Abstract: In this article, we introduce a quantum key distribution protocol for the line of sight channels based on coincidence measurements. We present a proof-of-concept implementation of our protocol. We show that using coincidence measurements to monitor multi-photon pulses results in a higher secure key rate over longer distances for such channels. This key rate is higher than popular implementations of quantum key distribution protocol based on BB84, for example, the GLLP analysis [Quant. Info. Comput. 4, 325 (2004)]. In the experiment, we could generate around 74% more key bits per signal pulse as compared to the GLLP analysis of BB84 protocol with similar parameters and equal value of mean photon number.

© 2021

1. Introduction

Quantum key distribution [1–3] is perhaps the most remarkable application of quantum theory. It exploits the principles of quantum mechanics to enable two distant parties to share a secret random key. Once the key has been established, the two can exchange encrypted messages using private key cryptographic methods. BB84 [4] was the first QKD protocol, based on two basis of orthogonal states, experimentally realised [5] followed by proposals with two nonorthogonal states [6] and the entanglement based protocol [7]. BB84 is proven to be unconditionally secure, based solely on the validity of the laws of quantum mechanics [8–10]. It was later pointed out that imperfection in practical implementations seriously undermine the security of the QKD protocols [11]. This led to proposals for various types of attacks exploiting the imperfections in the components of the QKD system [12–15]. One of them was the lack of ideal single photon sources. This led to the use of weak coherent pulses in which the number of photons in each pulse is governed by a Poissonian distribution. This leads to non-zero probability of pulses containing more than one photon. An eavesdropper can exploit this major vulnerability to extract information about the key during the transmission stage by using a photon number splitting attack [11]. This resulted in several innovative protocols [16–25] and proof of security with practical implementations [26–28]. Notable among the proposed protocols was the decoy state protocol [16,29] for its efficient mitigation of the photon number splitting attack. On the other hand, entanglement based protocols [21,22] suffered from very low key rates and problem of distributing entanglement over long distances reliably with high fidelity. As a result, the decoy state method emerged as the preferred method for long distance quantum key distribution [30–32] with a key rate that was substantially higher than the key rate for implementations with imperfect devices [27]. In this method, the sender, Alice, prepares a set of decoy pulses with varying intensities in addition to the standard BB84 states. The decoy pulses are inserted randomly within the actual signal pulse train unknown to the receiver, Bob, as well as any potential eavesdropper, Eve. Without any prior knowledge regarding the position of the decoy pulses, there is an equal
probability of Eve attacking both the decoy as well as the BB84 signal pulses. By monitoring the quantum bit error rate (QBER) of the decoy pulses, Alice and Bob can reliably estimate a lower bound for the secret key rate. But the improved performance comes at a cost. Implementation of the decoy state protocol requires multiple intensities of the weak coherent pulses, its calibration and increased complexities in hardware and processing.

The major contribution of this article is to demonstrate that, an increased key rate can be achieved without using decoy pulses when communicating parties are in direct line of sight (LOS) channel which can be monitored by other methods, for example, using Lidars [33, 34]. LOS channel are most commonly used in terrestrial communication between two towers in the same city or different cities and also in high altitudes [38, 39]. For small distance communication direct LOS channel can be realized through the drones [40]. The protocol utilises the inherent randomness in the number of photons per pulse of the source itself. Even if eavesdropper is injecting photons directed towards Bob’s receiver, it would result in increasing the two-photon and three-photon error in the coincidence detection. The presence of multi-photon pulses sent by Alice are tracked by coincidence detection at Bob’s end and secure key is extracted using some of the multi-photon pulses too. The difference in the number of actual recorded coincidences and expected number of coincidences for a given value of mean photon number for a given channel plays an important factor in this case. If the ratio of this difference with the actual number of coincidence increases above a threshold value, security is compromised and the protocol is aborted. Otherwise they form the key from the single as well as some of the multi-photon pulses followed by standard error correction and privacy amplification methods. We also use an additional figure of merit, the ratio of coincidences to singles to further monitor the security. Since we use coincidence measurements as a major tool, we call this the Coincidence Detection (CD) protocol.

