Experimental Two Way Quantum Key Distribution with Weak+Vacuum Decoy State

M. F. Abdul Khir, M. N. Mohd Zain, Iskandar Bahari, Suryadi and S. Shaari

1 Photonic Lab, IMEN, Universiti Kebangsaan Malaysia, UKM Bangi, Malaysia
2 Faculty of Science, International Islamic University of Malaysia (IIUM), Kuantan, Pahang, Malaysia
3 Photonics Technology and Product Development (PTPD), MIMOS Berhad, Kuala Lumpur, Malaysia
4 Cryptography Lab, Advanced Analysis and Modeling (ADAM) Cluster, MIMOS Berhad, Kuala Lumpur, Malaysia

E-mail: mfared@mimos.my, zman@mimos.my, iskandar.bahari@mimos.my, suryadi@iiu.edu.my and sahbudin@eng.ukm.my
*Corresponding author

ABSTRACT

We report a free space based experimental demonstration of a two way Quantum Key Distribution protocol with weak+vacuum decoy state. By utilizing a different key rate formula a better maximum secure distance closer to the theoretical infinite was achieved.

Keywords: Quantum Key Distribution protocol, formula, secure distance.

1. INTRODUCTION

Over the past twenty years, Quantum Cryptography (QC) or better known as Quantum Key Distribution (QKD) has undergone quiet an extensive developments in its realization. Many recent activities have
reported efforts on practical aspect of QKD implementation. One such effort is the decoy state protocol (Hwang 2003) which has attracted much attention within the QKD community. Being a tool to defeat the Photon Number Splitting (PNS) attack, the decoy state QKD has revived the practicality of a weak pulse based QKD implementation. This important discovery by Hwang et al. (2003) has led to many further important works by such as (Lo et al. (2005), Ma et al. (2005), Zhao et al. (2006)) for two decoy states and the weak+vacuum decoy state. However most of these works are confined within the prepare and measure scheme such as the BB84 protocol and the SARG04 protocol (Zhang et al. (2008), Zhang et al. (2009)). Recently, the extension of decoy state method for two way QKD protocol (Ostermeyer et al. (2008), Lucamarini et al. (2007), Shaari et al. (2006), Lucamarini et al. (2005), Cere (2006), Kumar et al. (2008)) was studied by Shaari et al. (2011). They have derived relevant bounds for the case of the LM05 protocol with two decoy states at different intensities similar to the one proposed for the BB84 protocol in (Ma et al. (2005)) and have shown that the maximum secure distance of the LM05 protocol can be increased by nearly double. In their work, two secure key rate formulas denoted as $R_{1+2}$ and $R_{12}$ were proposed, representing the case when the single and double photon contributions are separately calculated and the case when the single and double photon contributions are lumped. While the former enjoys better maximum secure distance, the latter enjoys the advantage of not having to concern on how Eve may manipulate the single and double photon contributions individually.

The significant work in (Shaari et al. (2011)) was further extended in (Abdul Khir et al. (2011a), Abdul Khir et al. (2011b)) for the case of weak+vacuum decoy state protocol which has yielded similar result. Having the vacuum state as the second decoy state simplifies the source setup and benefits in terms of cost saving. This is evidenced in our work in (Abdul Khir et al. (2012a)) when we demonstrated the first implementation of a two way QKD protocol with decoy state. In order to accommodate the proposed decoy state, we have upgraded the previously developed free space based LM05 system in (Abdul Khir (2012b)) which required just a simple modification at the source part and the software part. While the result in (Abdul Khir (2012a)) turned out to confirm the theoretical works in (Shaari et al. (2011), Abdul Khir (2011b)) for the case of $R_{12}$ formula it lacks the same for the $R_{1+2}$ formula. Hence, in this work, we continue the experiment with the $R_{1+2}$ formula and compare the performance with the theoretical values and previous works. The next section reviews the proposed decoy state method, followed by explanation on the experimental
setup in section three. The result is discussed in section four while section five conclude and suggest future works.

