IJL, Issue 1, Vol. 23, 2024
https://doi.org/10.31900/ijl.v23i1.455

Research Article

IJL IRAQI JOURNAL OF LASER

Estimation of mean photon number based on single photon detection of weak coherent pulses

Hawraa A. Ghanem*, **Shelan K. Tawfeeq**

Institute of Laser for Postgraduate Studies, University of Baghdad, Baghdad, Iraq
** Email address of the Corresponding Author: hawraa.abd2201m@ilps.uobaghdad.edu.iq*

Article history: Received 28 Feb. 2024; Revised 24 Mar.2024; Accepted 27 Mar.2024; Published online 15 Jun.2024

Abstract: The demand for single photon sources in quantum key distribution (QKD) systems has necessitated the use of weak coherent pulses (WCPs) characterized by a Poissonian distribution. Ensuring security against eavesdropping attacks requires keeping the mean photon number (μ) small and known to legitimate partners. However, accurately determining μ poses challenges due to discrepancies between theoretical calculations and practical implementation. This paper introduces two experiments. The first experiment involves theoretical calculations of μ using several filters to generate the WCPs. The second experiment utilizes a variable attenuator to generate the WCPs, and the value of μ was estimated from the photons detected by the BB84 detection setup. The second experiment represents an accurate method for estimating the value of μ because of using single photon detectors with high timing resolution and low dark counts, in addition to using a Time-to-digital convertor with a bin size of 81 ps.

Keywords: single-photon detection, mean photon number, Poissonian statistics, time to digital conversion, weak coherent pulses.

1. Introduction

In classical cryptography, Alice and Bob, two distant parties, use a communication channel to communicate secretly in the presence of an unwanted third party Eve. The ultimate goal of secure communication is to guarantee that information is completely preserved from unauthorized access. Information security can be achieved theoretically by the one-time-pad (OTP) method if Alice and Bob communicate a long random string that is kept secret from Eve. It should be noted that avoiding using the same key again is crucial for the information security of the OTP method. This implies that the key may only be used once and must be the same length as the message [1].

The OTP is considered a very secure method, but it has major drawbacks that have prevented it from becoming widely used. The key distribution is the main problem. Since the security of the OTP depends only on the secrecy of the key, the key distribution method must be at least as secure as the OTP itself; there is no efficient classical method to fulfill this requirement [2].

Heisenberg's uncertainty and the quantum no-cloning principles have provided a completely new opportunity to facilitate the implementation of quantum cryptography. Using these physical properties in quantum mechanics enables the secure exchange of a random key, which can be employed alongside the OTP scheme to be as close to unconditional security as possible [2,3]. This discovery led Bennett and Brassard to develop the BB84 protocol for secure key exchange [4].

The first and most widely used QKD protocol is called BB84, after its inventors, Bennett and Brassard. This is a prepare-and-measure protocol where Bob measures the quantum states after being prepared by Alice for encoding. The implementation setup of the polarization-encoded BB84 is shown in Figure 1. The photons are prepared by Alice with polarization selected at random from the following four states: horizontal (H), vertical (V), diagonal (D), and anti-diagonal (AD). Bob receives the photons one at a time via a quantum channel, which can be free space or optical fiber. Bob randomly selects Z or X basis (where Z basis is for V and H polarization, and X basis is for D and AD polarization) to measure each photon's polarization state [5]. The steps of implementing the protocol are shown in Table (1)[6].