2. Mathematical Background

In this section, we will provide the mathematical derivation of the key rate for our protocol. In what follows, we will compare the key rates of our proposed protocol with the GLLP analysis [27] since both these protocols make use of a single value of mean photon number. This makes our approach distinct from the decoy state method which uses more than one value of mean photon number. But before proceeding with the derivation, let us first briefly outline the protocol as follows: Alice sends weak coherent pulses to Bob prepared in the standard way for polarization based implementations of BB84. Since the number of photons in each pulse is governed by poissonian statistics, some of the pulses might contain more than one photon. Neither Alice nor Bob has any control over the occurrence of these pulses. Instead of looking at this inherent randomness in the photon number distribution as a drawback, we use it to our advantage. Bob, while recording the measurement results, also records all the 2 and 3-fold coincidence events. The coincidence window is set according to the pulse width of the signal pulses. The total number of coincidences are matched with the expected number of coincidences which are calculated from the value of $\mu$. It was already shown in [14] that the coincidences arising from multiphoton pulses can be tracked to ensure no information is leaked to Eve. Any change in the number of 2 and 3-fold coincidences than the expected value for a specific channel will reveal the presence of eavesdropper in the system assuming that Eve is randomly attacking the pulse (no collective and coherent attack). To estimate the number of 2 and 3-fold coincidence events, it is essential to consider how the pulses split at a balanced beam splitter. For $n$ photon input state, the photons are distributed between the reflected and transmitted ports as

$$|n\rangle \rightarrow \sum_{k=0}^{n} \binom{n}{k} |n-k\rangle_{R}|k\rangle_{T},$$

where $R(T)$ corresponds to the reflected (transmitted) port. $|\binom{n}{k}|^2$ is the probability of getting $n-k$ ($k$) photons in the reflected (transmitted) port. The possible cases for 2 and 3 photon pulses are
given below in the tables 1 and 2 respectively. We will take the coincidences arising out of this splitting of pulses into our consideration when deriving the final key rate.

Table 1. Splitting of a two-photon pulse at a beam splitter.

| Possible Cases | Number of Photons at Transmitted Port | Number of Photons at Reflected Port | Probability |
|----------------|--------------------------------------|-------------------------------------|-------------|
| 1              | 2                                    | 0                                   | 1/4         |
| 2              | 0                                    | 2                                   | 1/4         |
| 3              | 1                                    | 1                                   | 1/2         |

Table 2. Splitting of a three-photon pulse at a beam splitter.

| Possible Cases | Number of Photons at Transmitted Port | Number of Photons at Reflected Port | Probability |
|----------------|--------------------------------------|-------------------------------------|-------------|
| 1              | 3                                    | 0                                   | 1/8         |
| 2              | 0                                    | 3                                   | 1/8         |
| 3              | 1                                    | 2                                   | 3/8         |
| 4              | 2                                    | 1                                   | 3/8         |

In order to derive the key rate, we follow the treatment of [16]. We denote phase randomized signal state of the weak coherent pulses as mixture of coherent states

\[ \rho = \frac{1}{2\pi} \int_{0}^{2\pi} |\sqrt{\mu} e^{i\theta}\rangle (\sqrt{\mu} e^{i\theta}| d\theta. \]  

(2)

Here, \(\mu\) stands for average number of photons per pulse and the signal is assumed to be randomised over all \(\theta\). The probability \(P(n)\) of each pulse carrying \(n\) photons is derived from the Poissonian distribution as \(P(n) = e^{-\mu} \mu^n / n!\). Progressing onwards, the gain \(Q_\mu\) of each pulse is defined as

\[ Q_\mu = Y_0 e^{-\mu} + Y_1 e^{-\mu} \mu + Y_2 e^{-\mu} (\mu^2 / 2!) + \ldots + Y_n e^{-\mu} (\mu^n / n!), \]  

(3)

where \(Y_n\) is the conditional probability that Bob detects an “n photon” signal state given that Alice has sent an “n photon” state. Then, \(Q_n\) becomes the joint probability of Bob detecting “n photon” signal and Alice sending the same “n photon” signal state. For realistic cases, in the absence of an eavesdropper, the term \(Y_0\) gives the background rate of the system including detector dark counts, \(p_{\text{dark}}\). For \(n \geq 1\), yield \(Y_n\) consists of two terms, the detection of signal photons travelling through the channel and the background rate. Assuming that the background rate and the signal events are independent, the expression of \(Y_n\) is seen to be dependent on the channel [16] and approximated to

\[ Y_n \approx [\eta_n + p_{\text{dark}}]/2. \]  

