Volume 16, Number 1, 2023. pp. 15-24

Jordan Journal of Physics

ARTICLE

An Investigation of the Impacts of Available Real Single-photon Sources on Quantum Communication Secure Length

Azadeh Ahmadian[a], **Sara Tofighi**[b] and **Rasoul Malekfar**[a]

[a] *Department of Physics, Faculty of Basic Sciences, Tarbiat Modares University, Tehran, P.O. Box 14115-175, I.R. Iran.*
[b] *Department of Communication Technology, Iran Telecommunication Research Center, Tehran, I.R. Iran.*

Doi: **https://doi.org/10.47011/16.1.2**
Received on: 17/01/2021; *Accepted on: 25/07/2021*

Abstract: One of the most significant applications of single-photon sources is secure quantum communication. In this research, the security of the most famous protocol of quantum key distribution (BB84) has been studied by considering the characteristics of a single-photon source. This paper derives the impact of propagation on photon statistics. The result reveals that the propagation leads to a change in its value, especially in long distances. Besides, the parameter deviation from an ideal source causes a decrease in the confident length. We achieved a difference of up to 1800 km for the safe distance by studying the relation for minimum transmission coefficient in available single-photon sources.

Keywords: Quantum communication, Quantum key distribution, Security, Single-photon source.

1. Introduction

Quantum communication, which uses the laws of quantum mechanics, can guarantee the security of information [1] against the threat of quantum computers. Quantum communication has several branches and schemes, e.g. quantum key distribution (QKD), which is the most developed and widely studied. QKD distributes a shared random secret key between two users to encrypt and decrypt messages and implement a cryptographic protocol involving components of quantum mechanics [2-5]. Another branch is quantum secure direct communication (QSDC), which sends secret information directly through a quantum channel with provable security without setting up a key at the initial stage [6-8]. These branches can be divided into two main categories, depending on the type of quantum sources they are using: single-photon (SP) sources or entangled photon sources.

In the case of QKD and the absence of channel noise, every SP-based QKD protocol has an entanglement-based counterpart and can be implemented with the same level of security. However, under empirical conditions, the employment of SP-based QKD protocols is more accessible due to the fragility of entanglement against de-coherence, amplitude damping, phase damping and squeezed generalized amplitude damping noises [9].

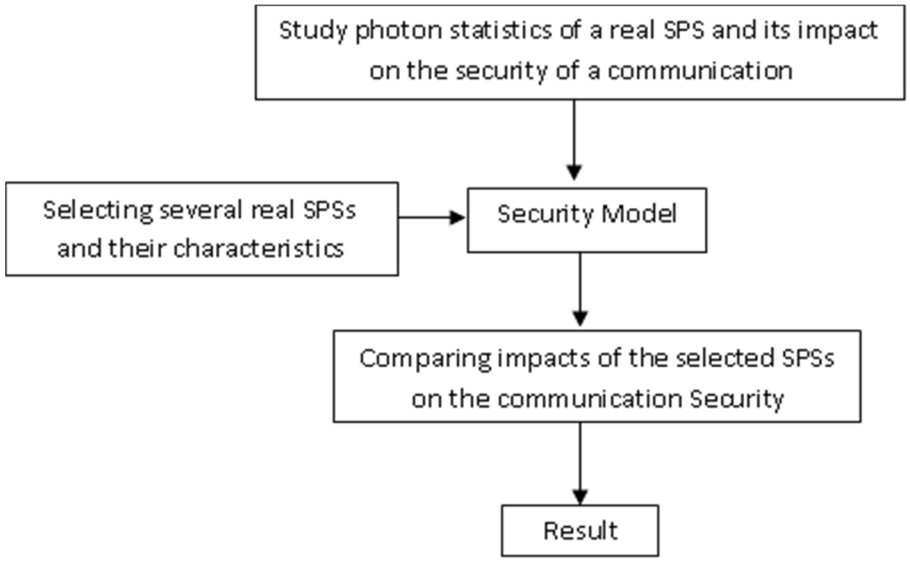
An ideal SP source (SPS) is a device that emits only an SP at any arbitrary time considering users' demands. Due to the explosive growth of quantum communications in recent years, SPS has been studied extensively as an element for transmitting quantum information through the quantum network. However, these sources are not limited to QKD protocols, such

Corresponding Author: Rasoul Malekfar **Email**: malekfar@modares.ac.ir

as BB84, COW, SARG04, E91 and B92, and are widely used in quantum communication, quantum computing and quantum state amplification [10-12].

In this research, focusing on BB84 as a QKD protocol, the impact of real SPSs on security has been studied. QKD protocols have unconditional security if ideal devices, such as ideal SPS, SP detector (SPD) as well as the noiseless and lossless channel, are incorporated. Therefore, one of the main challenges of these protocols is non-ideal devices and some papers are modeling the impact of real SPS on security [13-16] and other real devices in quantum communication [17-25]. However, up to now, the effect of propagation on the security of the BB84 protocol, which is the most famous protocol of QKD and is the primary point of this research, has not been studied.