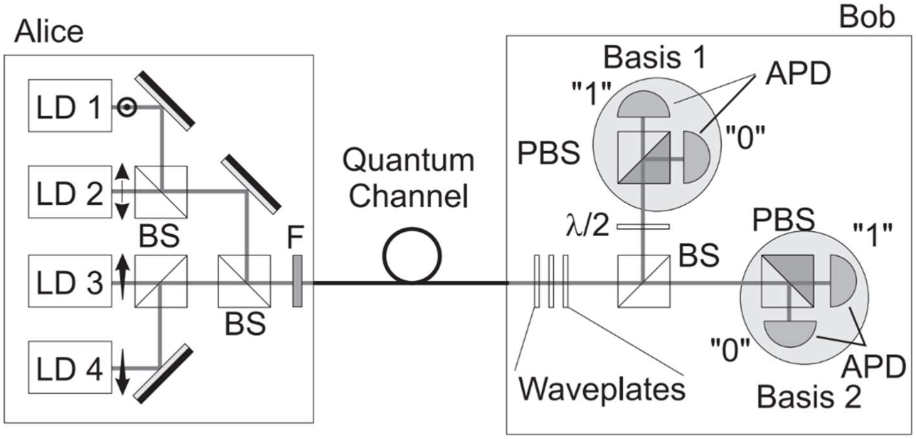


Fig. 1: Typical system for quantum cryptography using polarization coding (LD: laser diode, BS: beamsplitter, F: neutral density filter, PBS: polarizing beam splitter, λ/2: half waveplate, APD: avalanche photodiode) [5]

Table 1. BB84 protocol steps [6].

Alice's random bits	1	0	0	1	0	0	1	1	0
Alice's sending basis	R	D	R	D	D	D	D	D	R
Alice's photon polarization	↕	⤢	↔	⤡	⤢	⤢	⤡	⤡	↔
Bob's receiving basis	D	R	R	D	D	R	R	D	R
Bob's key bits	0		0		0	1	1	1	
Bob checks the bases with Alice			OK		OK			OK	
Bob and Alice check some keys OK bits randomly									
Sifted key			0					1	

To guarantee the security of QKD systems, they must be performed with single photon sources. These sources exhibit anti-bunching behavior and follow sub-Poissonian statistics. Thus, only a true single-photon source emits one photon at a time [7]. A perfect single-photon source generates single photons with 100% certainty, which means that there is a 0% probability of producing more than one photon or a vacuum state. Single atoms, ions, molecules, and solid-state emitters like quantum dots, color centers, carbon nanotubes, etc. These candidates have the potential to serve as sources for single photons. Despite the numerous efforts that have been made toward achieving a perfect single-photon source, it is still a difficult and challenging task [8]. These days, most QKD protocols utilize weak coherent pulses (WCPs) as an approximation to single photons. While these classical states are simple to produce, a fraction of them may contain two photons or more, which threatens the security of the key distribution process [9]. In brief, in the standard BB84 protocol, only signals that originate from single-photon pulses emitted by Alice are assured to be secure [10].

When attenuated laser pulses are employed as the source in the BB84 protocol. The vacuum components reduce the signal rate since there are no photons to be detected by Bob. The single photon components work perfectly, but the problem is in the presence of multiphoton components since each photon within the same pulse has the same polarization information. These multiphoton components make the protocol vulnerable to photon number splitting attacks, where Eve performs a photon number non-demolition measurement to determine Alice's multi-photon signals. Eve blocks part of Alice's single-photon signals so that Bob does not notice any change in the bit rate, steals one copy from multiphoton pulses, and sends the reminder to Bob over a lossless channel. After Alice and Bob reveal their basis during the sifting stage, Eve will have obtained complete knowledge about the key without being detected. However, decoy state protocols allow Alice and Bob to prevent the hypothetical PNS attacks [11,12].

In this paper, we present an acceptable estimation of the mean photon number achieved from the detected photons using the BB84 detection setup, which incorporates four single photon counting modules and a time-to-digital converter. Furthermore, we have successfully reduced the number of filters needed on the transmitter side to attain the necessary attenuation level for WCPs required in QKD systems.

2. Theory and concepts

Alice produces weak coherent pulses with a low mean photon number to approximate the single photon Fock-states. These pulses follow the Poisson statistics. The probability that one finds *n* photons in a coherent state is [13],

$$\mathrm{P(n,\mu)} = \frac{\mu^n}{n!} e^{-\mu} \tag{1}$$

where μ is the mean photon number.