2. THE PROTOCOL

An implementation of a weak+vacuum decoy state on the LM05 protocol is similar to the BB84 protocol and SARG04 protocol where in addition to the signal state with mean photon number $\mu$, two decoy states with mean photon number $\nu$ and zero are introduced. The state with zero intensity is called the vacuum state and is used to precisely obtain the background rate $Y_0$. With a proper optimization of the parameters involved, the lower bound of the secure key rate $R_{1+2}$ can be estimated. Note that the decoy state is not used as part of the final secure key. Its function is just to detect Eve’s attempt (Lo et al. (2005)) and estimating the secure key rate. As explained in (Abdul Khir et al. (2011a)) for the single photon gain, we directly used equation from (Ma et al. (2005)) while for the double photon gain, the single photon as well as the double photon error rate, we use the one derived for the case of weak+vacuum decoy state from (Shaari et al. (2011)).

The lower bound gain of single photon state ($Q_1$) and double photon state ($Q_2$) are given respectively in (Abdul Khir et al. (2011a), Abdul Khir (2011b)) as:

$$Q_1 \geq Q_1^l = \frac{\mu^2 e^{-\mu}}{\mu - \frac{\nu^2}{2}} \left( Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0 \right)$$

(1)

$$Q_2 \geq \frac{\mu^3 e^{-\mu}}{\nu^2 \mu - \nu^3} \left( Q_\nu e^\nu - \frac{\nu^3}{\mu^3} Q_\mu e^\mu - \frac{\mu^3 - \nu^3}{\mu^3} Y_0 - \frac{\nu \mu^2 - \nu^3}{\mu^2} Y_1^U \right)$$

(2)

where $Y_1^U$ is the upper bound of single photon yield given by

$$Y_1^U = \frac{(2Q_\nu e^\nu - 2Y_0 - Y_2^\infty \nu^2)}{2\nu}$$

(3)

The $Q_\nu$ is the gain from decoy state and the $Y_2^\infty$ is the double photon yield from infinite case. The upper bound error rate of the single photon ($e_1$) and double photon ($e_2$) are given respectively as
The lower bound of the key generation rate is given by Shaari et al. (2011)
as:

\[ e_1^U \leq e_1^L = \frac{(E_0^v Q_v e^v - e_0 Y_0^v) \mu^2 - (E_\mu^v Q_\mu e^\mu - e_0 Y_0^\mu) \nu^2}{Y_1^L (\nu \mu^2 - \mu \nu^2)} \]  

\[ e_2^U \leq e_2^L = \frac{(E_0^v Q_v e^v - e_0 Y_0^v) \mu - (E_\mu^v Q_\mu e^\mu - e_0 Y_0^\mu) \nu}{Y_2^L \left( \frac{1}{2} \nu \mu^2 - \frac{1}{2} \nu \mu^2 \right)} \]  

(4)  

(5)

The lower bound of the key generation rate is given by Shaari et al. (2011) as:

\[ R_{1+2} \geq R_{1+2}^L = -Q_\mu f(E_\mu) H(E_\mu) + \sum_{i=1}^{2} Q_i [1 - \tau(e_i)] \]  

(6)

where

\[ H(E_\mu) \] is the binary Shannon Entrophy and is given by

\[ H(E_\mu) = -E_\mu \log_2(E_\mu) - (1 - E_\mu) \log_2(1 - E_\mu) \]  

\( \tau(e) \) is the amount bits to be discarded during privacy amplification stage and is given as

\[ \tau(e_1) = \log_2(1 + 4e_1 - 4e_1^2) \] for \( e_1 < \frac{1}{2} \) and \( \tau(e_1) = 1 \) if \( e_1 \geq \frac{1}{2} \).

### 3. EXPERIMENTAL SETUP

#### 3.1 Optics

The schematic of the experimental setup is depicted in Figure 1. It is the same setup used in (Abdul Khir et al. (2012a)) which involved decoy states implementation with the \( R_{12} \) secure key rate formula. The optical setup at Bob consists of the source and detector package. The source package consists of two sets of laser source and a Pockels cell (PC1). The first set of laser source which is used as the signal source consists of LAS1 and LAS2 emitting horizontal and vertical pulse respectively. The second set of the laser source consists of LAS3 and LAS4 also emitting horizontal and vertical pulse respectively. After going through the beam splitters (BS1 and PBS1) and also a spatial filter (SF), each optical pulses are polarization modulated at Pockels cell (PC1) where the horizontal and vertical pulses are polarization transformed into anti-diagonal or diagonal pulses respectively.

