

Practical decoy-state BB84 quantum key distribution with quantum memory

Xian-Ke Li(李咸柯), Xiao-Qian Song(宋小谦), Qi-Wei Guo(郭其伟), Xing-Yu Zhou(周星宇), and Qin Wang(王琴)
Citation: Chin. Phys. B, 2021, 30 (**6**): 060305. DOI: 10.1088/1674-1056/abda31
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Continuous-variable quantum key distribution based on photon addition operation

Xiao-Ting Chen(陈小婷), Lu-Ping Zhang(张露萍), Shou-Kang Chang(常守康), Huan Zhang(张欢), and Li-Yun Hu(胡利云)
Chin. Phys. B, 2021, 30 (**6**): 060304. DOI: 10.1088/1674-1056/abd931

One-decoy state reference-frame-independent quantum key distribution

Xiang Li(李想), Hua-Wei Yuan(远华伟), Chun-Mei Zhang(张春梅), Qin Wang(王琴)
Chin. Phys. B, 2020, 29 (**7**): 070303. DOI: 10.1088/1674-1056/ab90f6

Hybrid linear amplifier-involved detection for continuous variable quantum key distribution with thermal states

Yu-Qian He(贺宇千), Yun Mao(毛云), Hai Zhong(钟海), Duang Huang(黄端), Ying Guo(郭迎)
Chin. Phys. B, 2020, 29 (**5**): 050309. DOI: 10.1088/1674-1056/ab8216

Reconciliation for CV-QKD using globally-coupled LDPC codes

Jin-Jing Shi(石金晶), Bo-Peng Li(李伯鹏), Duan Huang(黄端)
Chin. Phys. B, 2020, 29 (**4**): 040301. DOI: 10.1088/1674-1056/ab6d4f

Reference-frame-independent quantum key distribution with an untrusted source

Jia-Ji Li(李家骥), Yang Wang(汪洋), Hong-Wei Li(李宏伟), Wan-Su Bao(鲍皖苏)
Chin. Phys. B, 2020, 29 (**3**): 030303. DOI: 10.1088/1674-1056/ab695d

---

Practical decoy-state BB84 quantum key distribution with quantum memory*

Xian-Ke Li(李咸柯)[1,2,3], Xiao-Qian Song(宋小谦)[1,2,3], Qi-Wei Guo(郭其伟)[1], Xing-Yu Zhou(周星宇)[1,2,3], and Qin Wang(王琴)[1,2,3,†]

[1] *Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*
[2] *Broadband Wireless Communication and Sensor Network Technology, Key Laboratory of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*
[3] *Telecommunication and Networks National Engineering Research Center, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*

(Received 14 October 2020; revised manuscript received 31 December 2020; accepted manuscript online 11 January 2021)

We generalize BB84 quantum key distribution (QKD) to the scenario where the receiver adopts a heralded quantum memory (QM). With the heralded QM, the valid dark count rate of the receiver's single photon detectors can be mitigated obviously, which will lower the quantum bit error rate, and thus improve the performance of decoy-state BB84 QKD systems in long distance range. Simulation results show that, with practical experimental system parameters, decoy-state BB84 QKD with QM can exhibit performance comparable to that of without QM in short distance range, and exhibit performance better than that without QM in long distance range.

Keywords: quantum key distribution, quantum communication, quantum memory, decoy state

PACS: 03.67.Dd, 03.67.Hk, 42.65.Lm **DOI:** 10.1088/1674-1056/abda31

1. Introduction

Quantum key distribution (QKD)[1] can generate secure keys between two distant users (usually named as Alice and Bob), despite the presence of an eavesdropper (Eve), which has made remarkable progress since 1984.[2–6] Generally, the performance of QKD deteriorates with the increase of transmission distance. To improve the performance of QKD, quantum memory (QM) which has capability of receiving, storing, and retrieving photons, can be applied in QKD systems.[7]

Despite the technology of QM is not mature yet, the characteristics of QM have been greatly improved, such as long storage times,[8,9] high fidelities,[10–12] and high storage efficiencies.[13] More importantly, QM can work at room temperature,[14–16] which makes it more applicable than before. Recently, works on QKD with QM have been reported.[7,17] The authors in Ref. [7] adopted heralded QMs to enhance the performance of measurement-device-independent QKD (MDI-QKD),[18] while the authors in Ref. [17] utilized a portable QM to realize free-space QKD.