In second-order approximation, we obtain,

$$\mathrm{P}(0) \approx 1 - \mu + \frac{\mu^2}{2} \tag{2}$$

$$\mathrm{P}(1) \approx \mu - \mu^2 \tag{3}$$

$$\mathrm{P}(2) \approx \frac{\mu^2}{2} \tag{4}$$

Accordingly, the probability that a non-empty pulse contains more than 1 photon becomes,

$$\mathrm{P}(n \geq 2 \mid n > 0) = \frac{1 - P(0) - P(1)}{1 - P(0)} \approx \frac{\mu}{2} + \left(\frac{\mu^2}{2}\right) \tag{5}$$

The mean photon number can be practically calculated as follows,

$$\mu = \frac{\mathrm{P_{avg}}}{\mathrm{P_{single}}}\ \alpha \tag{6}$$

P_{avg} can be represented as [14],

$$P_{avg} = N\ h\ v\ f \tag{7}$$

$$P_{single} = h\ v\ f \tag{8}$$

where
P_{avg} is the average power of the laser source.
P_{single} is the average power of a single photon.
α is the level of attenuation.
N is the number of photons per pulse.
h is Planck's constant (6.634 x 10^{-34} J.s).
v is the frequency of the emitted photon in Hz.
f is the pulse repetition rate in Hz.

The number of photons per pulse is defined as,

$$N = \frac{P_{avg}}{P_{single}} \tag{9}$$

The attenuation level required to have single-photon generation is determined by,

$$\alpha = \frac{1}{N} = \frac{P_{single}}{P_{avg}} \tag{10}$$

Weak coherent pulses can be realized by utilizing calibrated attenuators to attenuate the laser pulses. These pulses are used in many implementations of QKD systems since they are extremely practical. One problem with WCPs with a low mean photon number, i.e., when μ = 0.1, is that 5% of the non-empty pulses contain more than one photon[15]. Figure 2 shows the probability that a pulse of a coherent beam contains *n* photons for μ=0.1 [16].

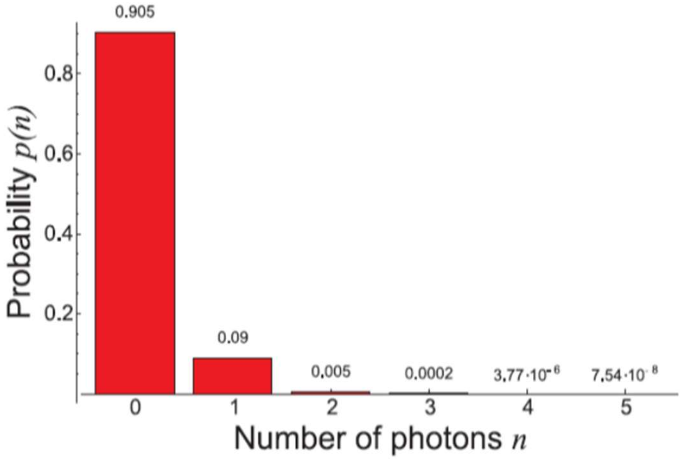


Fig. 2: Poisson distribution for $\mu = 0.1$ [16]

3. Experimental results and discussion

Two experiments were carried out to generate coherent pulses with a low value of μ. The first one is the traditional experiment that uses a laser source and optical filters. In the second experiment, a variable attenuator is implemented, and the time to digital converter (TDC) is used in determining the value of μ.

3.1. Generation of WCPs using optical filters and sheets of glass

Figure 3 illustrates the apparatus employed to produce WCPs using multiple filters and glass sheets. The laser source used in the setup is the nanosecond pulsed laser (NPL64B) from THORLABS. The operating wavelength is 640 nm, $P_{avg}\ of$ the laser source is 77 μW when it operated at f of 1 MHz with a pulse width(τ) of 5 ns. Neutral density filters (NDF) with a defined optical density (OD) were used. The OD determines the level of attenuation of the NDF applied to the laser pulses. The OD is defined as,

$$\text{OD} = log_{10}\left(\frac{1}{T}\right) \tag{11}$$

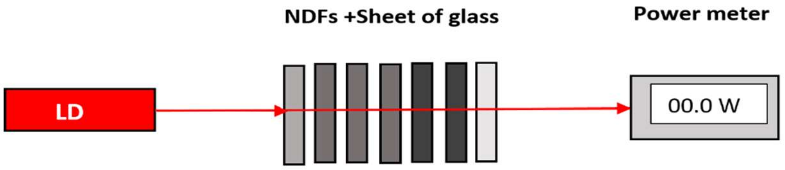


Fig. 3: setup for generating WCPs, LD: pulsed laser source, NDF: neutral density filter.