To achieve this goal, in Section 2, the emitted photons are being considered propagating in the fiber, and the photon statistics and the security model modification have been studied. Section 3 deals with the simulation results and comparison of the effect of using different types of SPS on the security of the BB84 protocol. In this section, we focus on the available SPSs and examine the effect of their deviating from ideal sources on the security of this protocol. The employing model for different types of SPSs is the same and experimental values are used to achieve the result. Section 4 of the paper presents the results of the study. The flow chart for the steps of this research is as follow:



2. Second Coherence Function after Going through the Path

It is proved that the second coherence function $g^{(2)}$is described as [26-30]:

$$g^{(2)} = \frac{\langle a^\dagger a^\dagger a a \rangle}{\langle a^\dagger a \rangle^2} \quad (1)$$

where $a_k^\dagger$ and a_k are creator and annihilator operators of electromagnetic fields, respectively.

This relation reveals that location and time parameters do not exist in $g^{(2)}$ relation and it gives information about the emitted photon state (for number state $g^{(2)}$<1, for coherent state $g^{(2)}$=1 and for thermal state $g^{(2)}$>1), but this formula is acquired in $r = 0$ and its average is based on the state $|\psi(x,t)\rangle = |\psi(0,0)\rangle$.

The question arises as to whether the second coherence function persists after propagating. As we know, a wave packet disperses along the path and this dispersion is related to the probability density change. For achieving $g^{(2)}$ in another location, the average should be calculated based on $|\psi(x,t)\rangle$, ($|\psi(0,0)\rangle$ is the wave function in the zero time and location). Therefore, the relation will be modified after the path,

$$g_l^2(0) = \frac{\langle \psi(x,0)|a^\dagger a^\dagger a a|\psi(x,0)\rangle}{\langle \psi(x,0)|a^\dagger a|\psi(x,0)\rangle^2} = \frac{\langle \psi(0,0)|\hat{n}(\hat{n}-1)|\psi(0,0)\rangle}{|\langle \psi(0,0)|\hat{n}|\psi(0,0)\rangle|^2} \frac{\sqrt{1+4t^2}}{(\sqrt{1+4t^2})^2} = \frac{\langle \hat{n}(\hat{n}-1)\rangle}{\bar{n}^2}\sqrt{1+4l^2/c^2}$$

$$g_l^2(0) = g^{(2)}(0,0)\sqrt{1+4l^2/c^2} \quad (2)$$

where l is the distance length and c is the speed of light.

The relation can limit the transmission coefficient: $T \geq \frac{1}{1-4\mu}\left(\frac{d}{\bar{n}} + \frac{\bar{n}g^{(2)}}{2}\right)$ [31] (see supplementary). After substituting Eq. (2) in this lower band, the result is:

$$T \geq \frac{1}{1-4\mu}\left(\frac{d}{\bar{n}} + \frac{\bar{n}g^{(2)}\sqrt{1+\frac{4l^2}{c^2}}}{2}\right) \quad (3)$$

$\bar{n}$ is the photon-number average, d is the dark count rate and μ is a baseline signal error rate which contains imperfect-state preparation, channel decoherence and imperfect-polarization optics.

We can define the channel loss according to ingoing (E_{in}) and outgoing (E_{out}) electromagnetic fields:

$\text{Loss} = -10\log\left(\frac{E_{out}}{E_{in}}\right)$.

Also, E_{out} can be described by E_{in} and the transmission coefficient:

$E_{in} \times \text{T} = E_{out}, \text{T} = \frac{E_{out}}{E_{in}}$

where $\text{length} \times \text{Loss} = 10\log(\text{T})$, $\text{length} = \frac{10\log(\text{T})}{\text{Loss}}$.

By using the above relations, the minimum value for the transmission coefficient is:

$$\text{T}_{\min} = \frac{1}{1-4\mu}\left(\frac{d}{\bar{n}} + \frac{\bar{n}g^{(2)}}{2}\sqrt{1+4[10\,(\log(\text{T}))/(\text{C.Loss})]^2}\right). \quad (4)$$

Eq. (4) shows that because of the light speed C, the second term in the square root is negligible but for high loss, which is usually in long distances. This means that the wave packet dispersion should be considered in the $g^{(2)}$and $\text{T}_{\min}$values over long distances.

3. The Impact of Existing Single-photon Sources on the Secure Length

As we described in the previous section, it has been shown that $T > \frac{1}{1-4\mu}\left(\frac{d}{\bar{n}} + \frac{\bar{n}g^{(2)}}{2}\right)$ [31]. We can conclude that if there is an ideal SPS, in which $\bar{n} = 1$ and $g^2(0) = 0$, the secure condition is $\text{T} > \frac{\text{d}}{1-4\mu}$. However, we skip discussing the ideal SPS, because a real one is our concern.

