measurements for which they used same basis. Measurements with different basis are discarded. It is noteworthy that in the absence of noise and eavesdropping (by Eve), Alice and Bob' s polarization data will be same. To crosscheck whether there is no tampering of data, Alice and Bob perform some tests such as parity check of a random subset of their received data. From such tests they compute important performance parameters such as quantum bit error rate (QBER) and sifted key rate. If this QBER exceeds the limit of prescribed value, they abort the protocol. Whereas, if QBER is within prescribed value, then the QKD protocol is successful and hence Alice and Bob can proceed for secret key generation. Further key processing (post processing) is carried through error correction and privacy amplification operations on classical channel.

1.2. QKD is vulnerable

QKD protocols are considered unconditionally secure assuming that the system devices are perfectly ideal. But in real implementations it is not the case. First and foremost is the use of single photon source. It is still an experimental challenge to develop sources emitting exactly single photon per unit time. Thus, in all recent QKD experiments a common experimental weak coherent laser pulse source is used. Such sources produce number of photons with Poisson distribution if are phase randomized. Fig. 1 shows typical Poisson distribution curve as a function of number of photons for different mean photon number (μ) values. For weak photon pulses the value of μ is restricted to $0 \leq \mu \leq 1$.

From Fig. 1, it is clear that, there is a non-zero probability of having multi-photons in every laser pulse. This opens up vulnera-

* Corresponding author.
E-mail addresses: minallopes@sfitengg.org (M. Lopes), nishasarvade@vjti.org.in (N. Sarwade).

https://doi.org/10.1016/j.jisa.2017.11.003
2214-2126/

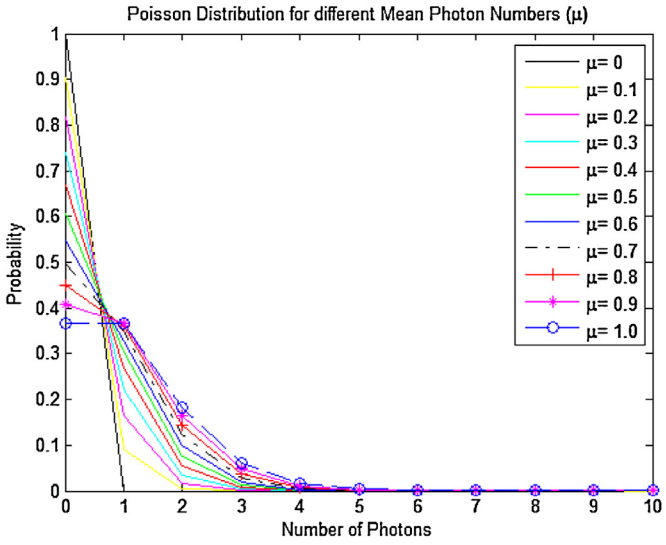

Fig. 1. Poisson distribution for $\mu = 0 : 0.1 : 1$.

bility for QKD security, known as 'photon number splitting (PNS) attack'.

To realize PNS attack, Eve can perform quantum measurement of number of photons in each pulse. If she gets a single photon pulse, she can suppress it. If she measures a multiphoton pulse, she can separate a photon and can store it in her quantum memory and resend the rest pulse to Bob. She may mask her presence by the usual loss in a quantum channel. Now, since Eve has an identical copy of Bob' s data, the unconditional security of QKD is completely compromised.

1.3. Solution to PNS attack

Hwang [3] has provided an intelligent method to defend against the PNS attack by Eve. He suggested that, in addition to regular signal states, Alice can use some decoy states. For each time period, Alice randomly sends either a signal state or a decoy state. The only difference between the decoy state and the standard signal states is their photon number distributions. After Bob' s measurements of all signals, Alice tells Bob which signals are decoy states. Then they can compare their outcomes for the decoy states and use this analysis to detect eavesdropper' s attack. Using QKD with decoy states has been proved far more beneficial as discussed further in this paper.