The specification of optical filters used in the experiment are listed in Table (2).

Table 2. Specifications of optical filters.

Filter type	OD	Transmittance (T)	No. of filters used
NE520B-A	2.0	0.01	2
NE13B-A	1.3	0.05	3
NE06B-A	0.6	0.25	1

The total transmittance (T) of these filters is determined as,

$$T= T_{NE520B-A} \times T_{NE520B-A} \times T_{NE13B-A} \times T_{NE13B-A} \times T_{NE13B-A} \times T_{NE06B-A}$$

In our experiment, two sheets of glass were used with a total transmittance of $\cong 0.155$. The attenuation obtained by these combination becomes, α= $0.01\times 0.01\times 0.05\times 0.05\times 0.05\times 0.25\times 0.155 = 4.843\times 10^{-10}$. Substituting the value of α in Eq. (6) will give a value of μ=0.12. To have 1 photon in every 10 optical pulses, i.e., μ =0.1, Eq. (10) is written as [17],

$$\alpha_{0.1} = \frac{0.1}{N}$$

$$P_{single} = h\,v\,f = 3.107\times 10^{-13}\ \mathrm{W}$$

$$N = \frac{77\times10^{-6}}{3.107\times10^{-13}} = 247827486$$

$$\alpha_{0.1} = \frac{0.1}{N} \quad = 4.035\times 10^{-10}$$

3.2 Estimating the value of the mean photon number from the WCPs detection

In this experiment, the QKD receiver based on the BB84 protocol, including the single photon counting modules and the TDC, is used to determine an acceptable estimation for the required value of μ. This method can be exploited in cases where the power meter is not capable of measuring the low-level attenuated light. Figure 4 illustrates the experimental setup for controlling the value of μ to generate WCPs. A combination of two NDFs (NE520B), a half-wave plate (AHWP05M-600), and a polarizing beam splitter (PBS121) was used as a setup functioning as a variable attenuator. This allows us to create WCPs with the desired mean photon number, denoted as μ_{des} .