The effect of some real SPS on the security of the protocol can be compared. For investigating the behavior of T, the main applied assumptions are $\bar{n} = 1$ and $d=10^{-5}$ for the dark count value, 2% for μ (acceptable value for proper protocols) and different values for $g^2(0)$, [32-33].

The function $g^{(2)}$ for a real SPS is not zero. Therefore, it is also possible to consider it as a source emitting two-photon or three-photon states. For this system, the probability of the presence of a multi-photon state is very low (less than 0.1) and with a good approximation, it is assumed that the maximum multi-photon state is limited to two-photon state.

By this discussion and using Eq. (4), the impact of different SPSs and the results for the related transmission coefficients are compared in Table 1. The $g^{(2)}$ is described by the following relation:

$$g^{(2)} = \frac{\sum_{n=0}^{\infty} n(n-1)p_n}{\left(\sum_{n=0}^{\infty} np_n\right)^2} = \frac{\sum_{n=0}^{\infty} n(n-1)p_n}{\bar{n}^2}.$$

While the photon-state distribution p_n is different for each source, the function $g^{(2)}$ for all the compared sources comes from the experimental value [35-37]. For example, a distribution of weak coherent source is $p_n = e^{-\alpha^2}\frac{\alpha^{2n}}{n!}$. Moreover, for a heralded SPS, it is: $p_n = [1-(1-d)(1-\eta)^n]e^{-\alpha^2}\frac{\alpha^{2n}}{n!}$, where η is the detection efficiency, d is the dark count rate and $\alpha = \sqrt{\frac{\pi}{2}}\Omega_0^2\,\tau/\kappa$ (Ω_0 is the Rabi frequency for the creation photons, τ is the pulse width and κ is the photon-photon interaction of the system creating photons) [36].

TABLE 1: The impact of different real SPSs on the value of transmission coefficients and secure length.

Source	$g_0^2(0)$	Wavelength (nm)	$T_{min}\times 10^2$	Secure length (km)
Laser ($\bar{n} = 0.1$)	1	1550	0.49	100
Single Molecule	0.09	500-750	0.015	340
QD (InGaAs)	0.15	932 nm	0.019	270
Ensemble (Rb, Cs)	0.25	Atomic line	0.24	210
NV diamond (bulk)	0.07	640-800	0.13	390
NV diamond (nano)	0.09	640-800	0.15	340
PDC (multiplexed)	0.08	Vis-IR	0.14	360
FWM (PCF)	0.01	Vis-IR	0.05	1000
Carbon nanotube	0.01	640-800	0.05	1000
Photon blockade	0.029	Vis-IR	0.083	600
QD	0.0028	932 nm	0.026	1900

Comparing the above values reveals that the minimum amount of T for ensemble (Rb, Cs) is higher than for the other SPSs (laser is not considered as an SPS). It can be concluded that employing this source should be accompanied by applying a better channel (with a lower loss) or operating at a shorter distance. The three last rows of Table 1 are newly presented sources, which are employed as optimal SPSs [35, 37] or as a scheme for increasing the key rate of QKD, such as SP blockade [36]. An SP blockade is defined as an SP that can impede the transmission of other photons, allowing a strong interaction between SPs. There are papers about this phenomenon and the relation of the probability of the emitted states and calculating its $g^2(0)$, but its T_{min} has been estimated in Table 1.

Another result is about the secure length which is written in the last column. In Table 1, the secure length can be defined as the length in which 50% of information transfers. By this definition, the secure length = $(50\%)/T_{min}$, where 50% is applied, because it is supposed to compare with 3 dB/km loss in many traditional channels. It should be considered that in a real operational test, the channel loss depends on the frequency of the source and the multi-mode or single-mode attribute of the channel. By comparing Table 1 contents, it is derived that three sources (four-wave mixing (FWM), carbon nanotube and a kind of QD) can be used for longer distances. The above values for secure length reveal the results comparatively. In addition to the above sources, other exotic schemes have been proposed recently, such as SPS based on Rydberg exciton blockade [38] or laser-corrected sub-natural-linewidth SPS [39], which can be investigated for developing quantum communication. If a method can increase this length for a particular source and can be employed for another source, probably the secure length can increase proportionally for the latter source. For example, preparing decoy-state protocol (DSP) of the weak coherent pulse (WCP) of a laser is very acceptable in operating QKD [21], in this respect employing it for other sources to boost the result [36].

