*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 1, Ver. IV (Jan.- Feb. 2018), PP 37-47*
*www.iosrjournals.org*

# Practical Qkd For Both Bb84 And Sarg04 Protocols

Majdi Abdellatief [1,2], Sellami Ali[1], And Mohammed A Alanezi [1]
[1]*Faculty of Computer Science and Information Technology, Shaqra University Shaqra, Kingdom of Saudi Arabia*
[2]*Department of Computer Science, MTC College, Sudan Technological University*
*Corresponding Author: Majdi Abdellatief*

***Abstract:*** *A decoy state method based on one decoy state protocol has been derived for both BB84 and SARG04. This method can give a different lower bound of the fraction of single-photon counts* $(y_1)$ *and the fraction of two-photon counts* $(y_2)$*, the upper bound QBER of single-photon pulses(*$e_1$*), the upper bound QBER of two-photon pulses(*$e_2$*), and the lower bound of the key generation rate for both BB84 and SARG04. The estimations have demonstrated that a decoy state protocol with only one decoy state (*$\nu \to 0$*) can approach the theoretical limit, and the estimations have provided an optimal key generation rate, which is the same as having an infinite number of decoy states for BB84 and SARG04.This finding has led to the introduction of the Vacuum Protocol. We have simulated an optical fiber-based QKD system using our decoy state method for both SARG04 and BB84. The simulation has shown that the fiber-based QKD systems using the proposed method for BB84 are able to achieve both a higher secret key rate and greater secure distance than those of SARG04.*

***Keywords:*** *Quantum cryptography, Quantum key distribution, Decoy state protocol and Optical communication.*

---

Date of Submission: 22-02-2018 Date of acceptance: 07-03-2018

---

## I. Introduction

Quantum key distribution (QKD) is a cryptographic protocol that allows two remote parties (Alice and Bob) to generate a random key (a string of bits) so that only Alice and Bob have any information regarding the key. The most well-known QKD protocol is the BB84 protocol [1], which has been proven to be unconditionally secure against any attacks allowed by quantum mechanics [2,3, 4 ];this does not guarantee the security of QKD in practice, due to various types of imperfections in a practical set-up. For real-life experimental set-ups, which are mainly based on faint laser pulses, the occasional production of multi-photons and channel loss make it possible for sophisticated eavesdroppers to launch various subtle eavesdropping attacks, including the PNS (photon number splitting) attack[5], in which she Alice blocks all single-photon pulses and splits multi-photon pulses. She keeps one copy of each of the split pulses to for herself and forwards another copy to Bob. Although [5, 6] showed that secure QKD is still possible even with imperfect devices, the PNS attack puts severe limits on the distance and key generation rate of an unconditionally secure QKD. A novel solution to the problem of imperfect devices in BB84 was proposed by Hwang [8], who used extra test states–called decoy states–to learn the properties of the channel and/or eavesdrop on the key-generating signal states. Lo and co-workers presented an unconditional security proof of decoy-state QKD [9, 10]. By combining the idea of the entanglement distillation approach by Gottesman, Lo, Lutkenhaus, and Preskill (GLLP) [11] with the decoy state method, they showed that decoy state QKD can exhibit a dramatic increase in distance and key generation rate compared to non-decoy protocols [12]. Moreover, many methods have been developed to improve the performance of the decoy state QKD, including more decoy states [13], non-orthogonal decoy-state method [14], photon number-resolving method [15], herald single photon source method [16, 17], modified coherent state source method [18], and the intensity fluctuations of the laser pulses [19] and [20]. Some prototypes of decoy state QKD have already been implemented [21- 26].

Additionally, there has been work on measuring-device independent (MDI) QKD, in which Alice and Bob independently prepare phase randomized coherent pulses in one of the four BB84 states (with decoy states) and send them to an untrusted third party, Charlie. Charlie then performs Bell state measurements (BSM) and announces to Alice and Bob over a public channel the successful BSM events. Alice and Bob can obtain a sifted key by dropping events, in which they send pulses to different bases [27]. This has been implemented and gives good key rates in the laboratory [28]. A further improvement using four-source decoy states has been examined

[29]. The preparation of phase-randomized coherent pulses could be achieved, for instance, by strongly modulating the laser diode, taking it below and above a threshold [30]. Importantly, the security of decoy-state QKD has been obtained in the case of finite-length keys [31,32]. A complete passive decoy-state QKD transmitter with coherent light has been presented in [33,34].

In this paper, we first present a simple method for studying the secure key generation rate when single-photon and two-photon pulses are employed to generate a secure key. We drive a general theory for the decoy state protocol, with one decoy state protocol for both BB84 and SARG04. This method can be used to estimate the lower bound of the fraction of single-photon counts $(y_1)$ and the fraction of two-photon counts $(y_2)$, the upper bound QBER of single-photon pulses $(e_1)$,and the upper bound QBER of two-photon pulses $(e_2)$, as well as to evaluate the lower bound of the key generation rate for both BB84 and SARG04. Then, we show the simulation of fiber-based Decoy State Quantum Key Distribution based on one decoy state protocol for both BB84 and SARG04.