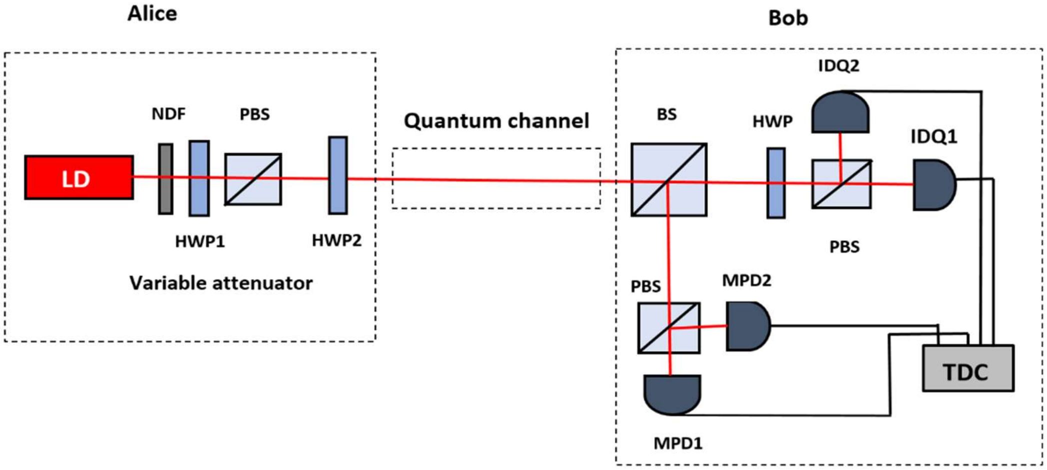
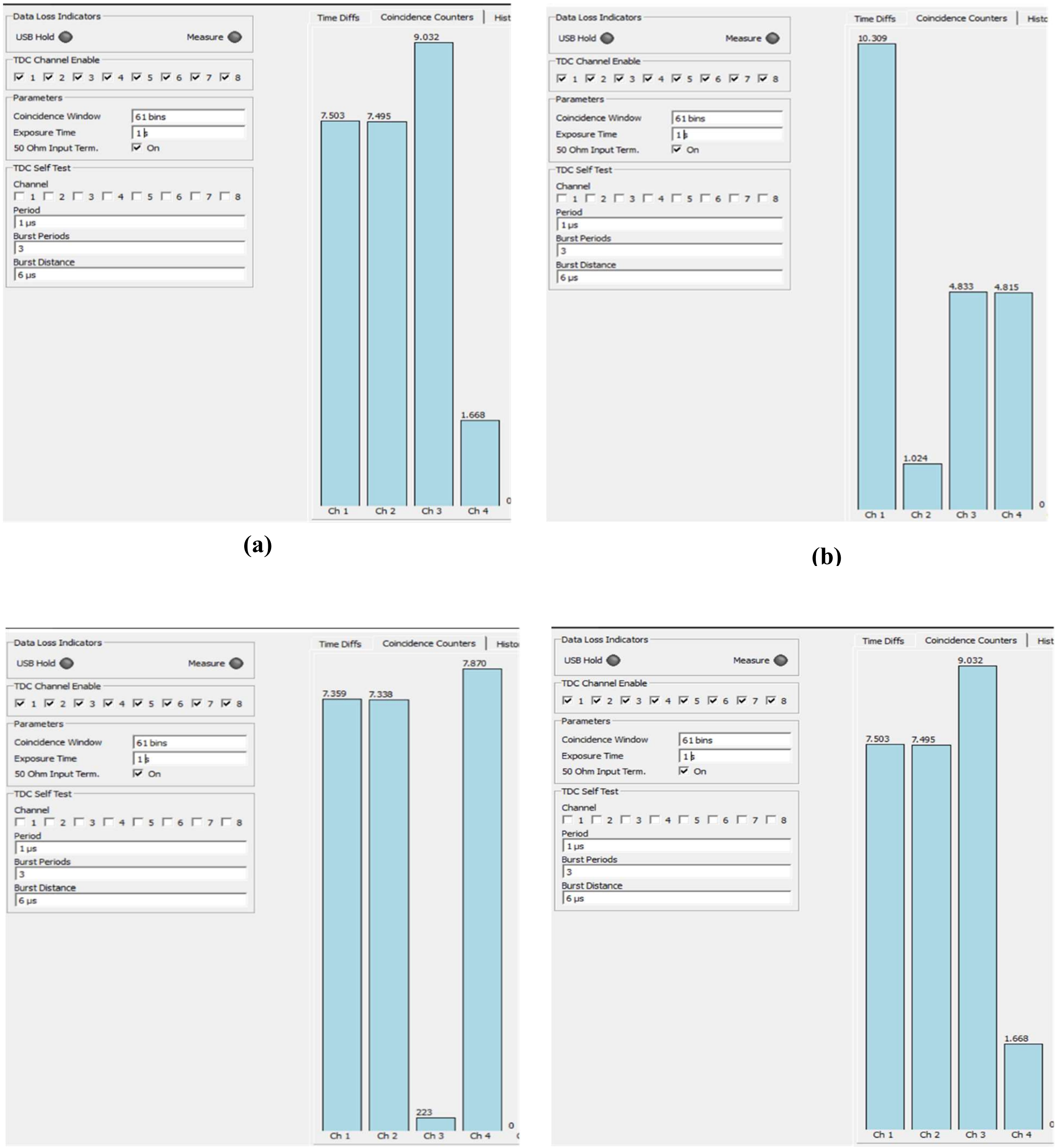