Investigating the behavior of T can be informative. Therefore, three kinds of different sources have been studied. For this purpose, the above assumption ($\bar{n} = 1, \mu = 2\%, d = 10^{-5}$) and three values for $g^2(0)$: 0 (for the ideal SPS), 1 (for a weak laser) and 0.09 (for a real SPS) are considered, where the results are shown in Fig. 1. To recognize the difference between results, the figure is plotted on a logarithmic scale. It reveals that if a laser is chosen as a source in quantum communication, the channel should be more appropriate (with higher magnitude values for the transmission coefficient). Since there are no significant differences between the WCP and real SPSs in usual channels (in comparison with the ideal and real SPS), as a good approximation, the actual existing WCP can be employed without security concerns in short distances. This result is the reason why the WCP of the laser is very popular in QKD operation.

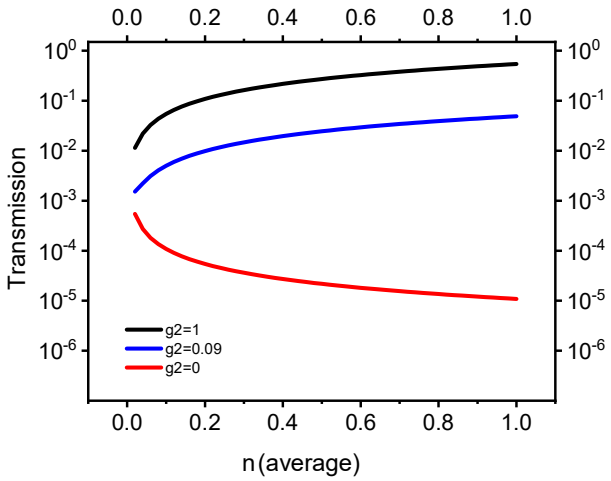


FIG. 1. The logarithm of transmission coefficient *versus* the average number of photons from three different sources. The curves: black for a weak laser, red for an ideal SPS and blue for a real photon source.

Another investigation can be considered for the minimum value of T relative to $\bar{n}$; we have:

$$T_{min} = \frac{\sqrt{2dg^{(2)}}}{1-4\mu} \quad . \tag{5}$$

By defining $\bar{n} = \bar{n}_c$; in which:

$$\bar{n}_c = \sqrt{\frac{2d}{g^{(2)}}} \, . \tag{6}$$

According to relation (3), there is a case in which the average number of the photons is 1 and the value of the transmission coefficient is minimum. This situation leads to $g^2 = 2d$. In this case, if the g^2 value is equal to 2×10^{-5}, the dark count is 10^{-5} and the error value is 2%, then the necessary value for the channel transmission is 1.9×10^{-5}, but as we know, this source is not yet introduced and the minimum condition is not satisfied. This means that the channel has to be changed for preparing the minimum-security situation.

The curve for the minimum-transmission value of the channel against g^2 has been plotted and is presented in Fig. 2. The slope of the graph provides some information about choosing an SPS.

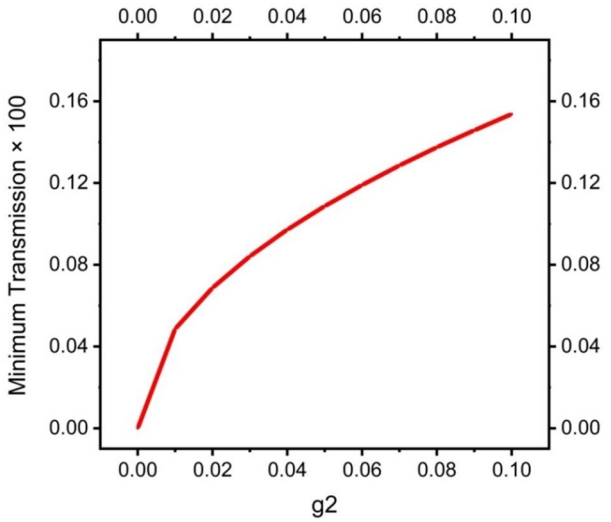


Fig. 2. The curve of minimum transmission of the channel *versus* the second coherence function. The range of the second coherence function is selected according to the value of the several different SPSs, based on QD and carbon lattices, such as nitrogen-vacancy centers in diamond and carbon nanotubes.

Fig. 2 shows that the difference of the minimum-transmission coefficient of the channel is in the order of 10^{-4}; therefore, based on the proposed SPS, the most appropriate channel can be chosen. Otherwise, if it is not possible to change the channel, the source can be altered for preparing the security conditions for reliable communication.

4. Declarations

Not applicable.

5. Conclusions

In this paper, quantum communication is considered consisting of a source, a relevant channel and a detector. Also, the impacts of the critical factors and the dispersion effect are modeled. The outcome presents the dispersion effects on the SP level of the source in long distances. The source of the emitted photons is supposed to be one of the real SPSs that are employed in various types of experiments. The range of the secure length for different kinds of the available SPSs can change approximately up to 1800 km. Since the value for the second coherence function of the existing real SPSs varies from 0.0028 to 1, considering the distance is another concern in selecting the SPSs and protecting the security of communication. Employing the results of this research can help in finding appropriate SPSs.