This combination prepares the four polarization states for signal and decoy states needed in realizing the LM05 protocol and decoy state
Experimental Two Way Quantum Key Distribution with Weak+Vacuum Decoy State

The detector package consists of one Pockels cell (PC4), a Wollaston prism (WOL) and two single photon counting modules (SPCM1 and SPCM2). The optical setup at Alice was a minimal one consists of a beam splitter (BS3) and the flipper (PC2 and PC3). Alice uses the flipper to encode logical bit 1 by triggering it and logical bit 0 by not doing anything. The flipper consists of two Pockels cells (PC2 and PC3) which is capable of orthogonally rotating any of the four polarization states sent by Bob. The purpose of beam splitter (BS3) is to give the effect of control mode which is not implemented in this setup.

### 3.2 Electronics

All active optical components at Bob and Alice including the laser sources, Pockels cells and detectors are controlled by a LabVIEW based program that run and synchronized using a pair of 40 MHz Reconfigurable I/O module of National Instruments (PXI-7833R). The random triggering for state preparations uses software based pseudo-random number generator. The pulses are distributed 50% for signal, 25% for decoy and 25% for vacuum with pulse repetition rate at 0.725 MHz.

![Diagram of experimental setup](image1)

**Figure 1:** The LM05 and decoy state experimental setup consists of LAS1, LAS2, photon source for signal state; LAS3, LAS4, photon source for decoy state; PBS1, polarization beam splitter; SF, spatial filter; PC1, first Pockels cell; ATTN1, variable attenuator; BS1, BS2 50/50 beam splitter; ATTN2, ATTN3 attenuator; PC2, second Pockels cell; PC3, third Pockels cell; PC4, Fourth Pockels cell; IF1, interference filter; WOL1, Wollaston Prism; SPCM1, H & D detector; SPCM2, V & A detector
4. RESULTS AND DISCUSSION

In the first stage of the experiment, the intrinsic parameters necessary for optimal mean photon number optimization i.e. the $\eta_{Bob}$ and the $e_{detector}$ were measured. These parameters are summarized in Table 1. The $\eta_{Bob}$ represents the overall intrinsic transmission of the system, taking into account the intrinsic loss and the quantum efficiency of the detectors. The $e_{detector}$ is the QBER when the background noise is negligible. It is obtained by measuring the QBER after sending train of pulses with high mean photon number. Next, numerical simulation was conducted to find the optimal mean photon number for a particular distance as well as the maximum secure distance capable with this setup. The maximum secure distance is defined as the maximum distance between Bob and Alice before the secure key generation rate hits zero. The optimal mean photon number ($\mu$) at particular distance is the $\mu$ that results in the highest key generation rate. However, as noted in (Ma et al. (2005)), the secure key generation rate does not change much with small changes in $\mu$. Hence, a fixed mean photon number, $\mu=0.15$ for LM05 and mean photon number for signal pulses $\mu=0.64$ and for decoy pulses $\nu=0.23$ were used throughout the experiment.

TABLE 1: Intrinsic parameters of the system

<table>
<thead>
<tr>
<th>Frequency [MHz]</th>
<th>Detector Efficiency ($\eta_{Det}$)</th>
<th>$e_{detector}$ [%]</th>
<th>Overall intrinsic transmission of the system ($\eta_{Bob}$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.725</td>
<td>0.55</td>
<td>0.045</td>
<td>0.072</td>
</tr>
</tbody>
</table>

We took several points corresponding to several channel losses, each with 140 Mbit of samples. The experimental result is shown in Table 2 which consists of channel loss in dB, the signal gain ($Q_\mu$) and QBER ($E_\mu$), the decoy gain ($Q_\nu$) and QBER ($E_\nu$), the background noise $Y_0$ and finally the secure key generation rate ($R^{L}$) calculated using Equations 1 - 6. We used error correction efficiency $f(E_\mu) = 1.22$ for secure key rate calculation. The corresponding graph is depicted in Figure 1. Note that for the case of without decoy state, we have made use of the secure key generation rate ($R_{LM}$) formula in (Lucamarini et al. (2007)).
The theoretical line for the case of when one uses the key rate formula $R_{12}$ in Abdul Khir (2011b), Abdul Khir (2012a) where the single and double photon contribution were lumped is also presented. This provides sort of a base comparison to better illustrate the improvement achieved and how well the proposed decoy state extension performs.