Fig. 4: setup for generating WCPs; LD: pulsed laser; NDF: neutral density filter; HWP: half-wave plate; PBS: polarizing beam splitter; BS: beam splitter; SPCM: single- photon counting module; TDC: time to digital converter

The rotation of the half-wave plate (HWP$_1$) provides a complete range of attenuation, i.e., allowing for the adjustment values of P_{avg} to be varied from maximum to minimum. Specifically, when the HWP$_1$ is set within the range of 0° to 45°, it is possible to achieve WCPs with lower values of the μ. These WCPs were then encoded with four different angles (0°, 22.5°, 45°, and 67.5°) for the BB84 protocol by using another half-wave plate (HWP$_2$) to represent bit values 1, 0, 0, and 1, respectively. The encoded photons were transmitted through the quantum channel to the BB84 detection setup. The BB84 detection setup, including four single-photon counting modules (SPCMs) series (ID100) with a dark count rate of less than 7 Hz and 40 ps timing resolution, and (MPD) with a dark count of one count per second and timing resolution of tenths of ps, were utilized to detect the WCPs. These SPCMs were connected to a four-channel (id800-

TDC, 8-Channel Time to Digital converter) with a bin size of 81ps for recording the number of detected photons for a detection time window of 5ns. Figure (5) illustrates the counts registered by the four SPCMs when HWP$_1$ was set at an angle of 33° which gives a low value of μ.



Data Loss Indicators
USB Hold ● Measure ●
TDC Channel Enable
☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8
Parameters
Coincidence Window 61 bins
Exposure Time 1 s
50 Ohm Input Term. ☑ On
TDC Self Test
Channel
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8
Period 1 µs
Burst Periods 3
Burst Distance 6 µs

(a)

Data Loss Indicators
USB Hold ● Measure ●
TDC Channel Enable
☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8
Parameters
Coincidence Window 61 bins
Exposure Time 1 s
50 Ohm Input Term. ☑ On
TDC Self Test
Channel
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8
Period 1 µs
Burst Periods 3
Burst Distance 6 µs

(b)

Data Loss Indicators
USB Hold ● Measure ●
TDC Channel Enable
☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8
Parameters
Coincidence Window 61 bins
Exposure Time 1 s
50 Ohm Input Term. ☑ On
TDC Self Test
Channel
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8
Period 1 µs
Burst Periods 3
Burst Distance 6 µs

(c)

Data Loss Indicators
USB Hold ● Measure ●
TDC Channel Enable
☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8
Parameters
Coincidence Window 61 bins
Exposure Time 1 s
50 Ohm Input Term. ☑ On
TDC Self Test
Channel
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8
Period 1 µs
Burst Periods 3
Burst Distance 6 µs

(d)

Fig. 5: The number of detected photons for HWP$_2$ angles of (a) 0, (b) 22.5, (c) 45 (d) 67.5, were: ch1 counts the photons detected by IDQ1, ch2 counts the photons detected by 1DQ2, ch3 counts the photons detected by MPD1, and ch4 counts the photons detected by MPD2.

μ_{des} can be estimated from the number of photons detected by four SPCMs [17]

$$N_{TDC} = \mu_{des} \cdot f \cdot \eta_d \tag{12}$$

Where
N_{TDC} is the number of detections per second measured by TDC.
η_d is detection efficiency for SPCM.

$$\mu_{des} = \frac{N_{TDC}}{f \times \eta_d} \tag{13}$$

The detection efficiency for each arm of the receiver setup can be calculated as,

$$\eta_{di} = \frac{\eta_c \times \eta_{b,i} \times \eta_{BOb}}{\eta_t} \tag{14}$$

Where
η_c is the quantum efficiency of the SPCM.
$\eta_{b,i}$ is the branching efficiencies, defined as the probability of a photon reaching a specific SPCM, where i= 1,2,3,4 for the four branches of the BB84 receiver.
η_{Bob} is the transmittance of Bob components.
η_t is channel transmissivity determined as, where $\eta_t = \frac{P_{received}}{P_{transmitted}}$

Table 3 shows the parameters used to calculate the detection efficiency.