6. Supplementary

1. Characteristics of Single-photon Sources

Whereas photons are nothing except an electromagnetic field, their quantum identity as single photons can be investigated by considering the electromagnetic field regarding quantum mechanical operators. As demonstrated in many educational books [20-24], it is supposed that the energy of electromagnetic field is confined in an environment such that cavity and its vector potential expand according to the discrete set of orthogonal mode functions. Therefore, it is quantized that:

$$A^{+}(r,t) = \sum_k C_k\, U_k(r)\, e^{-i\omega_k t} \qquad \text{(S1)}$$

where A is the vector potential as a function of location (r) and time (t), U_k represents the vector mode functions and ω_k is the mode frequency.

All these vector mode functions will satisfy the wave equation, and after solving the equation, it is found that:

$$A(r,t) = \sum_k \left(\frac{\hbar}{2\omega_k \varepsilon_0}\right)^{1/2} [\, a_k u_k(r) e^{-i\omega_k t} + a_k^{\dagger} U_k^{*}(r) e^{i\omega_k t}] \qquad \text{(S2)}$$

where $a_k^{\dagger}$ and a_k are creator and annihilator operation and $[a_k^{\dagger}, a_k] = 1$; moreover, the corresponding field is:

$$E(r,t) = i \sum_k \left(\frac{\hbar}{2\omega_k \varepsilon_0}\right)^{1/2} [\, a_k U_k(r) e^{-i\omega_k t} - a_k^{\dagger} U_k^{*}(r) e^{i\omega_k t}]. \qquad \text{(S3)}$$

The above equation reveals that the electrical field is quantized as harmonic oscillators; i.e., we can interpret an electromagnetic-field state as a harmonic oscillator state:

$$|\psi\rangle = |n_k\rangle = \frac{(a_k^{\dagger})^{n_k}}{(n_k!)^{1/2}} |0_k\rangle \; n_k = 0, 1, 2, \ldots \qquad \text{(S4)}$$

in which the quantization of the photon is as the quanta of the electromagnetic field.

By considering n = 1 in Eq. (S4), the photon state is the state of the single photon and it means that the number of photons in that mode is one. In other words, there is just one photon in a special time and space, while the other photons certainly exist in another time or another space and there is no correlation between them. The mathematical interpretation of correlation function related to the number of photons, which is known as the second coherence function, is:

$$g^{(2)} = \frac{\langle E^{-}(r_1,t_1) E^{-}(r_2,t_2) E^{+}(r_2,t_2) E^{+}(r_1,t_1)\rangle}{\langle E^{-}(r_1,t_1) E^{+}(r_1,t_1)\rangle \langle E^{-}(r_2,t_2) E^{+}(r_2,t_2)\rangle} \qquad \text{(S5)}$$

supposing that photons at different times are at the same place and employing Eqs. (S3) and (S5), the correlation function will be calculated as follows:

$$g^{(2)} = \frac{\langle E^{-}(t) E^{-}(\tau+t) E^{+}(\tau+t) E^{+}(t)\rangle}{\langle E^{-}(t) E^{+}(t)\rangle \langle E^{-}(\tau+t) E^{+}(\tau+t)\rangle} = \frac{\langle a^{\dagger} a^{\dagger} a a\rangle}{\langle a^{\dagger} a\rangle^2} = \frac{\langle \hat{n}(\hat{n}-1)\rangle}{\bar{n}^2}. \qquad \text{(S6)}$$

In a single-photon state (n=1), Eq. (S6) corresponds to $g^{(2)} = 0$ and it confirms no correlation for single-photon state. It can be described that the memory of the first detected photon is lost even in zero time and no information is transferred between succeeding photons.

All of the above descriptions were supposed under ideal conditions. However, it is acceptable that ideal devices and conditions are not introduced until now and there is no way except modeling them. One of the ideal conditions is that the modes are considered in a huge large-size cavity, which is not a good assumption, while another one is the lack of ideal single-photon sources. The first one corresponds to single photons as wave packets and the second means that there is always a possibility to exit two or more photons from a source at the same time. In other words, photons are in the state

number $|2\rangle$ or higher. By concentrating the real single-photon source, we can find that the correlation between the number of photons is not zero. In general, the second coherence function for a real single-mode source, which is in the state of $|\psi\rangle = \sum_{i=0}^{\infty} \sqrt{p(i)}\,|i\rangle$, can be demonstrated as [25]:

$$g^{(2)} = \frac{\langle \hat{n}(\hat{n}-1)\rangle}{\bar{n}^2} = \frac{\sum_{i=0}^{\infty} p(i)i(i-1)}{\bar{n}^2}$$

$$g^{(2)} = \frac{\sum_{i=2}^{\infty} p(i)i(i-1)}{\bar{n}^2}\,. \qquad \text{(S7)}$$

Comparing $g^{(2)}$ of the existing real single-mode sources can be very informative. In this respect, some important kinds of single-photon sources are selected. These kinds are some non-linear optical crystals (such as $LiNbO_3$, KDP, BBO, …,), some isolated systems, such as single molecules, color centers, quantum dots, single ion and single atom in a cavity and ensemble systems, such as Rubidium (Rb) and Cesium (Cs). The second coherence function of a parametric down-conversion (PDC), which is a non-linear optical crystal, can be between 0.0014 and 0.08; its value for a color center as an isolated system is 0.07 and for an ensemble of Rb atoms is 0.2 [26]. All these values represent that no existing single-photon source is an ideal one $g^{(2)} = 0$.