In this paper, we investigate the performance of BB84 QKD with a heralded QM, which does not need entanglement sources and can work with the widely used weak coherent sources (WCS). In order to combat the photon number splitting attacks[19,20] caused by multi-photons in WCS, the decoy-state method[21–24] is applied in our scheme. With practical experimental parameters, we demonstrate that decoy-state BB84 QKD with QM can exhibit performance better than that of without QM especially in long distance range.

2. Theory and security analysis of BB84 QKD with QM

The QM can be used to receive, store and retrieve photons. According to Ref. [25], we denote the writing efficiency as η_{in}, which is the probability that the pulse sent by Alice is stored in the QM. Alice and Bob know whether the pulse is stored or not, because the QM is supposed to send out a heralding signal when a photon state is successfully stored.[26–28] η_{out} represents retrieving probability of a pulse from the QM.

In our scheme (Fig. 1), Alice sends a sequence of encoded BB84 states to Bob. At Bob's side, the QM stores Alice's pulses with probability η_{in}, and reads out the stored pulses with probability η_{out}. In the present quantum key distribution systems, in order to reduce the dark count rate, Bob's single-photon detectors usually work with a gating mode, *i.e.*, they only open when there is triggering signal. Usually Bob's single-photon detectors are triggered by the synchronization signal of laser pulses, *i.e.*, the gating repetition rate is the same as the laser. Considering the heralding characteristic of the QM, Bob can discard those recording events without being heralded, *i.e.*, the photon pulses are not successfully stored in QM, resulting in substantially reduced dark count rate at Bob's side.

*Project supported by the National Key Research and Development Program of China (Grant Nos. 2018YFA0306400 and 2017YFA0304100), the National Natural Science Foundation of China (Grant Nos. 12074194 and 11774180), and the Leading-edge Technology Program of Jiangsu Provincial Natural Science Foundation, China (Grant No. BK20192001).

†Corresponding author. E-mail: qinw@njupt.edu.cn

© 2021 Chinese Physical Society and IOP Publishing Ltd

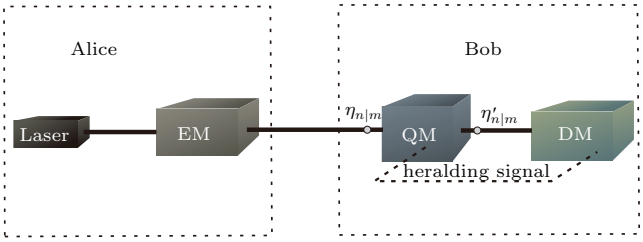


Fig. 1. Scheme of BB84 QKD with a heralded QM. EM: encoding module; DM: detection module.

Let $\eta_{\rm b}$ denote the transmittance in Bob's side, which includes the internal transmittance of optical components and detector efficiency. And $\eta_{\rm b}$ can be boiled down to the channel transmittance.[29] Hence, the overall transmittance between Alice and Bob, η, can be expressed as

$$\eta = \eta_{\rm b} 10^{-\alpha L/10}, \tag{1}$$

where α denotes the channel loss coefficient, and L is the fiber length.