Table 3 Experimental parameters used in the detection efficiency calculation.

Parameters		Value
Detector efficiency of (ID100)	η_{ID100}	36%
Detector efficiency of (MPD)	η_{MPD}	37%
Transmission of Polarizing beam splitter	T_{PBS121}	90%
Transmittance of Half Wave plate	$T_{\mathrm{AHWPO5M-600}}$	98%
Transmittance of Neutral density filter	$T_{\mathrm{NE13B-A}}$	5%
Branching efficiency	$\eta_{b,i,}$	50%
Channel transmissivity for a channel length of 1.5 m	η_t	96%

Where η_{di} is the detection efficiency for each arm of the BB84 receiver

$$\eta_{d1} = \frac{0.36\times0.5\times0.9\times0.98}{0.96} = 0.165$$

$$\eta_{d2} = \frac{0.36\times0.5\times0.9\times0.98}{0.96} = 0.165$$

$$\eta_{d3} = \frac{0.37\times0.5\times0.9}{0.96} = 0.173$$

$$\eta_{d4} = \frac{0.37\times0.5\times0.9}{0.96} = 0.173$$

From the above relationship η_d can be defined as,[17]

$$\eta_d = \frac{1}{4}\sum \eta_{di} \tag{15}$$

$$\eta_d = \frac{0.165+0.165+0.173+0.173}{4} \approx 0.17$$

By substituting the value η_d in equation (13) the value of μ_{des} can be obtained as listed in Table (4)

Table 4. values of mean photon number estimated from Eq. (13).

HWP 2	N_{ch1}	N_{ch2}	N_{ch3}	N_{ch4}	N_{total}	μ_{des}
0°	7503	7495	9032	1668	25698	0.15
22.5°	10309	1024	4833	4815	20981	0.12
45°	7359	7338	233	7870	22790	0.13
67.5°	1259	21158	4633	4587	31637	0.19

The fluctuation in the mean photon number with the variation of the HWP angle is attributed to several factors, such as imperfect optical components specifications and detection efficiency mismatch.

4. Conclusion

Based on the experimental results, it can be concluded that the mean photon number can be estimated with enhanced accuracy by considering the detector efficiency, branching efficiency, and transmission efficiency within the BB84 detection setup. Additionally, by employing a simplified configuration consisting of only two neutral density filters (NDF), a half-wave plate (HWP), and a polarizing beam splitter (PBS), our suggested configuration reduces the need for additional filters to optimize the target mean photon number. This approach facilitates more efficient and precise measurements in QKD systems as it employs SPCMs with low dark counts and high timing resolution and TDC with a time resolution reaching 81ps .

References

[1] F. Xu, X. Ma, Q. Zhang, H. K. Lo, and J. W. Pan, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys., vol. 92, no. 2, pp. 1–68 (2020).

[2] H. Weinfurter and A. Laubeeau, "Experimental Quantum Key Distribution," Diploma Thesis, University of Munich, Germany, 1998.

[3] R. Etengu, F. M. Abbou, H. Y. Wong, A. Abid, N. Nortiza, and A. Setharaman, "Performance comparison of BB84 and B92 satellite-based free space quantum optical communication systems in the presence of channel effects," J. Opt. Commun., vol. 32, no. 1, pp. 37–47 (2011)

[4] S. M. Salih and S. K. Tawfeeq, "Random signal generation and synchronization in lab-scale measurement device independent–quantum key distribution systems," J. Opt. Technol., vol. 86, no. 3, p. 137, (2019).

[5] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, and G. Ribordy, "Quantum cryptography," Appl. Phys. B Lasers Opt., vol. 67, no. 6, pp. 743–748, (1998)

[6] S. M. Salih, S. K. Tawfeeq, and A. I. Khaleel, "Generation of True Random TTL Signals for Quantum Key-Distribution Systems Based on True Random Binary Sequences," Iraqi J. Laser, vol. 18, no. 1, pp. 31–42 (2019).