(4)
The transmission efficiency $\eta_n$ of the channel is related to the number of photons as

$$\eta_n = 1 - (1 - \eta)^n,$$

(5)

where $\eta$ is the overall channel transmissivity. Now, the quantum bit error rate (QBER) corresponding to each signal state, $E_\mu$, is defined as

$$E_\mu = \sum_{n=0}^{\infty} Q_n E_n,$$

(6)

where $E_n$ is the error corresponding to the signal containing $n$ photons. Even in the absence of any signal pulse, Bob might record a detection due to background photons or dark current of the detector. This error results in $E_0$ and is equal to 1/4 since all four detectors have equal probability of registering a dark count. If the signal has $n \geq 1$ photons, then the error $E_n$ is given by

$$E_n = \eta_n \frac{E_{\text{detector}}}{2} + (1 - \eta_n) \frac{p_{\text{dark}}}{4} / Y_n,$$

(7)

where $E_{\text{detector}}$ is independent of $n$ and the values of $E_n$ and $Y_n$ can be experimentally derived from the measured values of $Q_\mu$ and $E_\mu$. Major change in these values for a specific channel will reveal the presence of eavesdropper.

Having defined all the necessary terms and variables, let us briefly look at how the equations governing the secret key rate evolves. It was shown in [9] that secret key rate in an ideal implementation scenario with a perfect single photon source and perfect detectors has the form

$$R \geq [1 - 2H_2(E_b)],$$

(8)

where $H_2$ is the binary Shannon entropy defined as $H_2(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ and $E_b$ is the QBER. This formula was later modified by [27] for a more realistic implementation with weak coherent pulses as

$$R \geq q Q_\mu \left[ - f(E_\mu) H_2(E_\mu) + \frac{Q_1}{Q_\mu} \left[ 1 - H_2 \left( \frac{Q_\mu E_\mu}{Q_1} \right) \right] \right],$$

(9)

where $q$ is an implementation dependent factor. In case of passive random basis selector, like balanced beam splitter, $q = 1/2$. $f(E_\mu)$ is the error correcting code efficiency. A severe shortcoming of the above approach was in estimating the maximal value of $\mu$. In order to minimise the number of pulses with 2 or above photons, $\mu$ had to be kept sufficiently small. This reduced the number of single photon pulses thereby greatly limiting the secret key rate. At the same time, the protocol was vulnerable to PNS attacks since the absence of multiphoton pulses could not be ensured. In the decoy state protocol [16], this was taken care of and the secret key rate was modified to

$$R \geq q \{ -Q_\mu f(E_\mu) H_2(E_\mu) + Q_1 [1 - H_2(E_1)] \}. $$

(10)

### 2.1. Key Rate Estimation for Coincidence Detection Method

It is seen in Eq 10 that only single photons are contributing to the key. Now, instead of discarding all the multiphoton pulses, we systematically include a fraction of all such pulses in the final secret key rate as

$$R_{\text{CD}} \geq \{- q Q_\mu f(E_\mu) H_2(E_\mu) + C_1 Q_1 [1 - H_2(E_1)] \}$$

$$+ C_2 Q_2 [1 - H_2(E_2)] + C_3 Q_3 [1 - H_2(E_3)] \},$$

(11)
where \( C_n \)'s are the coefficients of the contributing single, double and triple photons pulses with the implementation dependent factor \( q \) absorbed into them. This is the secret key rate of the CD protocol. In order to derive these coefficients, consider the following: a single photon pulse can only end in the correct basis with probability 1/2 in case of passive basis selector like a balanced beam splitter for which \( q = \frac{1}{2} \). This leads to \( C_1 = \frac{1}{2} \). A two-photon pulse will give rise to three cases as in Table 1 of which case 3 and only one of case 1 or case 2 will contribute to the key. So, \( C_2 = \frac{1}{2} + \frac{1}{4} = \frac{3}{4} \). Similarly, from Table 2 we obtain \( C_3 = \frac{3}{8} + \frac{3}{8} + \frac{1}{8} = \frac{7}{8} \). In this case, both cases 3 and 4 will contribute to the key since in both cases at least one photon will be detected in the correct basis. Please note that the probabilities in Tables 1 and 2 are calculated for a balanced beam splitter. So the factor of \( q = \frac{1}{2} \) is already accounted for while calculating the probabilities justifying the absorption of \( q \) into \( C_n \). Substituting these values in Eq. 11 we arrive at the final form of the secret key rate. The final secret key rate is as follows

\[
R_{CD} \geq \left\{ -\frac{1}{2}Q_{\mu}f(E_{\mu})H_2(E_{\mu}) + \frac{1}{2}Q_1[1 - H_2(E_1)] \right. \\
\left. + \frac{3}{4}Q_2[1 - H_2(E_2)] + \frac{7}{8}Q_3[1 - H_2(E_3)] \right\}.
\]