This paper is prepared as follows. In section 2, we propose a tight verification of the fraction of the single photon state and the quantum bit error rate (QBER) for the practical decoy method with one decoy state protocol for both BB84 and SARG04. In section 3, we simulate the key generation rate over transmission distance. The main conclusions are summarized in section 4.

## II. Proposed Decoy State Method

In this section, we propose a method for evaluating the lower bound of the key generation rate for both BB84 and SARG04 by estimating the lower bound of the fraction of one photon count $y_1$ and two photon counts $y_2$, upper bound of the quantum bit-error rate (QBER) of one photon $e_1$ and upper bound of the quantum bit-error rate (QBER) of two photons $e_2$. It is assumed that Alice can prepare and emit a weak coherent state $\left|\sqrt{\mu}e^{i\theta}\right\rangle$. Assuming that the phase $\theta$ of each signal is randomized, the probability distribution for the number of photons of the signal state follows a Poisson distribution with some parameter $\mu$ (the intensity of signal states), which is given by $p_i = e^{-\mu}\frac{\mu^i}{i!}$; Alice's pulse will contain an *i*-photon state. Therefore, it is assumed that any Poissonian mixture of the photon number states can be prepared by Alice. Moreover, Alice can vary the intensity for each individual pulse.

Assuming Alice and Bob choose the signal and decoy state with expected photon numbers $\mu, \nu_1$, respectively, they will obtain the following gains and QBERs for the signal state and decoy state [35]:

$$Q_\mu e^\mu = y_0 + \mu y_1 + \sum_{i=2}^{\infty} y_i \frac{\mu^i}{i!}$$
$$Q_\mu = y_0 + 1 - e^{-\eta\mu} \tag{1}$$

$$E_\mu Q_\mu e^\mu = e_0 y_0 + \mu e_1 y_1 + \sum_{i=2}^{\infty} e_i y_i \frac{\mu^i}{i!}$$
$$E_\mu = \frac{1}{Q_\mu}\left(e_0 y_0 + e_{\det}(1 - e^{-\eta\mu})\right) \tag{2}$$

$$Q_{\nu_1} e^{\nu_1} = y_0 + \nu_1 y_1 + \sum_{i=2}^{\infty} y_i \frac{\nu_1^i}{i!}$$
$$Q_{\nu_1} = y_0 + 1 - e^{-\eta\nu_1} \tag{3}$$

$$E_{\nu_1} Q_{\nu_1} e^{\nu_1} = e_0 y_0 + e_1 \nu_1 y_1 + \sum_{i=2}^{\infty} e_i y_n \frac{\nu_1^i}{i!}$$

$$E_{\nu_1} = \frac{1}{Q_{\nu_1}}\left(e_0 y_0 + e_{\det}(1-e^{-\eta\nu_1})\right) \tag{4}$$

$$Q_{\nu_2} e^{\nu_2} = y_0 + \nu_2 y_1 + \sum_{i=2}^{\infty} y_i \frac{\nu_2^i}{i!}$$

$$Q_{\nu_2} = y_0 + 1 - e^{-\eta\nu_2} \tag{5}$$

$$E_{\nu_2} = \frac{1}{Q_{\nu_2}}\left(e_0 y_0 + e_{\det}(1-e^{-\eta\nu_2})\right) \tag{6}$$

The transmittance of the *i*-photon state with respect to a threshold detector is

$$\eta_i = 1-(1-\eta)^i \tag{7}$$

for $i = 0,1,2,...$

The yield of an *i*-photon state is given by

$$y_i = y_0 + \eta_i - y_0\eta_i \approx y_0 + \eta_i \tag{8}$$

The error rate of the *i*-photon state is given by

$$e_i = \frac{e_0 y_0 + e_{\det}\eta_i}{y_i} \tag{9}$$

where $y_i$ is the yield of an *i*-photon state, which comes from two parts: background ( $y_0$ ) and true signal. $\eta$ is the overall transmittance, which is given by $\eta = \eta_{Bob} 10^{-\frac{\alpha l}{10}}$, where $\alpha$ (dB/km) is the loss coefficient , *l* is the length of the fiber and $\eta_{Bob}$ denotes the transmittance on Bob's side. $e_{\det}$ is the probability that a photon hits the erroneous detector, while $e_{\det}$ characterizes the alignment and stability of the optical system. The error rate of the background is $e_0 = \frac{1}{2}$.

***Case A1 of one decoy state protocol for BB84:*** In this protocol, we should estimate the lower bounds of $y_1$ and the upper bounds of $e_1$. Intuitively, only one decoy state is needed for the estimation. Here, we investigate how to use one decoy state to estimate those bounds.

Suppose that Alice randomly changes the intensity of her pump light among 2 values (one decoy state and a signal state) such that the intensity of one mode of the two mode source is randomly changed among $\nu$ and $\mu$, which satisfy the inequalities $0 \le \nu < \mu \le 1$. $\nu$ is the mean photon number of the decoy state and $\mu$ is the expected photon number of the signal state.