In the framework of BB84 QKD with QM, $\eta_{n|m}$ represents the transmittance of an n-photon state given that Alice sends an m-photon state before QM. $Y_{n|m}$ and $\eta'_{n|m}$ respectively represent the yield and transmittance at Bob's side given that the QM successfully stores and retrieves an n-photon state when Alice sends an m-photon state. And $Y_{n|m}$ mainly comes from two parts, one coming from the detector dark count rate, the other from the detection of true signal. The combination gives

$$Y_{n|m} = Y_{0_{n|m}} + \left(1 - Y_{0_{n|m}}\right)\eta'_{n|m} \approx Y_{0_{n|m}} + \eta'_{n|m}, \tag{2}$$

where $Y_{0_{n|m}}$ represents the conditional probability of a detection event at Bob's side given that the QM successfully stores an n-photon state but fails to retrieve it when Alice sends an m-photon state, *i.e.*,

$$Y_{0_{n|m}} = Y_0 C_m^n \eta^n (1-\eta)^{m-n} \eta_{\rm in}(1-\eta_{\rm out}). \tag{3}$$

And other quantities can be expressed as

$$\eta_{n|m} = C_m^n \eta^n (1-\eta)^{m-n}, \tag{4}$$

$$\eta'_{n|m} = C_m^n \eta^n (1-\eta)^{m-n} \eta_{\rm in}\eta_{\rm out}. \tag{5}$$

Note that, due to the assumption that the QM is heralded, there will be no heralding signal if the QM stores no photons. Hence, we have $m \geq n > 0$ in Eqs. (2)–(5).

According to Eqs. (2)–(4) and Ref. [24], we have the error rate $e_{n|m}$

$$e_{n|m} = \frac{e_0 Y_{0_{n|m}} + e_{\rm d}\eta_{n|m}}{Y_{n|m}}, \tag{6}$$

where $e_{\rm d}$ is the probability that a photon hits a wrong detector, and e_0 is the error rate of the background.

Combining Eqs. (1)–(6), the corresponding average gain Q_ξ and the average quantum bit error rate (QBER) $E_\xi Q_\xi$ can be expressed as

$$Q_\xi = \sum_{m=1}^{\infty}\sum_{n=1}^{m} Y_{n|m} P_m^\xi, \tag{7}$$

$$E_\xi Q_\xi = \sum_{m=1}^{\infty}\sum_{n=1}^{m} Y_{n|m} P_m^\xi e_{n|m}, \tag{8}$$

where ξ denotes the average photon number, and $P_m^\xi = {\rm e}^{-\xi}\xi^m/m!$ represents the photon number distribution for ξ intensity.

Below let us give brief security analysis for our scheme according to information theory,[30] the lower bound of secure key rate of QKD system is equal to the mutual information between Alice and Bob $I(A:B)$ minus the mutual information between Eve and Bob (Alice) $I(B:E)$ ($I(A:E)$), that is

$$R = I(A:B) - I(B:E). \tag{9}$$

When Bob's detector has a no-click event or Bob chooses the wrong measurement basis, there is no correlation between Bob's measurement results and the data sent by Alice, that is, $I(A:B) = 0$. When Bob selects the right basis and detector has a click event, $I(A:B) = 1 - H_2(E_\xi)$. $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ represents the binary Shannon information function. Therefore,

$$I(A:B) = \left(1 - Q_\xi\right) \times 0 + Q_\xi \times \left[1 - H_2\left(E_\xi\right)\right]. \tag{10}$$

For Eve, when Bob's detector has a no-click event or Bob chooses the wrong measurement basis, the data is discarded and Eve cannot obtain valid information, $I(B:E) = 0$. When Bob selects the right basis and detector has a click event, there are two cases to discuss considering that QM has heralding characteristic. First, when the sifted key is generated by the single-photon state, Eve can obtain information of $H_2\left(e_{1|1}\right)$.[31] Second, when the sifted key is generated by the multiple-photon state, Eve can obtain all information.

