Quantum key distribution with multiphoton pulses: An advantage

Ayan Biswas[1,2], Anindya Banerji[1],* Nijil Lal[1,2], Pooja Chandravanshi[1], Rupesh Kumar[3], and Ravindra P. Singh[1†]
[1] *Quantum Science and Technology Laboratory, Physical Research Laboratory, Ahmedabad 380009, India*
[2] *Indian Institute of Technology, Gandhinagar 382355, India and*
[3] *Quantum Communications Hub, Department of Physics, University of York, York, YO10 5DD, UK*
(Dated: August 18, 2020)

In this letter we present proof-of-concept implementation of quantum key distribution protocol based on BB84 with imperfect devices. We show that using coincidence measurements to monitor multiphoton pulses results in a higher secure key rate over longer distances. This key rate is higher than the decoy state protocol, the most popular practical implementation of quantum key distribution protocol based on BB84. In the experiment, we obtained a key rate of 0.053934 ± 0.004088 per signal pulse compared to 0.031051± 0.003303 for decoy state protocol with similar parameters.

Keywords: quantum key distribution, weak coherent pulse, decoy state protocol

Quantum key distribution [1–3] is perhaps the most remarkable application of quantum theory. It exploits the principles of quantum mechanics to enable secure exchange of information. Quantum key distribution (QKD) protocols allow two distant parties to share a secret random key. Once the key has been established, the two can exchange encrypted messages with the help of a one-time pad. BB84 [4] was the first such protocol to be experimentally realised [5] followed by proposals for implementation of QKD 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]. 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 simpler implementation which did not require much additional hardware. 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, 31] with a key rate that was substantially higher than the estimated key rate for implementations with imperfect devices [27]. In this method, the sender, hereafter called 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, hereafter called Bob as well as any potential eavesdropper, hereafter called 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.

The major contribution of this article is to demonstrate that using present technology, similar security with an increased key rate can be achieved without using decoy pulses. This is done utilising the inherent randomness in the number of photons per pulse of the source itself. Presence of multiphoton pulses sent by Alice can be tracked by coincidence detections at Bob's end. By accurately estimating the number of multi-photon pulses expected in a given channel during a given window, the presence of Eve can be detected by looking at the number of coincidences between conjugate bases. If the number of coincidences is less than an estimated threshold, the protocol is aborted. Otherwise they form the key with the detection results following standard error correction and privacy amplification methods.

Following the treatment of [16], we denote phase randomized signal state of the weak coherent pulses as $|\sqrt{\mu}e^{i\theta}\rangle$. Here μ stands for average number of photons per pulse and the signal is assumed to be randomised over all θ. 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_μ of each pulse is defined as

$$\begin{aligned} Q_\mu =& Y_0 e^{-\mu} + Y_1 e^{-\mu}\mu + Y_2 e^{-\mu}(\mu^2/2!) + ... \\ &+ ... + Y_n e^{-\mu}(\mu^n/n!), \end{aligned} \tag{1}$$

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_{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

$$Y_n \approx [\eta_n + p_{dark}]/2, \tag{2}$$

The transmission efficiency η_n of the channel is related to the number of photons as

$$\eta_n = 1 - (1-\eta)^n, \tag{3}$$

where η is the overall channel transmissivity. Now, the quantum bit error rate (QBER) corresponding to each signal state, E_μ, is defined as

$$E_\mu Q_\mu = \sum_{n=0}^{\infty} Q_n E_n, \tag{4}$$

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

$$E_n = \big(\eta_n \frac{E_{detector}}{2} + (1-\eta_n)\frac{p_{dark}}{4}\big)/Y_n, \tag{5}$$

where $E_{detector}$ is independent of n and the values of E_n and Y_n can be experimentally derived from the measured values of Q_μ and E_μ. 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

$$R \geq [1 - 2H_2(E_b)], \tag{6}$$

where H_2 is the binary Shannon entropy defined as $H_2(x) = -xlog_2x - (1-x)log_2(1-x)$ and E_b is the QBER. This formula was later modified by [27] for a more realisitic implementation with weak coherent pulses as

$$R \geq qQ_\mu\Big\{-f(E_\mu)H_2(E_\mu) + \frac{Q_1}{Q_\mu}\Big[1 - H_2\big(\frac{Q_\mu E_\mu}{Q_1}\big)\Big]\Big\}, \tag{7}$$

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 μ. In order to minimise the number of pulses with 2 or above photons, μ had to be kept sufficiently small. This reduced the number of single photon pules thereby greatly limiting the secret key rate. At the same time, the protocol was vulnerable against 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

$$R \geq q\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1 - H_2(E_1)]\}. \tag{8}$$

Before proceeding with the derivation of the secret key rate for our proposed protocol, 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 μ. 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

$$|n\rangle \rightarrow \sum_{k=0}^{n} C_k^n |n-k\rangle_R |k\rangle_T \tag{9}$$

where $R(T)$ corresponds to the reflected (transmitted) port. $|C_k^n|^2$ 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 I and II respectively.