It is evident that some of the pulses with multiple photons also contribute, leading to a higher secret key rate. This protocol, a modification of BB84 protocol, works best with four SPCMs (Single Photon Counting Modules) as more number of multiphoton pulses can be tracked and the keys can be extracted from them. For two detector system Eq. 12 will be modified by omitting the last term as only two fold coincidences will be observed. For single detector setup only the first and second term will remain in Eq. 12.

2.2. Security against Eavesdropper

The standard security analysis of a QKD protocol involves calculating the difference in mutual information between the communicating parties and the eavesdropper. For direct reconciliation (DR) the difference in mutual information between Alice-Bob and Alice-Eve while, it is Alice-Bob and Bob-Eve for reverse reconciliation (RR). If the mutual information between Alice-Bob exceeds that between Alice-Eve (DR) or Bob-Eve (RR), a secure key can be extracted and the channel is deemed secure. An additional parameter is the QBER. For BB84 based protocols using ideal source and detector, the QBER has an upper limit of 11% against collective attacks [3,9]. After the protocol is executed, if the estimated QBER exceeds that limit, the channel is discarded and the protocol is repeated again. For all those attacks that affect the QBER, it serves as a powerful tool at the hands of the communicating parties.

The security for our protocol is derived from monitoring the QBER as well as the total number of coincidences for a pre-characterised channel within acceptable statistical fluctuations due to device and channel limitations. This means, that the channel transmittance is known and is trusted. This is ensured by actively monitoring the channel during the characterisation process. The total number of coincidences expected are

\[
P_n(\mu) \text{ is the Poissonian probability of a pulse containing } n \text{ photons for a given } \mu. \text{ Since the yield } Y_n \text{ depends on } \eta, \text{ the coincidences depend on both } \mu \text{ and } \eta. \text{ The fractions } (1/2) \text{ and } (3/4) \text{ arise due to the use of a balanced (50:50) beam splitter as the basis selector. The equation (13) means that a two-photon pulse will produce a coincidence half of the times while a three-photon pulse will result in a coincidence 3 out of 4 times. Now, the yields are related as already seen in Eq 4}
\]

\[
Y_2 = 2\eta; Y_3 = 3\eta = \frac{3}{2}Y_2.
\]
Substituting these values and writing $P_3(\mu)$ in terms of $P_2(\mu)$ in Eq. (13), we can write the total number of coincidences as

$$C = \left(\frac{4 + 3\mu}{8}\right) Y_2 P_2 (\mu). \quad (15)$$

Now, we can define a figure of merit $\Xi = \Delta C / C$, which is the ratio of change in coincidences to the total number of coincidences. Under normal circumstances, the coincidences will vary due to statistical fluctuations. As the number of coincidences depend on $\eta$ and $\mu$, the statistical fluctuation $\Delta C_{stat}$ can be written as

$$\Delta C_{stat} = \left| \frac{\partial C}{\partial \eta} \right| \Delta \eta + \left| \frac{\partial C}{\partial \mu} \right| \Delta \mu. \quad (16)$$

Both these terms can be rewritten in terms of the $Y_2$ and $P_2 (\mu)$. This will help us to compare $\Delta C_{stat}$ with $C$. Making the necessary substitutions, we arrive at the form

$$\Delta C_{stat} = \frac{8 + 5\mu - 3\mu^2}{8\mu} Y_2 P_2 (\mu) \Delta \mu + \frac{4 + 3\mu}{8\eta} Y_2 P_2 (\mu) \Delta \eta. \quad (17)$$