From what has been discussed above, the mutual information $I(B:E)$ can be expressed as

$$I(B:E) = Q_{1|1} \times H_2\left(e_{1|1}\right) + Q_{\rm multi} \times 1. \tag{11}$$

Where $Q_{\rm multi} = \sum_{m=2}^{\infty}\sum_{n=1}^{m} Y_{n|m} P_m^\xi$, representing the gain generated by multiple-photon state. Then,

$$\begin{aligned} R &= I(A:B) - I(B:E) \\ &= Q_\xi\left[1 - H_2\left(E_\xi\right)\right] - Q_{1|1}H_2\left(e_{1|1}\right) - Q_{\rm multi} \times 1 \\ &= -Q_\xi H_2\left(E_\xi\right) + Q_{1|1}\left[1 - H_2\left(e_{1|1}\right)\right]. \end{aligned} \tag{12}$$

Considering that the error correction efficiency f is slightly bigger than one, and $Q_{1|1} = Y_{1|1}P_1^\xi$, this formula can be modified as

$$R = -Q_\xi f H_2\left(E_\xi\right) + Y_{1|1}P_1^\xi\left[1 - H_2\left(e_{1|1}\right)\right]. \tag{13}$$

From the above security analysis, we now obtain the lower bound of secure key rate for the asymptotic case.

3. The three-intensity decoy-state BB84 protocol with QM

To implement the scheme of BB84 QKD with a heralded QM, we employ the three-intensity decoy-state method,[24] where Alice randomly modulates the WCS pulses into three different intensities u, v, and 0 ($u > v > 0$).

Similar to Eq. (7), the gains of these two decoy states are given by

$$Q_u = \sum_{m=1}^{\infty}\sum_{n=1}^{m} Y_{n|m} P_m^u, \tag{14}$$

$$Q_v = \sum_{m=1}^{\infty}\sum_{n=1}^{m} Y_{n|m} P_m^v. \tag{15}$$

When any $m \geq 2$, the m-photon probability of WCS satisfies

$$\frac{P_m^u}{P_m^v} \geq \frac{P_2^u}{P_2^v} \geq \frac{P_1^u}{P_1^v}. \tag{16}$$

Combining Eqs. (14)–(16), we have

$$\begin{aligned} P_2^u Q_v - P_2^v Q_u &= Y_{1|1}\left(P_1^v P_2^u - P_2^v P_1^u\right) \\ &\quad + \sum_{n=3}^{\infty}\left[\left(Y_{1|n} + Y_{2|n} + \cdots + Y_{n|n}\right)\left(P_n^v P_2^u - P_2^v P_n^u\right)\right] \\ &\geq Y_{1|1}\left(P_1^v P_2^u - P_2^v P_1^u\right). \end{aligned} \tag{17}$$

By solving inequality (17), the lower bound of the single-photon yield $Y_{1|1}^L$ is given by

$$Y_{1|1} \geq Y_{1|1}^L = \frac{P_2^u Q_v - P_2^v Q_u}{P_2^u P_1^v - P_2^v P_1^u}. \tag{18}$$

When $\xi = v$, we can use Eq. (8) to work out the upper bound of the single-photon error rate $e_{1|1}^U$,

$$e_{1|1} \leq e_{1|1}^U = \frac{E_v Q_v}{P_1^v Y_{1|1}}. \tag{19}$$

4. Numerical simulations

In practical QKD systems, statistical fluctuations have to be considered. Here for simplicity, we assume the channel fluctuation satisfies a Gaussian distribution, and we adopt the Gaussian analysis method to estimate the channel parameters.[32] Here the number of standard deviations in Gaussian approximation analysis method is reasonably set as 6.4, corresponding to a failure probability of 10^{-10}. We simulate all results in this section based on the experimental parameters listed in Table 1.

Table 1. Simulation parameters for decoy-state BB84 QKD with and without the heralded QM.