According to Eq. (1), the gain of the signal and one decoy state are given by:

$$Q_\mu e^\mu = y_0 + \mu y_1 + \sum_{i=2}^{\infty} y_i \frac{\mu^i}{i!}$$

$$Q_\nu e^\nu = y_0 + \nu y_1 + \sum_{i=2}^{\infty} y_i \frac{\nu}{i!} \tag{10}$$

By using the inequality (8) in [36] , with $0 \le \nu < \mu \le 1$ , we obtain

$$\frac{\sum_{i=2}^{\infty} P_i(\nu) y_i}{\sum_{i=2}^{\infty} P_i(\mu) y_i} \le \frac{P_2(\nu)}{P_2(\mu)} \tag{11}$$

Then,

$$\frac{\sum_{i=2}^{\infty} y_i \frac{v^i}{i!}}{\sum_{i=2}^{\infty} y_i \frac{\mu^i}{i!}} \le \frac{v^2}{\mu^2}$$

Multiplying both sides by $\mu^2 \sum_{i=2}^{\infty} y_i \frac{\mu^i}{i!}$, we get

$$\mu^2 \sum_{i=2}^{\infty} y_i \frac{v^i}{i!} \le v^2 \sum_{i=2}^{\infty} y_i \frac{\mu^i}{i!} \tag{12}$$

Using Eq. (10), we obtain

$$\mu^2 \left( Q_v e^v - y_0 - v y_1 \right) \le v^2 \left( Q_\mu e^\mu - y_0 - \mu y_1 \right) \tag{13}$$

By solving inequality (13), the lower bound of $y_1$ is given by

$$y_1 \ge y_1^{L,v} = \frac{1}{\left( \mu^2 v - v^2 \mu \right)} \left[ \mu^2 Q_v e^v - v^2 Q_\mu e^\mu - \left( \mu^2 - v^2 \right) y_0 \right] \tag{14}$$

According to Eq. (1), the lower bound of the gain of a single photon state is then given by

$$Q_1^{L,v} = \frac{\mu e^{-\mu}}{\left( \mu^2 v - v^2 \mu \right)} \left[ \mu^2 Q_v e^v - v^2 Q_\mu e^\mu - \left( \mu^2 - v^2 \right) y_0 \right] \tag{15}$$

The QBER of the one decoy state is given by

$$\begin{aligned} E_v Q_v e^v &= e_0 y_0 + v e_1 y_1 + \sum_{i=2}^{\infty} e_i y_i \frac{v^i}{i!} \\ &\ge e_0 y_0 + e_1 v y_1 \end{aligned} \tag{16}$$

By solving inequality (16), the upper bound of $e_1$ is

$$e_1 \le e_1^{U,v} = \frac{1}{v y_1^{L,v}} \left[ E_v Q_v e^v - e_0 y_0 \right] \tag{17}$$

Here, we will see how good are our estimations are for $y_1$ and $e_1$ for one decoy state protocol. By substituting Eqs. (1), (3), and (5) into Eq. (14), the lower bound of $y_1$ becomes

$$\begin{aligned} y_1^{L,v}\Big|_{v \to 0} &= \frac{1}{\left( \mu^2 v - v^2 \mu \right)} \left[ \mu^2 (y_0 + \eta v) e^v - v^2 (y_0 + \eta \mu) e^\mu - \left( \mu^2 - v^2 \right) y_0 \right] \Bigg|_{v \to 0} \\ &= y_0 + \eta \end{aligned} \tag{18}$$

which matches the theoretical value $y_1 \approx y_0 + \eta$ from Eq. (8) (see appendix).

Next, substituting Eqs. (2), (4), and (6) into Eq. (17), the upper bound of $e_1$ becomes

$$\begin{aligned} e_1 \le e_1^{U,v}\Big|_{v \to 0} &= \frac{1}{v y_1^{L,v}} \left[ (e_0 y_0 + e_{\text{det}} \eta v) e^v - e_0 y_0 \right] \Bigg|_{v \to 0} \\ &= \frac{e_{\text{det}} \eta + e_0 y_0}{y_1^L} \end{aligned} \tag{19}$$

Our estimation of the upper bound of $e_1$ matches the theoretical value from Eq. (9) (see appendix).

The above calculation seems to suggest that our estimations for $y_1$ and $e_1$ for a one decoy state protocol are as good as those for the most general protocol when $v \to 0.$

***Case B1 of one decoy state protocol for SARG04:*** In this protocol, we should estimate the lower bounds of $y_2$ and the upper bounds of $e_2$ to obtain the lower bound of the key generation rate for SARG04. Intuitively, only one decoy state is needed for the estimation. Here, we investigate how to use one decoy state to estimate these bounds.

Suppose that Alice randomly changes the intensity of her pump light among 2 values (one decoy state and a signal state) such that the intensity of one mode of the two mode source is randomly changed among $v$ and $\mu$, which satisfy the inequalities $0 \le v < \mu \le 1,$. $v$ is the mean photon number of the decoy state and $\mu$ is the expected photon number of the signal state.