The factors $\Delta \mu$ and $\Delta \eta$ are implementation dependent factors. The fluctuation in $\mu$ can arise from imperfect attenuators while fluctuations in $\eta$ can arise due to atmospheric changes. Let us assume that $\mu$ varies by a factor of $\alpha$ over the duration for which the protocol is run i.e. $\Delta \mu = \alpha \mu$. For the same duration, let the transmissivity vary by a factor of $\beta$. So, $\Delta \eta = \beta \eta$. Under these conditions, Eq. (17) is given by

$$\Delta C_{stat} = \frac{\alpha (8 + 5\mu - 3\mu^2) + \beta (4 + 3\mu)}{8} Y_2 P_2 (\mu). \quad (18)$$

We can now define a bound for $\Xi$ that takes into account the statistical fluctuations. We denote it by $\Xi_{stat} = \Delta C_{stat} / C$, which has the form

$$\Xi_{stat} = \frac{8\alpha + 4\beta + (5\alpha + 3\beta) \mu - 3\alpha \mu^2}{4 + 3\mu}. \quad (19)$$

Assuming that the experimental conditions do not change much during the course of the runtime of the protocol, we can make the realistic assumption that the factors $\alpha$ and $\beta$ are quite small. This helps us to set a theoretical bound on $\Xi_{stat}$. The variations of mean photon number ($\mu$) and transmissivity ($\eta$) are well within 1% on an average in our experiment. Therefore, theoretically for setting up the bound we take the values of $\alpha$ and $\beta$ to be around 1%. Additionally, $\Xi_{stat}$ acts as an upper bound for the statistical fluctuations in the number of coincidences recorded during the course of the protocol.

2.2.1. Additional figure of merit for security and optimal $\mu$

We also define an additional figure of merit. The ratio of coincidences to singles. The total number of single detection events can be written as

$$S = Y_1 P_1 (\mu) + \frac{1}{2} Y_2 P_2 (\mu) + \frac{1}{4} Y_3 P_3 (\mu). \quad (20)$$

Using Eq. (14) and (15), we arrive at the following expression for the ratio of coincidences to singles, $\zeta$, as follows

$$\zeta = \frac{C}{S} = \frac{3\mu^2 + 4\mu}{\mu^2 + 4\mu + 8}. \quad (21)$$
Fig. 1. Experimental setup for coincident detection based quantum key distribution protocol. SMF: Single mode fiber; MMF: Multi-mode fiber; NDF: Neutral density filter; HWP: Half-wave plate; PBS: Polarizing beam splitter; BS: 50:50 beam splitter, IF: Interference filter; SPCM: Single photon counting module; TDC: Time to digital converter.

The above analysis derives parameters that give additional security bounds specific to our protocol. These parameters along with QBER estimation suffice to establish the security of our protocol.

3. Experimental Implementation and Results

We have performed the proof of principle demonstration of our protocol. The details of the experimental setup is shown in Fig. 1. We have generated weak coherent pulses by using variable optical attenuator at the output of a pulsed laser (Coherent Vitara T (Ti-Sapphire)) with a repetition rate of 80 MHz. After that the encoded state is propagated in free space lossy medium in the laboratory with channel transmissivity estimated at 70%. At Bob’s end we have usual polarization based BB84 detection setup: balanced beam splitter (passive random basis selector) with polarizing beam splitter (PBS) on the reflected arm (measurement in \{H,V\}) and a combination of half wave plate with PBS (measurement in \{D, A\}) at the transmitted arm. Photons at the output ports of the PBS are detected by fiber coupled avalanche photo diodes (Excelitas SPCM AQRH-14-FC). The avalanche photo diodes are connected to a 8 channel time to digital converter (IDQuantique ID-800) for recording the counts per integration time. It records singles, 2-fold and 3-fold coincidences between various detectors. The coincidence window should be less than or equal to the temporal pulse width of the signal pulse to minimize the probability of a coincidence being recorded between two successive signal pulses or between a signal pulse and any stray pulse. For field applications we can divide our protocol into two categories based on the available channel: I. LOS channel based implementation and II. non-LOS channel based implementation.

3.1. Direct LOS channel

Here we propose to use the CD protocol for realistic atmospheric channels where the line of sight between Alice and Bob is under surveillance. This means, Eve’s presence can be detected by monitoring the channel by other means and Eve is not allowed to alter the channel transmittance. From application point of view, these assumptions are realistic and give practical security. Here the channel is pre-characterized so the amount of coincidences that Bob will receive is
known and is given by Eq.(13). The key rate for this can then be given by Eq.(12) and the security comes from observing the figure of merit $\Xi$ defined in Eq.(19). This results in increase in the optimal $\mu$ for the protocol as given in Fig. 2, which results in increase in the key rate.