2. BB84 Protocol

Since the primary goal of this paper is dedicated to investigating the impact of the properties of single-photon sources on the security of quantum communication, it is worthy to review the first QKD protocol, BB84, to understand the role and importance of an ideal single-photon source to the security of this protocol. In BB84 protocol, which is developed by Charles Bennett and Gilles Brassard in 1984, there is a sender (Alice) who aims to exchange a random bit string as a key with a receiver (Bob) in a secure manner. An eavesdropper (Eve) tries to attack their communication and obtain any information.

To make secure communication, Alice utilizes the superposition principle to encode the information and Bob employs quantum measurement for decoding. The basic steps of the BB84 protocol are as follows:

1- Alice and Bob agree to attribute the bit value 0 to the quantum states $|0\rangle$, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and the bit value 1 to the quantum states $|1\rangle, |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

2- Alice generates a truly random bit string using a quantum random number generator.

3- Alice encodes each bit of her generated string randomly on either standard basis $\{|0\rangle, |1\rangle\}$ or Hadamard basis $\{|+\rangle, |-\rangle\}$ and sends the prepared qubits to Bob.

4- Bob selects randomly one of two bases and measures the received qubits. So, the probability that Bob chooses the correct basis for measurement is 50%. If Bob measures the received qubit on an accurate basis, he will obtain the same bit value that Alice sent. However, if Bob chooses a wrong basis, he gets a correct value with a 50% chance.

5- Alice and Bob announce their basis *via* a public classical channel and both of them discard the results for which Bob used a different basis.

In the above description, the presence of an eavesdropper is ignored. Eve can employ several strategies to attack the QKD protocols. However, the laws of quantum mechanics ensure that Eve cannot get any information without leaving a signature of her activity. One of the most well-known attacks on QKD protocols is the intercept & resend attack. In this attack, Eve employs the same strategy as Bob to obtain the information. She measures the qubits and according to the result of measurement, re-prepares a qubit to send to Bob. With a probability of 50%, Eve's choice of basis does not coincide to that of Alice. So, she re-prepares a wrong state and sends it to Bob. Bob measures this wrongly prepared state on the same basis as Alice with the probability of 50%. Therefore, in the presence of Eve, after checking the bases by Alice and Bob (step 5), around 25% of outcomes are erroneous [27] and the error lower than 25% =1/4 reveals secure communication.

Photon-number splitting is another common attack which is related to lack of ideal single-photon source. Realistic single-photon sources have a probability distribution in their photon number (n). In other words, the probability of having $n = 0$ and $n \geq 2$ photons in the output of non-ideal single-photon source is non-zero. Eve can exploit this imperfection, keeping one of the photons and sending the rest to Bob. With this strategy, Eve can obtain information without introducing any additional error and being

detected by Bob, provided that the probability of the multi-photon state is less than the probability of the photon detection. In other words, Bob concludes that reducing the number of photons is related to detection issues, such as channel loss or detector limitations. So, for secure communication, the probability of detection should be more than the probability of multi-photon state: P_{detect}>P(m).

3. Estimating the Security of the BB84 Protocol

For investigating the security of quantum communication protocols, effective components including sources, channels (optical fiber or free space for photon propagation) and detectors should be considered. In the beginning, a source model is considered [25] and its impacts on the security parameters will be estimated. According to this assumption, Eq. (S7) for this source leads to the following relation (by the assumption that the probability of sending the multi-photon state is limited to two-photon state):

$$g^{(2)} = \frac{2p(2)}{\bar{n}^2} \quad , \quad \frac{g^{(2)}\bar{n}^2}{2} = p(2) \, . \tag{S8}$$

Eq. (S8) shows that the probability of emitting a two-photon state can be calculated as a function of the second-order coherence.