According to Eq. (1), the gain of the signal and one decoy state are given by:

$$Q_\mu e^\mu = y_0 + \mu y_1 + \frac{\mu^2}{2} y_2 + \sum_{i=3}^{\infty} y_i \frac{\mu^i}{i!}$$

$$Q_v e^v = y_0 + v y_1 + \frac{v^2}{2} y_2 + \sum_{i=3}^{\infty} y_i \frac{v}{i!} \tag{20}$$

By using inequality (8) in [2] , with $0 \le v < \mu \le 1$ we obtain

$$\frac{\sum_{i=3}^{\infty} P_i(v) y_i}{\sum_{i=3}^{\infty} P_i(\mu) y_i} \le \frac{P_3(v)}{P_3(\mu)} \tag{21}$$

Then,

$$\frac{\sum_{i=3}^{\infty} y_i \frac{v^i}{i!}}{\sum_{i=3}^{\infty} y_i \frac{\mu^i}{i!}} \le \frac{v^3}{\mu^3} \tag{22}$$

Multiplying both sides by $\mu^3 \sum_{i=3}^{\infty} y_i \frac{\mu^i}{i!}$, we get

$$\mu^3 \sum_{i=3}^{\infty} y_i \frac{v^i}{i!} \le v^3 \sum_{i=3}^{\infty} y_i \frac{\mu^i}{i!} \tag{23}$$

Using Eq. (24), we obtain

$$\mu^3 \left( Q_v e^v - y_0 - v y_1 - \frac{v^2}{2} y_2 \right) \le v^3 \left( Q_\mu e^\mu - y_0 - \mu y_1 - \frac{\mu^2}{2} y_2 \right) \tag{24}$$

By solving inequality (24), the lower bound of $y_2$ is given by

$$y_2 \ge y_2^{L,v} = \frac{2}{\left(\mu^3 v^2 - v^3 \mu^2\right)} \left( \mu^3 Q_v e^v - v^3 Q_\mu e^\mu - (v\mu^3 - v^3 \mu) y_1 - \left(\mu^3 - v^3\right) y_0 \right) \tag{25}$$

According to Eq. (20), the lower bound of the gain of a two photon state is then given by

$$Q_2^{L,v} = \frac{\mu^2 e^{-\mu}}{\left(\mu^3 v^2 - v^3 \mu^2\right)} \left( \mu^3 Q_v e^v - v^3 Q_\mu e^\mu - (v\mu^3 - v^3 \mu) y_1^{L,v} - \left(\mu^3 - v^3\right) y_0 \right) \tag{26}$$

The QBER of the one decoy state is given by

$$E_\nu Q_\nu e^\nu = e_0 y_0 + \nu e_1 y_1 + \frac{\nu^2}{2} e_2 y_2 + \sum_{i=3}^{\infty} e_i y_i \frac{\nu^i}{i!}$$

$$\geq e_0 y_0 + \nu e_1 y_1 + \frac{\nu^2}{2} e_2 y_2 \qquad (27)$$

By solving inequality (27), the upper bound of $e_2$ is

$$e_2 \leq e_2^{U,\nu} = \frac{2}{\nu^2 y_2^{L,\nu}} \left( E_\nu Q_\nu e^\nu - \nu e_1 y_1 - e_0 y_0 \right) \qquad (28)$$

Here, we will see, how good are our estimations are for $y_2$ and $e_2$ for a two decoy state protocol. By substituting Eqs. (1), (3), (5) and $y_1 \leq y_0 + \eta$ into Eq. (25), the lower bound of $y_2$ becomes

$$y_2 \geq y_2^{L,\nu}\Big|_{\nu\to 0} = \frac{2}{\left(\mu^3\nu^2 - \nu^3\mu^2\right)} \left( \mu^3 (y_0 + \eta\nu) e^\nu - \nu^3 (y_0 + \eta\mu) e^\mu - (\nu\mu^3 - \nu^3\mu) y_1 - \left(\mu^3 - \nu^3\right) y_0 \right) \Bigg|_{\nu\to 0}$$

$$= 2\eta + y_0 \qquad (29)$$

which matches the theoretical value $y_2 \leq 2\eta + y_0$ from Eq. (8). (see appendix).

Here, substituting Eqs. (2), (4), (6) and $e_1 = \frac{e_{\text{det}}\eta + e_0 y_0}{y_1}$ into Eq. (28), the upper bound of $e_2$ becomes

$$e_2 \leq e_2^{U,\nu}\Big|_{\nu\to 0} = \frac{2}{\nu^2 y_2^{L,\nu}} \left( (e_0 y_0 + e_{\text{det}}\eta\nu) e^\nu - \nu e_1 y_1 - e_0 y_0 \right) \Big|_{\nu\to 0}$$

$$= \frac{2 e_{\text{det}}\eta + e_0 y_0}{y_2} \qquad (30)$$

Our estimation of the upper bound of $e_2$ matches the theoretical value from Eq. (9). (see appendix).

The above calculation seems to suggest that our estimations for $y_1$, $y_2$, $e_1$ and $e_2$ for the one decoy state protocol are as good as those of the most general protocol when $\nu \to 0$.

Our estimations match the theoretical values when $\nu$ tends toward zero, which gives an optimal key generation rate (for BB84 and SARG04) and is the same as having an infinite number of decoy states.