η_b (%)	Y_0 (10^{-6})	e_d (%)	e_0	α (dB/km)	f
14.5	6.02	1.5	0.5	0.2	1.16

First, considering different η_{in} and η_{out}, we investigate the performance of decoy-state BB84 QKD with the heralded QM. For comparison purpose, we also investigate the performance of decoy-state BB84 QKD without QM. Here for simplicity, we assume η_{in} and η_{out} with the same value, *i.e.*, $\eta_{QM} = \eta_{in} = \eta_{out}$. Moreover, considering the storage efficiency of the state-of-art quantum memory can reached 92%,[9] we reasonable set $\eta_{QM} = 1, 0.8, 0.5$ in our simulations, corresponding simulation results are shown in Fig. 2. As shown in Fig. 2, with reasonable $\eta_{QM} < 1$,[9,33] the performance of BB84 with QM is slightly worse than that of without QM in short distance range; However, due to the heralding feature of QM, which can reduce the valid dark count rate of Bob's single photon detectors, the performance of BB84 QKD with QM is obviously better than that of BB84 without QM in long distance range.

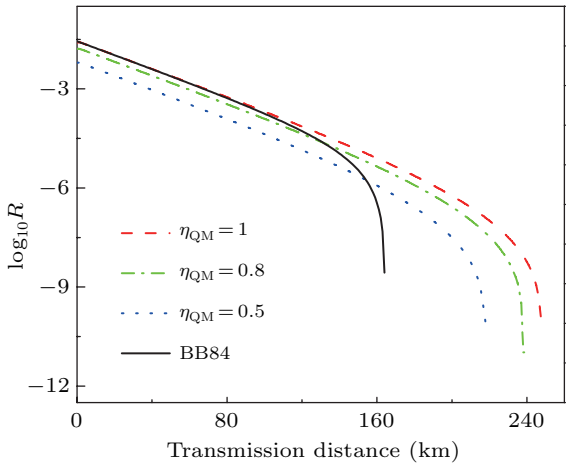


Fig. 2. Comparison between decoy-state BB84 QKD with and without QM.

Then, we study the effect of statistical fluctuations on decoy-state BB84 QKD with and without QM, and corresponding results are shown in Fig. 3. From Fig. 3, we can see that the performance of BB84 with and without QM degrades with the decrease of the total number of pulses N. However, due to the reduce of valid dark count rate by QM, the performance of BB84 with QM is still better than that of without QM.

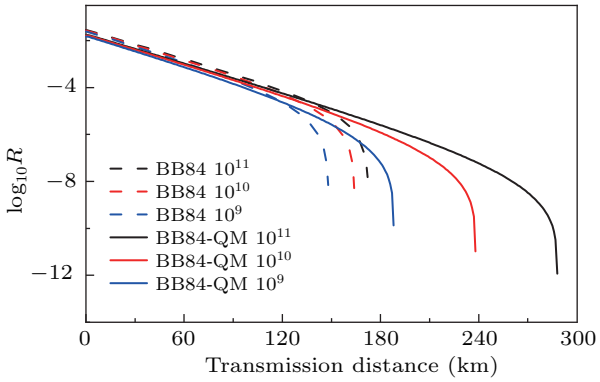


Fig. 3. Statistical fluctuations on decoy-state BB84 QKD without QM and with QM. Here, we reasonably set η_{QM} as 0.8.

5. Conclusion

In conclusion, we have investigated the performance of decoy-state BB84 QKD with a heralded QM. Due to the mitigation of the valid dark counts of Bob's single photon detectors, the transmission distance of decoy-state BB84 QKD can be greatly extended, which shows the feasibility of adopting QM in practical QKD systems. Furthermore, our present method can also be extended to the measurement-device-independent quantum key distribution (MDI-QKD) protocol, and it could show even more interesting characteristics. We believe our work will provide a valuable reference for researchers both in QKD and QM.

Acknowledgment

We thank Dr. Chun-Mei Zhang and Mr. Chen-Chen Mao for useful discussions.