The channel transmissivity is calculated as the ratio of signals received to signals sent at the detector. This comes out to be $\eta_t = 0.70$. $\eta$ can be found from $\eta_t$ by dividing it with the efficiencies of detector and the fiber coupler. The yield $Y_\eta$ and $Q_\mu$ can then be calculated by using equations (4) and (3) respectively. We use the calculated value of $\eta$ along with the value of $\mu$ to estimate the number of coincidence events. We list the number of coincidences $C$ along with $\Xi$ and $\zeta$ in table 3. It can be seen, the numbers agree within acceptable tolerance with the predicted values from theoretical simulation and as expected, higher values of $\mu$ lead to higher number of coincidences. By tracking the number of coincidences, $\Xi$, and $\zeta$, we can monitor the presence of the eavesdropper. If the quantity $\Xi$ is below $\Xi_{stat}$, we can extract keys otherwise the protocol is aborted. Please note that we assume a passive eavesdropper who can only listen in on the communication channel between Alice and Bob and enjoys no control over the channel. In Fig.
3. we study the secure key rate as a function of the channel length for different values of $\mu$. We see that the secure key rate increases with increasing values of $\mu$ due to increased presence of pulses containing photons.

![Fig. 3. Secure key rate as function of the channel length with $\mu$ as a parameter. The value of $\mu_{optimal}$ is obtained from Fig. 2 and is equal to 2.2. Two other values of $\mu$ used in the plot are 0.8 ($\mu < \mu_{optimal}$) and 2.9 ($\mu > \mu_{optimal}$).]

Next, we compare the secure key rates of our protocol with that calculated from [27] for the same set of parameters, in Fig. 4. The results show that we have higher key rate along with increase in the transmission distance. For the given channel and $\mu = 0.41$, we expected a key rate of 0.054 bits per pulse. From the experimental data, we obtained 0.053 ± 0.004. This matches very well with our theoretical model. For the same set of parameters, using the GLLP analysis, the expected key rate was 0.032 bits per pulse and the experimentally obtained key rate was 0.031 ± 0.003.

The increase in key rate is due to the fact that some of two and three photon pulses also contribute to the key. In addition, this protocol has greater tolerance to higher values of $\mu$ as shown in Fig. 2. In general, the secure key rate starts decreasing when multiphoton pulses start dominating over single photon pulses. Since coincidence measurements alongwith the security parameters $\Xi$ and $\zeta$ can successfully track and extract key from two-photon and three-photon pulses as well as from all the single photon pulses, this results in a much higher tolerance of mean photon number.

3.2. Non direct LOS channel based implementation

For the case when direct LOS is not available eavesdropping will be easier as regular channel monitoring will be a difficult task. Eve can take the advantage of this and can vary the losses accordingly (tamper the channel) to match with the original channel after extracting photons from each of the multi-photon pulses for gaining information of the key. This can be averted by incorporating the extra pulses with variable intensities randomly in between the signals akin to decoy state protocol. Lack of knowledge about the extra pulses makes Eve randomly attacking both the signal and extra pulses with equal possibility. The ratio is generally 70 (signal) : 30 (extra) so if Eve attacks them equally the relative loss in the detected number of photons for
signal and extra pulses will be different. This change can be observed if the timing information is matched for the received signal and extra pulses with the transmitted. Checking the relative loss between the signal and extra pulses (i.e. if the loss of signal is not equal to the extra pulses) can reveal the presence of eavesdropper, making the protocol secure. It must be noted that the introduction of extra pulses does not affect the higher key rate achieved through our protocol in comparison to decoy state protocol. The key rate formula will remain the same as it uses the optimal mean photon number ($\mu$) in which the protocol must operate to achieve higher key rate. The presented protocol will require a good spectral and temporal filtering mechanism. For spectral filtering, narrow bandwidth band pass filter has to be used. For accurate temporal filtering, a high speed event timer has to be used with a resolution of picoseconds.