Here, we estimate $e_1$ and $e_2$ for a one decoy state protocol. These estimations will be needed in the case of a two decoy state protocol. The QBERs of the signal and one decoy state are given by

$$E_\mu Q_\mu e^\mu = e_0 y_0 + \mu e_1 y_1 + \sum_{i=2}^{\infty} e_i y_i \frac{\mu^i}{i!}$$

$$E_\nu Q_\nu e^\nu = e_0 y_0 + e_1 \nu y_1 + \sum_{i=2}^{\infty} e_i y_i \frac{\nu^i}{i!} \qquad (31)$$

By using Eq. (31) , with $0 \leq \nu < \mu \leq 1$, we obtain

$$\sum_{i=2}^{\infty} e_i y_i \frac{\mu^i}{i!} \geq \sum_{i=2}^{\infty} e_i y_i \frac{\nu^i}{i!} \qquad (32)$$

Then,

$$E_\mu Q_\mu e^\mu - e_0 y_0 - \mu e_1 y_1 \geq \left( E_\nu Q_\nu e^\nu - e_0 y_0 - \nu e_1 y_1 \right) \qquad (33)$$

By solving inequality (33), the upper bound of $e_1$ is

$$e_1 \le e_1^{U,v} = \frac{1}{(\mu - v) y_1^{L,v}} \left[ E_\mu Q_\mu e^\mu - E_v Q_v e^v \right] \quad (34)$$

Next, we estimate $e_2$. By using Eq. (31) , with $0 \le v < \mu \le 1,$ we obtain

$$\sum_{i=3}^{\infty} e_i y_i \frac{\mu^i}{i!} \ge \sum_{i=3}^{\infty} e_i y_i \frac{v^i}{i!} \quad (35)$$

Then,

$$E_\mu Q_\mu e^\mu - e_0 y_0 - \mu e_1 y_1 - \frac{\mu^2}{2} e_2 y_2 \ge \left( E_v Q_v e^v - e_0 y_0 - v e_1 y_1 - \frac{v^2}{2} e_2 y_2 \right) \quad (36)$$

By solving inequality (36), the upper bound of $e_2$ is

$$e_2 \le e_2^{U,v} = \frac{2}{(\mu^2 - v^2) y_2^{L,v}} \left[ E_\mu Q_\mu e^\mu - E_v Q_v e^v - (\mu - v) e_1 y_1 \right] \quad (37)$$

After estimating the lower bounds of $y_1$ and $y_2$ and the upper bounds of $e_1$ and $e_2$ for each decoy state protocol. we can then use the following formula to calculate the final key generation rate of our QKD system for both the BB84 and SARG04 protocols [37]:

$$R_{BB84} \ge R_{BB84}^L = q\{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1^L [1 - H_2(e_1^U)]\} \quad (55)$$

$$R_{SARG04} \ge R_{SARG04}^L = -Q_\mu f(E_\mu) H_2(E_\mu) + Q_1^L [1 - H_2(e_1^U)] + Q_2^L [1 - H_2(e_2^U)] \quad (56)$$

where q depends on the implementation (1/2 for the BB84 protocol because half of the time, Alice and Bob disagree with the bases; if one uses the efficient BB84 protocol [10], q ≈ 1) f(x) is the bi-direction error correction efficiency as a function of the error rate (normally, f(x) ≥ 1 with the Shannon limit f(x) = 1), and $H_2(x)$ is the binary Shannon information function, which has the form $H_2(x) = -x \log2(x) - (1 - x) \log2 (1 - x)$.

## III. Optical Fiber Based Qkd System Simulation

We attempt to simulate an optical fiber-based QKD system using our decoy state method for both SARG04 and BB84 ; the losses in the quantum channel can be derived from the loss coefficient $\alpha$ in dB/km and the length of the fiber *l* in km. The channel transmittance can be written as $\eta_{AB} = 10^{-\frac{\alpha l}{10}}$, and the overall transmission between Alice and Bob is given by $\eta = \eta_{Bob} \eta_{AB}$, where $\alpha = 0.21 dB/km$ in our set-up is the loss coefficient, and $\eta_{Bob}$ is the transmittance on Bob's side. We choose a detection efficiency of $\eta = 4.5 \times 10^{-2}$, detectors dark count rate of $y_0 = 1.7 \times 10^{-6}$, the probability that a photon hits the erroneous detector $e_{\det ector} = 0.033$,wavelength $\lambda = 1550 nm$ and the total number of pulses sent by Alice $N = 100 Mbit$. These parameters are taken from the GYS experiment [38]. We choose the intensities, the percentages of the signal state and decoy states that could result in the optimization of the key generation rate and the maximum secure distance of one decoy state protocol for BB84 and SARG04. The search for optimal parameters can be obtained via numerical simulation using Matlab.