[7] M. S. M. Leifgen, "Protocols and Components for Quantum Key Distribution Dissertation zur Erlangung des akademischen Grades doctor rerum naturalium im Fach Physik eingereicht an der Mathematisch-Naturwissenschaftlichen Fakult ̈ at der at zu Berlin von," (2016).

[8] A. Jain, P. V. Sakhiya, and R. K. Bahl, “Design and Development of Weak Coherent Pulse Source for Quantum Key Distribution System,” Proc. CONECCT 2020 - 6th IEEE Int. Conf. Electron. Comput. Commun. Technol., no. 2, pp. 0–4 (2020).

[9] R. Alléaume et al., “Experimental open-air quantum key distribution with a single-photon source,” New J. Phys., vol. 6, pp. 1–14 (2004).

[10] H. K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” Phys. Rev. Lett., vol. 94, no. 23, pp. 1–5 (2005).

[11] H.-K. Lo and N. Lütkenhaus, “Quantum Cryptography: from Theory to Practice,”(2007).

[12] J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt, “Enhancing practical security of quantum key distribution with a few decoy states,” vol. 87545(2005).

[13] S. Félix, N. Gisin, A. Stefanov, and H. Zbinden, “Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses,” J. Mod. Opt., vol. 48, no. 13, pp. 2009–2021, (2001).

[14] C. W. Park et al., “Single-photon counting in the 1550-nm wavelength region for quantum cryptography,” J. Korean Phys. Soc., vol. 49, no. 1, pp. 111–114 (2006).

[15] K. I. Hajim, S. K. Tawfiq, and A. M. Meki, “Quantum Cryptography and a Quantum Key Distribution Protocol,” vol. 3, pp. 1–10 (2004).

[16] F. A. Yassien, S. K. Tawfeeq, A. I. Khalil, and F. R. Aziz, “Generation of Weak Coherent Pulses for Quantum Cryptography Systems,” Iraqi J. Laser, Part A, vol. 9, no. 2, pp. 1–8 (2010).

[17] T. Sharma, A. Biswas, J. Ramakrishnan, P. Chandravanshi, and R. P. Singh, “Mitigating the source-side channel vulnerability by characterization of photon statistics,” pp. 1–8 (2023).

تحقيق تجريبي لتوليد نبضات ضعيفة متشاكهة بناء على كشف الفوتون المنفرد

حوراء عبد غانم ، شيلان خسرو توفيق

معهد الليزر للدراسات العليا، جامعة بغداد، بغداد،العراق

*البريد الالكتروني للباحث: hawraa.abd2201m@ilps.uobaghdad.edu.iq

الخلاصة: استلزم الطلب على مصادر الفوتون المنفرد في منظومات توزيع المفتاح الكمي QKD)) استخدام النبضات الضعيفة المتشاكهة والتي تتميز بتوزيع بواسون. يتطلب ضمان الأمن ضد هجمات التنصت الحفاظ على معدل لعدد فوتونات قليل ومعروف للشركاء الموثوقين. مع ذلك، فإن تحديد معدل عدد الفوتونات بدقة يواجه تحديات بسبب الاختلافات بين الحسابات النظرية والتنفيذ العملي.تقدم هذه المقالة تجربتين.تتضمن التجربة الاولى حسابات نظرية لحساب معدل عدد الفوتونات بأستخدام عدة مرشحات لتوليد النبضات الضعيفة المتشاكهة. أما التجربة الثانية، فاستخدمت مخففًا متغيرًا لتوليد نبضات ضعيفة متشاكهة، وتم تقدير قيمة μ من الفوتونات التي تم اكتشافها بواسطة نظام الكشفBB84. وتمثل التجربة الثانية طريقة دقيقة لتقدير قيمة μبسبب استخدام كواشف الفوتون المنفرد ذات دقة توقيت عالية وقيم منخفضة للعد المظلم , بالاضافة الى استخدام محول الزمن الى اشارة رقمية بتقسيم 81 ps.