The outline of this paper is as follows: In Section 2 fundamental decoy state protocol by Hwang and a practical modification to it by Hoi–Kwong Lo is discussed. It also comments on possible optimization of decoy state protocol with a global lower bound on privacy amplification equation. Section 3 focuses on establishing a QKD model for decoy state protocol and its optimization with two decoy states and global privacy amplification term. Section 4 specifies the test data from few QKD experiments which will be used for model verification and testing. Optimization of signal and decoy state mean photon numbers is also covered. Section 5 present numerical results for improved secret key rates and discusses them thoroughly.

2. Decoy state protocol

Decoy state protocol was first proposed by Hwang [3]. As per the protocol, a legitimate user intentionally and randomly replaces signal pulses by multi-photon pulses which are called "decoy-states". At the end of the transmission, he announces which are the decoy states. Then both users can check for any loss in these states. If the loss of the decoy-states is abnormally less than that of signal pulses, the whole protocol is aborted. Otherwise, to continue the protocol, they estimate loss of signal multi-photon pulses based on that of decoy states. This estimation can be done with an assumption that the two losses have similar values. i.e.

$$\begin{aligned} Y_n(signal) &= Y_n(decoy) = Y_n \\ e_n(signal) &= e_n(decoy) = e_n \end{aligned} \tag{1}$$

where, Y_n is the yield and e_n is the QBER at detector side which contributes to overall gain Q_μ and overall QBER E_μ respectively, of the signal states.

Hwang specifically proposed to use m-decoy states (where m is an integer) each with an average number of photon (v) greater than or equal to 1 which is rather high by QKD standards. Whereas Hoi–Kwong Lo [6] proposed to use either Vacuum (no light pulses) or very weak coherent states or both as decoy states. He also showed that a decoy state protocol with vacuum and a weak decoy state converges to the theoretical limit of the decoy state protocol with an infinite number of decoy states.

2.1. Vacuum + weak decoy state QKD protocol

This protocol is a special case of m-decoy state QKD protocol proposed and analyzed by Hoi–Kwong Lo in [6,7]. The protocol uses two decoy states, (1) vacuum (no light pulse) and (2) very weak coherent state. By using a vacuum as a decoy state, Alice and Bob can verify the so called dark count rates of their detectors. On the other hand, by using a very weak coherent pulse as a decoy state, they can easily lower bound the yield of single-photon pulses.

Using m-decoy state QKD protocol, Alice and Bob can experimentally measure the gain Q_μ and the QBER E_μ for all the m values of decoy states. Since the relations between the variables Q_μ' s and Y_n' s and between E_μ' s and e_n' s are linear, for any given set of $Q_\mu$and E_μ, Alice and Bob can calculate Y_n and e_n with high confidence and can constrain their values within acceptable range. Thus any attempt by Eve that will change the values of any Y_n' s and e_n' s, will substantially be caught with high probability.

In Vacuum+Weak decoy state protocol, vacuum decoy state allows Alice and Bob to know their channel properties well. Thus they can deduce the acceptable range of Y_n and e_n' s. The weak decoy state provides the values of Y_n and e_n' s to examine the eavesdropping. In summary, decoy state protocol greatly strengthens the power of Alice and Bob to detect the eavesdropper, thus dramatically improving the performance of QKD system.

2.2. Advantages of decoy states

Although Decoy state protocol is primarily devised as a countermeasure to PNS attack, it brings many other advantages inherently.

(a) Decoy state QKD achieves secure key distribution even with high channel loss.
(b) It increases secure key rate as compared to BB84 protocol.
(c) It is simple to implement with minor modifications in existing QKD set ups. Thus unlike prior art solutions based on single-photon sources, this protocol does not require appalling technological developments.
(d) Theoretically it is very difficult to obtain a good lower bound on single photon yield 'Y_1' and a good upper bound on single photon error rate 'e_1'. But, decoy state QKD is a simple method that provides very good bounds to Y_1 and e_1.