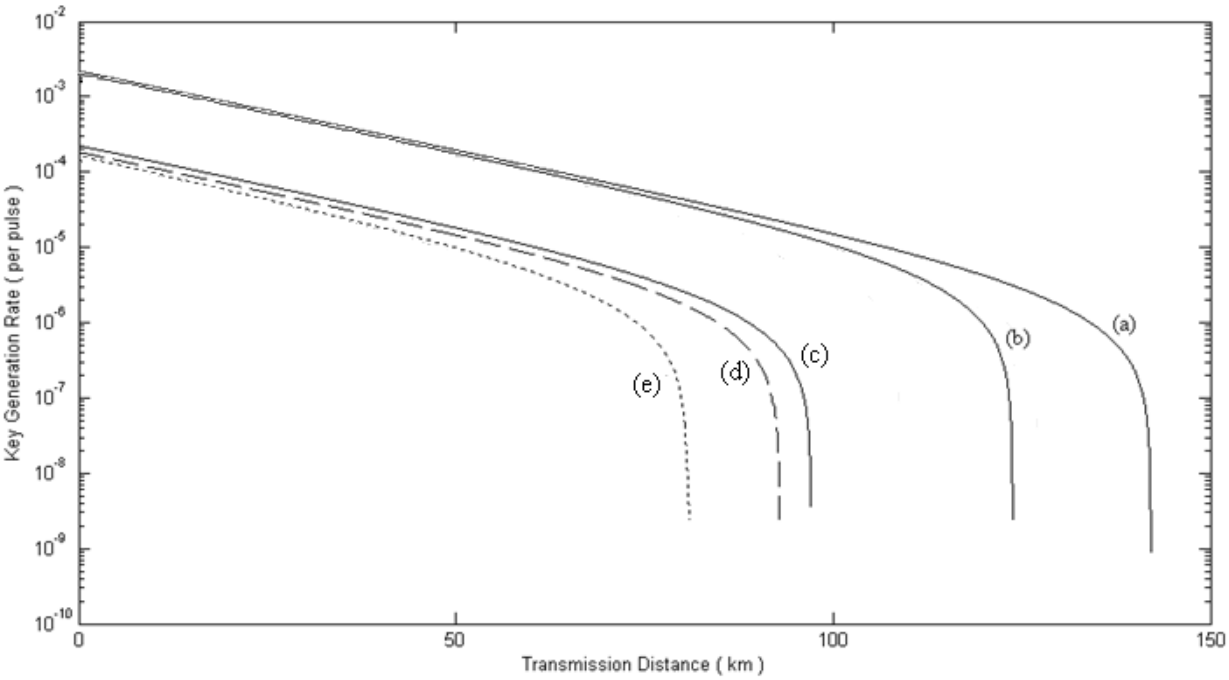


**Figure 1:** The simulation results of the key generation rate versus the secure distance of fiber link for different decoy state protocols. (a) The asymptotic decoy state method (with an infinite number of decoy states) for BB84. (b) The key generation rate of one decoy state protocol for BB84. (c) For both single and two photon contributions (SARG04). (d) For only single-photon contributions. (SARG04). (e) One decoy state protocol for SARG04.

Figure 1 illustrates the simulation results of the key generation rate versus the secure distance of fiber link for different decoy state protocols with statistical fluctuation. (a) The asymptotic decoy state method (with an infinite number of decoy states) for BB84. (b) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84). (c) The asymptotic decoy state method (with an infinite number of decoy states) for both single and two-photon contributions (SARG04). (d) The asymptotic decoy state method (with an infinite number of decoy states) for only single-photon contributions (SARG04). (e) The key generation rate of one decoy state protocol with the statistical fluctuations (SARG04). Comparing these curves, it can be observed that the fiber-based QKD system using the one decoy state method for BB84 is able to achieve both a higher secret key rate and greater secure distance than SARG04. The maximal secure distances of the five curves are 142 km, 111.9 km, 97 km, 94 km, and 69 km.

## IV. Conclusions

We have studied the one-decoy-state protocol ( $\nu \to 0 \leq \nu < \mu \leq 0$ ), where one decoy state of intensity $\nu$ and signal state with intensity $\mu$ are employed for BB84 and SARG04. We have performed optimization on the choice of intensity of the one decoy states. The estimations show that a decoy state protocol with only one decoy state ( ) can approach the theoretical limit and gives an optimal key generation rate, which is the same as having an infinite number of decoy states for BB84 and SARG04. Our results show that the fiber-based QKD system, using the proposed method for BB84, is able to achieve both a higher secret key rate and greater secure distance than that of SARG04. Hence, the two-photon part has a contribution to the key generation rates at all distances.

## V. References

[1]. C.H. Bennett and G. Brassard, in : Proc. IEEE Int. Conf. on Computers, systems, and signal processing, Bangalore (IEEE, New York, 1984) p.175.
[2]. D. Mayer, J. Assoc. Comput. Mach. 48, 351 (2001). Its preliminary version appeared in"Advances in Cryptology-Proc. Crypto'96, Vol. 1109 of Lecture Notes in Computer Science,Ed. N. Koblitz, Springer-Verlag, New York, 1996, p. 343.
[3]. P.W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000).
[4]. A.K. Ekert, Phys. Rev. Lett. 67, 661 (1991), C.H. Bennett, D.P. DiVincenzo, J.A. Smolin,and W.K. Wootters, Phys. Rev. A 54, 3824 (1996); A.K. Ekert, Phys. Rev. Lett. 67, 661(1991), C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A 54,3824 (1996).