4. Conclusion

In this article we have proposed Coincidence Detection based BB84 quantum key distribution protocol with weak coherent pulse under restricted eavesdropping assumption set for LOS channel. We have proposed and derived an analytical expression for the secret key rate taking into account the contribution of pulses with more than one photon in the final key. We argue that by closely monitoring the number of coincidence events arising at the receiver end and matching it with the expected number of coincidences, any attempt at channel tampering can be monitored. We have also presented a security proof in support of our protocol and introduced two figures of merit to verify the security of our protocol. We have shown that this results in a higher key rate over longer distances compared to popular implementations of BB84 based protocols for the same set of parameters. We have also performed a proof-of-principle experiment to verify our predictions. The numbers obtained from the experiment agree quite well with the predicted results. One possible demerit might be the need for accurate characterization of the channel which might limit the implementation scenario to clear line of sight situations. Such a situation is mitigated by introducing extra pulses of variable intensities. Introduction of these pulses provide security like decoy state protocol [37]. The overall simpler setup is beneficial for free space lossy channel since it can achieve higher key rates over longer distances.

**Funding.** This work has been partially funded by DST through QuST program.
Acknowledgments. A.B, A.B, N.J, P.C and R.P.S acknowledge the partial funding support from DST through QuST program/ R. K. acknowledges the support from UK EPSRC through Quantum Technology Hub for Quantum Communications Technology, grant no. EP/T001011/1. The authors would also like to thank Prof. Alexander V. Sergienko for his helpful comments.