TABLE I: 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

Now, instead of discarding all the multiphoton pulses, we systematically include a fraction of all such pulses in the final secret key rate as

$$\begin{aligned} R \geq \{&-qQ_\mu f(E_\mu)H_2(E_\mu) + C_1Q_1[1 - H_2(E_1)] \\ &+ C_2Q_2[1 - H_2(E_2)] + C_3Q_3[1 - H_2(E_3)]\}, \end{aligned} \tag{10}$$

where C_n's are the coefficients of the contributing single, double and triple photons pulses with the implementa-

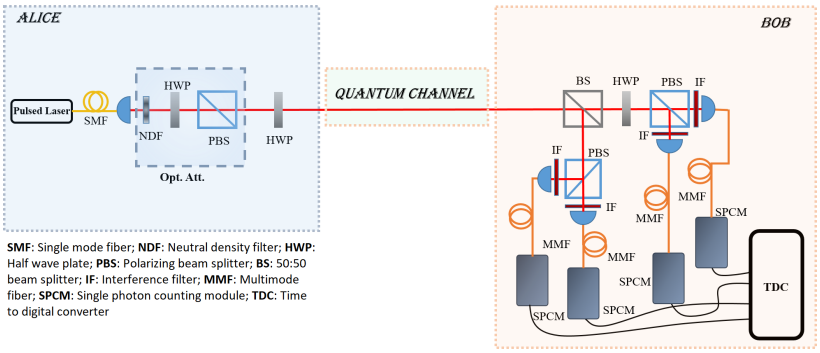

FIG. 1: Experimental setup for coincident detection based quantum key distribution protocol.

TABLE II: 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

tion dependent factor q absorbed into them. 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 spliter leading to $C_1 = 1/2$. A two-photon pulse will give rise to three cases as in Table I of which case 3 and only one of case 1 and 2 will contribute to the key. So, $C_2 = 1/2 + 1/4 = 3/4$. Similarly, from Table II we obtain $C_3 = 3/8 + 3/8 + 1/8 = 7/8$. 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. Substituting these values in Eq. 10 we arrive at the final form of the secret key rate as follows

$$R \geq \{-\frac{1}{2}Q_\mu f(E_\mu)H_2(E_\mu) + \frac{1}{2}Q_1[1 - H_2(E_1)] + \frac{3}{4}Q_2[1 - H_2(E_2)] + \frac{7}{8}Q_3[1 - H_2(E_3)]\}. \quad (11)$$

As is evident, since some of the pulses with multiple photons also contribute to the secret key rate, we can achieve a higher key rate compared to the decoy state protocol. 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. From mean photon number at the source, an estimation can be made on the number of two fold and three fold coincidences expected at Bob's end assuming Alice and Bob know their channel well.

The channel transmissivity is calculated as the ratio of signals sent to signals received at the detector. This comes out to be $\eta_t = 0.70 \pm 0.028$. η can be found from η_t by dividing it with the efficiencies of detector and the fiber coupler. The yield Y_n and Q_μ can then be calculated by using equations (2) and (1) respectively. We use the calculated value of η along with the value of μ to estimate the number of coincidence events. We list the expected numbers and the actual number of coincidences in table III. As can be seen, the numbers agree within acceptable tolerance and as expected, higher values of μ lead to higher number of coincidences. By tracking these number of coincidences we can monitor the presence of the eavesdropper. If there is any substantial difference between the predicted and measured values, the protocol is adjourned. In Fig. 2, we study the secure key rate as a function of the channel length for different values of μ. We see that the secure key rate increases with increasing values of μ due to increased presence of pulses containing photons. Next, we compare the secure key rates of our protocol with that calculated from the decoy state

TABLE III: Comparison between expected and actual number of coincidences for the given channel.