[5].D. Gottesman, H.-K. Lo, N. L¨ukenhaus, and J. Preskill, Quantum Information and Computation 5, 325 (2004), arXiv:quant-ph/0212066.
[6].H. Inamori, N. L¨ukenhaus, and D. Mayers (2001), arXiv:quant-ph/0107017.
[7].W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
[8].H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).
[9].H.-K. Lo, in Proc. of IEEE International Symposium on Information Theory (ISIT) 2004 (2004), p. 137, arXiv:quant-ph/0509076.
[10].D. Gottesman *et al.*, Quantum Inf. Comput. **4**, 325 (2004).
[11].H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[12].X.-B. Wang, Phys. Rev. A 72, 012322 (2005)
[13].J.-B. Li, and X.-M. Fang, Chin. Phys. Lett. 23, No. 4 (2006)
[14].Qing-yu Cai, and Yong-gang Tan, Phys. Rev. A. 73, 032305 (2006)
[15].Tomoyuki Horikiri, and Takayoshi Kobayashi, Phys. Rev. A 73, 032331 (2006)
[16].Qin Wang, X.-B. Wang, and G.-C. Guo, Phys. Rev. A 75, 012312 (2007)
[17].Z.-Q. Yin, Z.-F. Han, F.-W. Sun, and G.-C. Guo, Phys. Rev. A 76, 014304 (2007)
[18].X.-B. Wang, C.-Z. Peng, and J.-W. Pan, Appl. Phys. Lett. 90, 6031110 (2007)
[19].X.-B.Wang, Phys. Rev. A 75, 052301 (2007)
[20].Y. Zhao et al., Phys. Rev. Lett. 96, 070502 (2006)
[21].Yi Zhao et al, Proceedings of IEEE International Symposiumon Information Theory 2006, pp. 2094-2098
[22].C.-Z. Peng et al., Phys. Rev. Lett. 98, 010505 (2007)
[23].D. Rosenberg, J. W. Harrington, P. R. Rice, et al., Phys. Rev. Lett. 98, 010503 (2007)
[24].Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. 90 011118 (2007)
[25].Tobias Schmitt-Manderbach et al., Phys. Rev. Lett. 98, 010504 (2007)
[26].Wang, X.B. 2013 Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Phys. Rev. A*, 87(1), 012320. arXiv:1308.56
[27].Tang, Z., Liao, Z., Xu, F., Qi, B., Qian, L., & Lo, H.K. 2014 Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 112(19), 190503.
[28].Jiang, H., Gao, M., Wang, H., Li, H., & Ma, Z. 2015 Four-intensity Decoy state Quantum Key Distribution with enhanced resistance against statistical fluctuation. Preprint. arXiv:1502.0224
[29].Abellán, C.; Amaya, W.; Jofre, M.; Curty, M.; Acín, A.; Capmany, J.; Pruneri, V.; Mitchell, M.W. Ultra-Fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode. Opt. Express 2014, 22, 1645–1654
[30].Hayashi, M.; Nakayama, R. Security analysis of the decoy method with the Bennett–Brassard 1984 protocol for finite key lengths. New J. Phys. 2014, 16, 063009.
[31].Lim, C.C.W.; Curty, M.; Walenta, N.; Xu, F.; Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. Phys. Rev. A 2014, 89, 022307.
[32].Wang, J.-Y.; Yang, B.; Liao, S.-K.; Zhang, L.; Shen, Q.; Hu, X.-F.;Wu, J.-C.; Yang, S.-J.; Jiang, H.; Tang, Y.-L.; et al. Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. Nat. Photonics 2013, 7, 387–39
[33].[34] Marcos Curty, Marc Jofre, Valerio Pruneri and Morgan W. Mitchell. Passive Decoy-State Quantum Key Distribution with Coherent Light. Entropy 2015, 17, 4064-4082; doi:10.3390/e17064064
[34].X. Ma, B. Qi, Yi Zhao and H.-K. Lo: quant-ph/0410075
[35].W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication", Phys. Rev. Lett. 91, 057901 (2003)
[36].K. Tamaki and H.-K. Lo. Unconditionally secure key distillation from multiphotons. *Physical Review A* 73, 010302(R) (2006).
*[37].*C. Gobby, Z. L. Yuan, and A. J. Shields, *"Quantum key distribution over 122 km of standard telecom fiber"*, Applied Physics Letters, Volume 84, Issue 19, pp. 3762-3764, (2004).

**Appendix**

***Case A1 of one decoy state protocol for BB84:***

Substituting Eqs. (1), (3), and (5) into Eq. (14), the lower bound of $y_1$ becomes

$$y_1^{L,\nu} = \frac{1}{\left(\mu^2\nu - \nu^2\mu\right)}\left[\mu^2(y_0+\eta\nu)e^{\nu} - \nu^2(y_0+\eta\mu)e^{\mu} - \left(\mu^2-\nu^2\right)y_0\right]\Bigg|_{\nu\to 0}$$

$$= \frac{0}{0} \qquad \text{(A1)}$$

Using l'Hopital's rule to evaluate the limit for the indeterminate case,

$$y_1^{L,\nu}\Big|_{\nu\to 0} = \frac{1}{\left(\mu^2 - 2\nu\mu\right)}\left[\mu^2(y_0+\eta\nu)e^{\nu} + \mu^2\eta e^{\nu} - 2\nu(y_0+\eta\mu)e^{\mu} + 2\nu y_0\right]\Bigg|_{\nu\to 0}$$