Photons of the source are emitted by the probability p(n), cross-over the channel and are received by a detector, while the total absorption and transmission coefficients of the channel and the detector are L and T, respectively. If p(1) is the probability of emitting one photon and L is the absorption coefficient, then the probability of photon loss is p(1) × L and the probability of receiving the signal is p(1) - p(1) × L. In the same way, If p(2) is the probability of emitting 2 photons, the probability of photon loss is p(2) × L^2 and the probability of receiving the signal is p(2) -p(2) × L^2. If $P_{n\,signal}$ is the probability of receiving the signal n, then:

$$p(0) - p(0).L^0 = p_{0\,signal}$$
$$p(1) - p(0).L^1 = p_{1\,signal}$$
$$p(2) - p(2).L^2 = p_{2\,signal}$$
$$p(n) - p(n)L^n = p(n)(1 - L^n) = P_{n\,signal}$$
$$P_{signal} = P_{0\,signal} + P_{1\,signal} + P_{2\,signal} + \cdots$$
$$P_{signal} = p(0) - p(0) \times L^0 + p(1) - p(1) \times L^1 + p(2) - p(2) \times L^2 + \cdots + p(n)(1 - L^n) \tag{S9}$$

The following probability function can interpret this formula:

$$P_{signal} = \sum_{n=0}^{\infty} p(n)(1 - (1 - T)^n) \tag{S10}$$

where T is the transmission coefficient and $T + L = 1$.

By supposing that the receiving probability of the multi-photon state signals (n>1) is small, the following relation can be achieved:

$$P_{signal} = \bar{n}T \, . \tag{S11}$$

The above relation is the result of modeling for receiving the signal. The next step in this article is to study a model for the detector and investigate its parameter impacts on the whole process of sending and receiving the signals. While detectors receive dark count in addition to the signal, the probability of signal detection is as follows:

$$P_{detect} = P_{signal} + d = \bar{n}T + d \tag{S12}$$

where d is the reference or dark-count detection limit.

Some imperfections between the sending and receiving systems produce errors in the receiving system, e.g. the total signal cannot enter to a real detector and this is one kind of detector imperfections. In this case, we suppose a coefficient of the signal, μ, which is detected wrongly. Also, there is always a probability of dark-count detection and because it is accidental, its probability is ½. Generally, the probability of the signal error is different from that of the noise error and they can be considered separately. By this clarification, the error rate, which is defined as the ratio of the error detection probability to the total detection probability, will be shown as:

$$e = \frac{P_{error\ detection}}{P_{detect}} = \frac{\mu P_{signal} + d/2}{P_{detect}} \tag{S13}$$

where e is the error in detection.

The protocol will be secure against the two QKD attacks (I&R and PNS) if the two conditions (P_{detect}>P(m) and e>1/4) combine. By using Eqs. (S8) to (S13), it can be shown that the probability of the total transmission should follow the relation [25]:

$$e = \frac{P_{error\ detection}}{P_{detect}} < 1/4$$

$$P_{detect} > 4.P_{error\ detection} \rightarrow P_{detect} > 4\left(\mu P_{signal} + \frac{d}{2}\right) \rightarrow P_{detect} > 4\mu P_{signal} + 2d$$

$$P_{detect} > p(2) \rightarrow P_{detect} > \frac{g^{(2)}\bar{n}^2}{2}. \quad \text{(S14)}$$

By considering that all values are positive, combining two inequalities and employing Eqs. (S11) and (S12), the following relation, which is correct for real sources, can be attained:

$$P_{detect} > 4\mu P_{signal} + 2\mathrm{d} + \frac{g^{(2)}\bar{n}^2}{2} \rightarrow \mathrm{nT} + \mathrm{d} > 4\mu(\mathrm{nT}) + 2\mathrm{d} + \frac{g^{(2)}\bar{n}^2}{2}$$

$$(1-4\mu)\mathrm{nT} > d + \frac{g^{(2)}\bar{n}^2}{2}$$

$$T > \frac{1}{1-4\mu}\left(\frac{d}{\bar{n}} + \frac{\bar{n}g^{(2)}}{2}\right). \quad \text{(S15)}$$

References

[1] Bennett, C.H. and Brassard, G., Systems and Signal Processing, 175 (1984) 8.

[2] Jia, Q., Xue, K., Li, Z., Zheng, M., Wei, D.S.L. and Yu, N., Quantum Information Processing, 20 (2021) 69.

[3] Su, H.Y., Quantum Information Processing, 19 (6) (2020) 1.

[4] Basset, F.B, Valeri, M., Roccia, E., Muredda, V., Poderini, D., Neuwirth, J., Spagnolo, N., Rota, M.B., Carvacho, G., Sciarrino, F. and Trotta, R., Science Advances, 7 (2021) 12.

[5] Wang, L.J., Zhang, K.Y., Wang, J.Y., Cheng, J., Yang, Y.H., Tang, S.B., Yan, D., Tang, Y.L., Liu, Z., Yu, Y., Zhang, Q. and Pan, J.W., Quantum Information, 7 (2021) 67.

[6] Pan, D., Lin, Z., Wu, J., Zhang, H., Sun, Z., Ruan, D., Yin, L. and Long, G.L., Photonics Research, 8 (9) (2020) 1522.

[7] Hu, J.Y. et al., Light Sci. Appl., 5 (2016) e16144.