**TABLE 2:** Experimental results for $Q_\mu$, $E_\mu$, $Q_\nu$, $E_\nu$ and $Y_0$ for six cases of channel loss.

<table>
<thead>
<tr>
<th>Channel Loss (dB)</th>
<th>$Q_\mu$</th>
<th>$E_\mu$</th>
<th>$Q_\nu$</th>
<th>$E_\nu$</th>
<th>$Y_0$</th>
<th>$R^L$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.19</td>
<td>$1.57 \times 10^{-2}$</td>
<td>$4.75 \times 10^{-2}$</td>
<td>$5.81 \times 10^{-3}$</td>
<td>$4.67 \times 10^{-2}$</td>
<td>$4.30 \times 10^{-6}$</td>
<td>$3.90 \times 10^{-3}$</td>
</tr>
<tr>
<td>5.20</td>
<td>$4.02 \times 10^{-3}$</td>
<td>$4.95 \times 10^{-2}$</td>
<td>$1.45 \times 10^{-3}$</td>
<td>$4.94 \times 10^{-2}$</td>
<td>$3.72 \times 10^{-6}$</td>
<td>$8.44 \times 10^{-4}$</td>
</tr>
<tr>
<td>7.42</td>
<td>$1.39 \times 10^{-3}$</td>
<td>$5.09 \times 10^{-2}$</td>
<td>$4.84 \times 10^{-4}$</td>
<td>$5.45 \times 10^{-2}$</td>
<td>$4.24 \times 10^{-6}$</td>
<td>$2.03 \times 10^{-4}$</td>
</tr>
<tr>
<td>9.51</td>
<td>$5.58 \times 10^{-4}$</td>
<td>$5.42 \times 10^{-2}$</td>
<td>$2.10 \times 10^{-4}$</td>
<td>$5.96 \times 10^{-2}$</td>
<td>$3.37 \times 10^{-6}$</td>
<td>$7.67 \times 10^{-5}$</td>
</tr>
<tr>
<td>11.49</td>
<td>$2.26 \times 10^{-4}$</td>
<td>$6.22 \times 10^{-2}$</td>
<td>$8.64 \times 10^{-5}$</td>
<td>$6.45 \times 10^{-2}$</td>
<td>$3.63 \times 10^{-6}$</td>
<td>$3.22 \times 10^{-5}$</td>
</tr>
<tr>
<td>13.58</td>
<td>$8.17 \times 10^{-5}$</td>
<td>$8.01 \times 10^{-2}$</td>
<td>$3.31 \times 10^{-5}$</td>
<td>$1.23 \times 10^{-1}$</td>
<td>$3.42 \times 10^{-6}$</td>
<td>$6.95 \times 10^{-6}$</td>
</tr>
</tbody>
</table>

Figure 2: Experimental plots and numerical simulation results for the case of $R_{12}$, $R_{LM}$, $R_{12}$ and $R_{4+2}$. The dash line is $R_{LM}$, the dashdot line is the theoretical line for the case of $R_{12}$ using the key rate used in (Abdul Khir et al. 2011a), the $R_{12}$ is the key rate obtained with formula in Eq. 6 and the dot line is the theoretical curve for the case of infinite decoy state.

From Figure 2, it is obvious that without decoy state ($R_{LM}$), a maximum secure distance will reach less than 7 dB channel loss. In contrast, using the proposed weak+vacuum decoy state, the maximum secure distance of the setup was extended by almost double. We verified that at 16.18 dB, the key rate is already negative. The achieved maximum secure distance was also better than the one obtained with the other key rate $R_{12}$ used in (Abdul Khir et al. 2011a) where the single and doublephoton contribution is lumped.
We note that the achieved key rate was good since it is not far from the one obtained from the case of theoretical infinite decoy state ($R_\infty$). If one were to use the optimal $\mu$ and $\nu$ for every distance, this gap will be closer. The result also showed quite a good agreement between the experimental and theoretical result.

5. CONCLUSIONS AND FUTURE WORKS

A QKD system based on a two way protocol namely the LM05 protocol and the decoy state method was successfully demonstrated. Using a better estimation of decoy state parameters has resulted in a better maximum secure distance, closer to the theoretical limit achievable with an infinite decoy state. Besides the weak+ vacuum decoy state used in this work, another practical decoy state method which utilizes only one decoy state was also proposed in (Abdul Khir et al. (2011b)). It is interesting to see this one decoy state protocol in action. We leave this as our future work.

REFERENCES