$$= \frac{1}{\mu^2}\left[\mu^2 y_0 + \mu^2\eta\right]$$

$$= y_0 + \eta \qquad \text{(A2)}$$

Next, substituting Eqs. (2), (4), and (6) into Eq. (17), the upper bound of $e_1$ becomes

$$e_1 \le e_1^{U,\nu} = \frac{1}{\nu y_1^{L,\nu}}\left[(e_0 y_0 + e_{\text{det}}\eta\nu)e^{\nu} - e_0 y_0\right]\Big|_{\nu\to 0}$$

$$= \frac{0}{0} \qquad \text{(A3)}$$

Using l'Hopital's rule to evaluate the limit for the indeterminate case,

$$e_1 \le e_1^{U,\nu} = \frac{1}{y_1^{L,\nu}}\left[(e_0 y_0 + e_{\text{det}}\eta\nu)e^{\nu} + e_{\text{det}}\eta e^{\nu}\right]\Big|_{\nu\to 0}$$

$$= \frac{e_{\text{det}}\eta + e_0 y_0}{y_1^{L}} \qquad \text{(A4)}$$

***Case B1 of one decoy state protocol for SARG04:***

Substituting Eqs. (1), (3), (5) and $y_1 \square\ y_0 + \eta$ into Eq. (25), the lower bound of $y_2$ becomes

$$y_2 \ge y_2^{L,\nu} = \frac{2}{\left(\mu^3\nu^2 - \nu^3\mu^2\right)}\left(\mu^3(y_0+\eta\nu)e^{\nu} - \nu^3(y_0+\eta\mu)e^{\mu} - (\nu\mu^3 - \nu^3\mu)(y_0+\eta) - \left(\mu^3 - \nu^3\right)y_0\right)\Big|_{\nu\to 0}$$

$$= \frac{0}{0} \qquad \text{(A5)}$$

Using l'Hopital's rule to evaluate the limit for the indeterminate case,

$$y_2^{L,\nu}\Big|_{\nu\to 0} = \frac{2}{\left(2\mu^3\nu - 3\nu^2\mu^2\right)}\left[\mu^3(y_0+\eta\nu)e^{\nu} + \mu^3\eta e^{\nu} - 3\nu^2(y_0+\eta\mu)e^{\mu} - (\mu^3 - 3\nu^2\mu)(y_0+\eta) + 3\nu^2 y_0\right]\Big|_{\nu\to 0}$$

$$= \frac{0}{0} \qquad \text{(A6)}$$

Using the second l'Hopital's rule to evaluate the limit for the indeterminate case,

$$y_2^{L,\nu}\Big|_{\nu\to 0} = \frac{2}{\left(2\mu^3 - 6\nu\mu^2\right)}\left[\mu^3(y_0+\eta\nu)e^{\nu} + \mu^3\eta e^{\nu} + \mu^3\eta e^{\nu} - 6\nu(y_0+\eta\mu)e^{\mu} + 6\nu\mu(y_0+\eta) + 6\nu y_0\right]\Big|_{\nu\to 0}$$

$$= \frac{2}{2\mu^3}\left[2\mu^3\eta + \mu^3 y_0\right]$$

$$= 2\eta + y_0 \qquad \text{(A7)}$$

Here, substituting Eqs. (2), (4), (6) and $e_1 = \frac{e_{\text{det}}\eta + e_0 y_0}{y_1}$ into Eq. (28), the upper bound of $e_2$ becomes

$$e_2 \le e_2^{U,\nu} = \frac{2}{\nu^2 y_2^{L,\nu}}\left(E_\nu Q_\nu e^{\nu} - \nu e_1 y_1 - e_0 y_0\right)\Big|_{\nu\to 0}$$

$$= \frac{2}{\nu^2 y_2^{L,\nu}}\left((e_{\text{det}}\eta\nu + e_0 y_0)e^{\nu} - \nu(e_{\text{det}}\eta + e_0 y_0) - e_0 y_0\right)\Big|_{\nu\to 0}$$

$$= \frac{0}{0} \tag{A8}$$

Using l'Hopital's rule to evaluate the limit for the indeterminate case,

$$e_2^{U,\nu}\Big|_{\nu\to 0} = \frac{2}{2\nu y_2^{L,\nu}}\left((e_{\text{det}}\eta\nu + e_0 y_0)e^{\nu} + e_{\text{det}}\eta e^{\nu} - (e_{\text{det}}\eta + e_0 y_0)\right)\Big|_{\nu\to 0}$$

$$= \frac{0}{0} \tag{A9}$$

Using the second l'Hopital's rule to evaluate the limit for the indeterminate case,

$$e_2^{U,\nu}\Big|_{\nu\to 0} = \frac{2}{2y_2^{L,\nu}}\left[(e_{\text{det}}\eta\nu + e_0 y_0)e^{\nu} + e_{\text{det}}\eta e^{\nu} + e_{\text{det}}\eta e^{\nu}\right]\Big|_{\nu\to 0}$$

$$= \frac{2e_{\text{det}}\eta + e_0 y_0}{y_2} \tag{A10}$$

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

* M. Abdellatief. " Practical QKD For Both BB84 And SARG04 Protocols." IOSR Journal of Computer Engineering (IOSR-JCE) 20.1 (2018): 37-47.