[8] Qi, R.Y. et al., Light. Sci. Appl., 8 (2019) 22.

[9] Sharma, V., Thapliyal, K., Pathak, A. and Banerjee, S.A., Quantum Information Processing, 15 (11) (2016) 4681.

[10] Sheng, Y.B. and Zhou, L., Phys. Rev. A, 98 (2018) 052343.

[11] Xiang, Y., Wang, Y., Ruan, X., Zua, Z. and Guo, Y., Physica Scripta, 96 (2021) 6.

[12] Zhou, L. and Sheng, Y.B., Laser Phys. Lett., 12 (2015) 045203.

[13] Trushechkin, A.S., Kiktenko, E.O., Kronberg, D.A. and Fedorov, A.V., Physics-Uspekhi, 64 (2021) 1.

[14] Zhao, L.Y, Wu, Q.J., Qiu, H.K., Qian, J.L. and Han, Z.F., Phys. Rev. A, 103 (2021) 022429.

[15] Christandl, M., Ferrara, R. and Horodecki, K., Phys. Rev. Lett., 126 (2021) 160501.

[16] Kupko, T., Helversen, M.V., Rickert, L., Schulze, J.H., Strittmatter, A., Gschrey, M., Rodt, S., Reitzenstein, S. and Heindel, T., NPJ Quantum Information, 6 (2020) 29.

[17] Navarrete, A., Pereira, M., Curty, M. and Tamaki, K., Phys. Rev. Applied, 15 (2021) 034072.

[18] Xu, F., Ma, X., Zhang, Q., Lo, H.K. and Pan, J.W., Reviews of Modern Physics, 92 (2) (2020) 02500.

[19] Wu, Z., Huang, A., Chen, H., Sun, S.H., Ding, J., Qiang, X., Fu, X., Xu, P. and Wu, J., Optics Express, 28 (2020) 17.

[20] Marøy, Ø., Makarov, V. and Skaar, J., Quantum Science and Technology, 2 (2017) 4.

[21] Wang, T., Huang, P., Zhou, Y., Liu, W., Ma, H., Wang, S. and Zeng, G., Optics Express, 26 (2018) 3.

[22] Wei, W., Liu, H., Ma, H., Yang, X., Zhang, Y., Sun, Y., Xiao, J. and Ji, Y., Scientific Report, 7 (2017) 449.

[23] Park, C.H., Woo, M.K., Park, B.K., Lee, M.S., Kim, Y.S., Cho, Y.W., Kim, S., Han, S.W. and Moon, S., IEEExplore, 6 (2018) 58587.

[24] Lin, J. and Lütkenhaus, N., Phys. Rev. Applied, 14 (2020) 064030.

[25] Bedington, R., Arrazola, J.M. and Ling, A., NPJ Quantum Information, 3 (2017) 30.

[26] Walls, D.F. and Milburn, G.J., "Quantum Optics", (Springer, 1994).

[27] Gerry, C.C. and Knight, P., "Introductory Quantum Optics", (Cambridge. Univ. Press, 2005).

[28] Mandle, F. and Shaw, G., "Quantum Field Theory", (John Wiley & Sons, 1998).

[29] Scully, M.O. and Zubairy, M.S., "Quantum Optics", (Cambridge. Univ. Press, 1997).

[30] Loudon, R., "The Quantum Theory of Light", (Oxford, 2001).

[31] Waks, E., Santori, C. and Yamamoto, Y., Phys. Rev. A, 66 (2002) 042315.

[32] Brassard, G., Lutkenhaus, N., Mor, T. and Sanders, B.C., Phys. Rev. Lett., 86 (2000) 1350.

[33] Leifgen, M., Schröder, T., Gädeke, F., Riemann, R., Métillon, V., Neu, E., Hepp, C., Arend, C., Becher, C., Lauritsen, K. and Benson, O., New Journal of Physics, 16 (2014) 023021.

[34] He, X., Hartmann, N.F., Ma, X., Kim, Y., Ihly, R., Blackburn, J.L., Gao, W., Kono, J., Yomogida, Y., Hirano, A., Tanaka, T., Kataura, H., Htoon, H. and Doorn, S.K., Nature Photonics, 11 (2017) 577.

[35] Migdal, A., Polyakov, S., Fan, J. and Bienfang, J.C., "Single-photon Generation and Detection", (Elsevier, 2013).

[36] Li, A., Chen, T., Zhou, Y. and Wang, X., Opt. Lett., 41 (2016) 1921.

[37] Somaschi, N. et al., Nat. Photon, 10 (2016) 340.

[38] Khazali, M., Heshami, K. and Simon, C., J. Phys. B.: At. Mol. Opt. Phys., 50 (2017) 21.

[39] López Carreño, J.C., J. Phys. B: At. Mol. Opt. Phys., 52 (2019) 3.