Disclosures. Authors declare no conflict of interest

Data Availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

References
1. N Gisin, G Riborvy, W. Titel and H. Zbinden, Quantum Cryptography, Rev. Mod. Phys. 74, 145 (2002).
2. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. 81, 1301 (2009).
3. S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. Usenko, G. Vallone, P. Villoresi and P. Wallden, Advances in Quantum Cryptography, preprint arxiv:1906.01645 (2019).
4. C. H. Bennett and G. Brassard, in Proceedings of the conference on computers, Systems and Signal Processing (IEEE Press, New York, 1984), pp. 175.
5. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, Experimental quantum cryptography, J. Cryptology 5, 3 (1992).
6. C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett 68, 3121 (1992).
7. A. K. Ekert, Quantum cryptography based on Bell’s theorem, Phys. Rev. Lett. 67, 661 (1991).
8. D. Mayers, Unconditional security in quantum cryptography, J. Acm. 48, 351 (2001).
9. P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. 85, 441 (2000).
10. D. Mayers, Shor and Preskill’s and Mayer’s security proof for the BB84 quantum key distribution protocol, The Euro. Phys. J. D - Atom. Mol. Opt. Opt. Plasm Phys. 18, 161 (2002).
11. G. Brassard, N. Lutkenhaus, T. Mor and B. C. Sanders, Limitations on practical quantum cryptography, Phys. Rev. Lett. 85, 1330 (2000).
12. A. Vakhitov, V. Makarov and D. R. Hjelme, Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography, J. Mod. Opt. 48, 2023 (2001).
13. F. Xu, B. Qi and H.-K. Lo, Experimental demonstration of phase-remapping attack in a practical quantum key distribution system, New J. Phys. 12, 113206 (2010).
14. S. Felix, N. Gisin, A. Stefanov and H. Zbinden, Faint laser quantum key distribution: eavesdropping exploiting multiphoton pulses, J. Mod. Opt. 48, 2009 (2001).
15. S. Nauerth, M. Farst, T. Schmitt-Manderbach, H. Weier and H. Weinfurter, Information leakage via side channels in free space BB84 quantum cryptography, New J. Phys. 11, 0655001 (2009).
16. H.-K. Lo, X. Ma and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. 94, 230504 (2005).
17. V. Scarani, A. Acin, G. Ribordy and N. Gisin, Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations, Phys. Rev. Lett. 92, 057901 (2004).
18. K. Tamaki and H.-K. Lo, Unconditionally secure key distillation from multiphotons, Phys. Rev. A 73, 010302 (2006).
19. X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett. 94, 230503 (2005).
20. M. Koashi and J. Preskill, Secure quantum key distribution with an uncharacterized source, Phys. Rev. Lett. 90, 057902 (2003).
21. H.-K. Lo, M. Curty and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. 113, 130503 (2012).
22. U. Vazirani and T. Vidick, Fully device-independent quantum key distribution, Phys. Rev. Lett. 113, 140501 (2014).
23. M. Lucamarini, Z. L. Yuan, J. F. Dynes and A. J. Shields, Overcoming the rate distance limit of quantum key distribution without quantum repeaters, Nature 557, 400 (2018).
24. M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lutkenhaus and A. Forbes, Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases, Phys. Rev. A 88, 032305 (2013).
25. A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischof, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Hein, C. Marquardt, G. Leuchs, R. Boyd and E. Karimi, High-dimensional intracity quantum cryptography with structured photons, Optica 4, 1006 (2017).
26. N. Lutkenhaus, Security against individual attacks for realistic quantum key distribution, Phys. Rev. A 61, 052304 (2000).
27. D. Gottesman, H.-K. Lo, N. Lutkenhaus and J. Preskill, Security of quantum key distribution with imperfect devices, Quant. Info. Comput. 4, 325 (2004).
28. H. Inamori, N. Lutkenhaus and D. Mayers, Unconditional security of practical quantum key distribution, The Eur. Phys. J. D 41, 599 (2007).
29. W.-Y. Hwang, Quantum key distribution with high loss: Towards global secure communication, Phys. Rev. Lett. 91, 057901 (2003).
30. A. Boaron, G. Bosco, D. Rusca, C. Autebert, M. Caloz, M. Perrenoud and H. Zbinden, Secure Quantum Key Distribution over 421 km of Optical Fiber, Phys. Rev. Lett. 121, 190502 (2018).
31. Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, Feng-Zhi Li, Xiu-Wei Chen, Li-Hua Sun, Jian-Jun Jia, Jin-Cai Wu, Xiao-Jun Jiang, Jian-Feng Wang, Yong-Mei Huang, Qiang Wang, Yi-Lin Zhou, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Qiang Zhang, Yu-Ao Chen, Nai-Le Liu, Xiang-Bin Wang, Zhen-Cai Zhu, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang and Jian-Wei Pan, Satellite-to-ground quantum key distribution, Nature (London) 549, 43 (2017).
32. A. R. Dixon and J. F. Dynes and M. Lucamarini and B. Fröhlich and A. W. Sharpe and A. Plews and S. Tam and Z. L. Yuan and Y. Tanizawa and H. Sato and S. Kawamura and M. Fujiwara and M. Sasaki and A. J. Shields, High speed prototype quantum key distribution system and long term field trial, Opt. Express, 23, 7583–7592 (2015)
33. M. Legre and B. Huttner, Quantum-enhanced physical layer cryptography: A new paradigm for freespace key distribution, QCrypt 2017, 18-22 September 2017 in Cambridge, United Kingdom.
34. S. Bahrami, M. Ghahai, C. Liorini, A. Ling, R. Kumar, B. Huttner, S. Pirandola, C. C. W. Wen, T. Spiller, N. Lutkenhaus and M. Razavi, Satellite based quantum communication under realistic threat model, QCrypt 2019, 26-30 August, 2019, Montreal, Canada.
35. Bing Qi, Bennett-Brassard 1984 quantum key distribution using conjugate homodyne detection, Phys. Rev. A 103, 1 (2021).
36. H. Endo, M. Fujiwara, M. Kitamura, O. Tsuzuki, R. Shimizu, M. Takeoka, and M. Sasaki, Group key agreement over free-space optical links, OSA Continuum 3 (2020).
37. M. Lucamarini, J.F. Dynes, B. Fröhlich, Zhiliang Yuan and A.J. Shields, Security bounds for efficient decoy-state quantum key distribution, IEEE Journal of Selected Topics in Quantum Electronics 21, 197 (2015).
38. Y. Chu, R. Donaldson, R. Kumar, D. Grace, Feasibility of Quantum Key Distribution from High Altitude Platforms, 2020, arXiv:2012.07479.
39. S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick and H. Weinfurter, Air-to-ground quantum communication, Nature Photon 7, 382–386 (2013).
40. S. Isaac, A. Conrad, A. Hill, K. Herndon, B. Wilens, D. Chaffee, D. Sanchez-Rosales, R. Cochran, D. Gauthier, and P. Kwiat, Drone-Based Quantum Key Distribution, 2020 Conference on Lasers and Electro-Optics (CLEO), San Jose, CA, USA, 1-2 (2020)