References

[1] Bennett C H and Brassard G 1984 *Proceddings of the IEEE International Conference on Computers, Systems and Signal Processing*, 1999, Bangalore, India (IEEE, New York, 1984) p. 175
[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[3] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 *Rev. Mod. Phys.* **84** 621
[4] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[5] Boaron A, Boso G, Rusca D, Vulliez C, Autebert C, Caloz M, Perrenoud M, Gras G, Bussiéres F, Li M J, Nolan D, Martin A and Zbinden H 2018 *Phys. Rev. Lett.* **121** 190502
[6] Wang C, Song X T, Yin Z Q, Wang S, Chen W, Zhang C M, Guo G C and Han Z F 2015 *Phys. Rev. Lett.* **115** 160502
[7] Abruzzo S, Kampermann H and Bruß D 2014 *Phys. Rev. A* **89** 012301
[8] Novikova I, Walsworth R L and Xiao Y H 2012 *Laser Photon. Rev.* **6** 333
[9] Hsiao Y F, Tsai P J, Chen H S, Lin S X, Hung C C, Lee C H, Chen Y H, Chen Y F, Yu I A and Chen Y C 2018 *Phys. Rev. Lett.* **120** 183602
[10] Riedl S, Lettner M, Vo C, Baur S, Rempe G and Dürr S 2012 *Phys. Rev. A* **85** 022318
[11] Gündoğan M, Ledingham P M, Almasi A, Cristiani M and Riedmatten H D 2012 *Phys. Rev. Lett.* **108** 190504
[12] Saglamyurek E, Jin J, Verma V B, Shaw M D, Marsili F, Nam S W, Oblak D and Tittel W 2015 *Nat. Photon.* **9** 83
[13] Hosseini M, Sparkes B M, Campbell G, Lam P K and Buchler B C 2011 *Nat. Commun.* **2** 174
[14] Namazi M, Kupchak C, Jordaan B, Shahrokhshahi R and Figueroa E 2017 *Phys. Rev. Appl.* **8** 034023
[15] England D G, Fisher K A G, MacLean J P W, Bustard P J, Lausten R, Resch K J and Sussman B J 2015 *Phys. Rev. Lett.* **114** 053602
[16] Ledingham P M, Munns J H D, Thomas S E, Champion T F M, Qiu C, Kaczmarek K T, Feizpour A, Poem E, Walmsley I A, Nunn J and Saunders D J 2016 *Phys. Rev. Lett.* **116** 090501
[17] Namazi M, Vallone G, Jordaan B, Goham C, Shahrokhshahi R, Villoresi P and Figueroa E 2017 *Phys. Rev. Appl.* **8** 064013
[18] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[19] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev. A* **51** 1863
[20] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[21] Wang Q, Wang X B and Guo G C 2007 *Phys. Rev. A* **75** 012312
[22] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[23] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[24] Zhang C H, Luo S L, Guo G C and Wang Q 2015 *Phys. Rev. A* **92** 022332
[25] Duan L M, Lukin M, Cirac L and Zoller P 2001 *Nature* **414** 413
[26] Dou J P, Yang A L, Du M Y, Lao D, Gao J, Qiao L F, Li H, Pang X L, Feng Z, Tang H and Jin X M 2018 *Commun. Phys.* **1** 55
[27] Duan L M, Cirac J I and Zoller P 2002 *Phys. Rev. A* **66** 023818
[28] Gujarati T P, Wu Y K and Duan L M 2018 *Phys. Rev. A* **97** 033826
[29] Wang Q, Zhang C H and Wang X B 2016 *Phys. Rev. A* **93** 032312
[30] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Proceedings International Symposium on Information Theory (ISIT)*, 2004. p. 136
[31] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[32] Wang Q, Chen W, Xavier G, Swillo M, Zhang T, Sauge S, Tengner M, Han Z F, Guo G C and Karlsson A 2008 *Phys. Rev. Lett.* **100** 090501
[33] Sabooni M, Li Q, Kröll S and Rippe L 2013 *Phys. Rev. Lett.* **110** 133604