μ	C_{exp}	C_{act}
0.13	3178	3189 ± 53
0.19	6414	6249 ± 69
0.22	8828	8756 ± 85
0.32	18657	18367 ± 111
0.41	30337	30140 ± 237

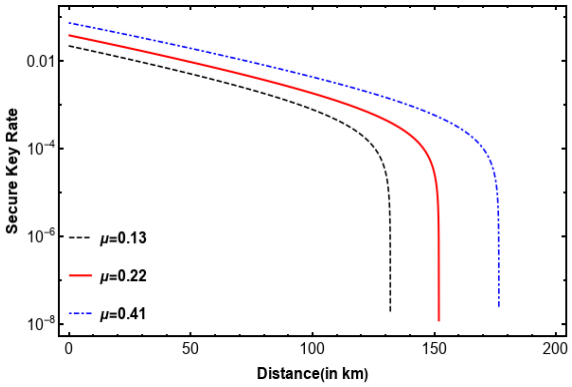

FIG. 2: Secure key rate as function of the channel length with μ as a parameter.

protocol for the same set of parameters, in Fig. 3. The results show that we have higher key rate along with increase in the transmission distance. For the given channel and μ =0.41, we expected a key rate of 0.054327 per pulse. From the experimental data, we obtained 0.053934 ± 0.004088. This matches very well with our theoretical model. For the same set of parameters, in case of the decoy state protocol, the expected key rate was 0.031735 per pulse and the experimentally obtained key rate was 0.031051 ± 0.003303. The increase in key rate is due

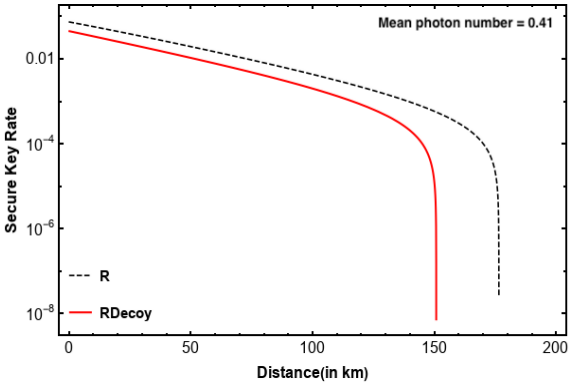

FIG. 3: Comparison of secure key rates between decoy state protocol and CD protocol for the same set of parameters.

to the fact that some of two and three photon pulses

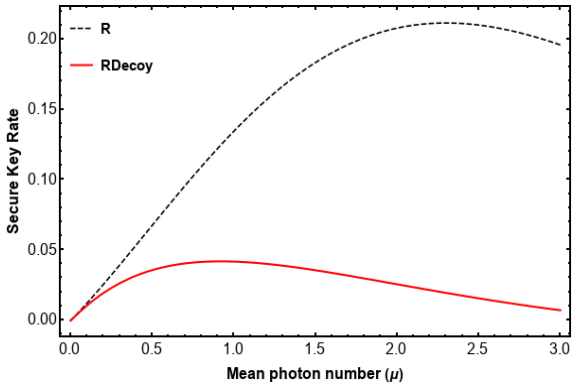

FIG. 4: Optimal mean photon number μ for decoy state and CD protocol.

also contribute to the key. In addition, this protocol has greater tolerance to higher values of μ as compared to the decoy state protocol. We study this tolerance in Fig. 4. In general, the secure key rate starts decreasing when multiphoton pulses start dominating over single photon pulses. Since coincidence measurements 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.

In this article we have proposed Coincidence Detection based BB84 quantum key distribution protocol with WCP. We call this the CD protocol in short. 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. The expected number of coincidences is calculated with the help of mean photon number, μ and the probability $P(n)$ of a pulse containing n photons along with the channel transmissivity η. We have shown that this results in a higher key rate over longer distances compared to the much used decoy state protocol 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. While conceding that this is true, we further point out that the clear line of sight needs to be maintained while characterizing the channel before the start of the actual protocol. Once the channel has been characterized there is no further need to maintain the line of sight since any tampering of the channel will affect the asymptotic statistics of the coincidences thereby exposing the presence of an adversary.

Also, the 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. The overall simpler setup is beneficial for free space lossy channel since it can achieve higher key rates over longer distances.

This work is partially supported by DST through QuEST program. R. K. acknowledge the support from UK EPSRC through Quantum Technology Hub for Quantum Communications Technology, grant no. EP/T001011/1.

* abanerji09@gmail.com
† rpsingh@prl.res.in

[1] N Gisin, G. Riborby, W. Tittel 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 *et al.*, 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. 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. Furst, 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 *et al.* Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases, Phys. Rev. A **88**, 032305 (2013).
[25] A. Sit *et al.*, 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. Boso, 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] S.-K. Liao *et al.*, Satellite-to-ground quantum key distribution, Nature (London) **549**, 43 (2017).