Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution

Zhengyu Li[1,2], Yichen Zhang[3], Xiangyu Wang[3], Bingjie Xu[2], Xiang Peng[1], and Hong Guo[1*]
[1] *State Key Laboratory of Advanced Optical Communication Systems and Networks, Center for Computational Science & Engineering (CCSE) and Center for Quantum Information Technology, School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China*
[2] *Science and Technology on Security Communication Laboratory, Institute of Southwestern Communication, Chengdu 610041, China and*
[3] *State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China*
(Dated: November 12, 2015)

Photon subtraction operation can enhance the performance of continuous-variable quantum key distribution (CV QKD). However, the enhancement will be reduced by the imperfections of single-photon detector, especially the non-unit detection efficiency, which makes it not practical. In this paper, we propose a *non-Gaussian* postselection method that can emulate the photon subtraction used in CV QKD protocols using coherent states, including subtracting more than 1 photons. The *virtual* photon subtraction not only can avoid the complexity and inefficiency of a practical single photon detector, which extends secure transmission distance as the ideal case, but also its parameter can be adjusted flexibly according to the channel parameters to optimize the performance. Moreover, our preliminary tests about the information reconciliation suggest, for the non-Gaussian data generated by photon subtraction, that the reconciliation efficiency can still approach 0.95 via multi-dimensional reconciliation algorithm for low signal-to-noise ratio regime, which implies the feasibility of practically implementing this *virtual* photon subtraction method.

PACS numbers: 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum key distribution (QKD) is the most applicable technology of quantum information, which can allow two users generate secure keys remotely through insecure quantum channel. Continuous-variable (CV) QKD [1, 2] is one of the two main branches of QKD, which has the advantage of being compatible with standard telecommunication technology, thus leads to an expectation of better application. However, limited by the practical experimental techniques and non-unit reconciliation efficiency, the transmission distances of early CV QKD experiments were not sufficiently long for network applications. Therefore, towards the practical implementation, researches on extending transmission distance have attracted much attention.

Beside the improvement of experimental techniques [3], additional operations, for instance, noiseless linear amplification (NLA) [4] and photon subtraction (PS) [5], were also introduced to improve the performance of CV QKD. Although photon subtraction is a non-Gaussian operation, it can significantly improve the transmission distance when applied in protocols using two-mode squeezed vacuum (TMSV) as the source [6]. However, the improvement will be reduced by the imperfections of single-photon detector (SPD), especially when using a non-photon-number-resolving detector such as an avalanche photodiode (APD) based SPD.

Here, we propose a *non-Gaussian* postselection method that can emulate the photon substraction used in CV QKD protocols using coherent states, which is operated in Alice's station right before the emission of coherent states. The *virtual* photon subtraction can remove the complex physical operation, therefore, it is unaffected by practical devices' imperfections. Furthermore, it can be adjusted flexibly according to the channel parameters to optimize the performance. Moreover, our preliminary tests about the information reconciliation suggest that for the non-Gaussian data generated by photon subtraction the reconciliation efficiency can still approach 0.95 via multi-dimensional reconciliation algorithm for low signal-to-noise ratio regime. Thus, we can practically use this method to extend the secure transmission distance of CV QKD.

II. VIRTUAL PHOTON SUBTRACTION VIA NON-GAUSSIAN POSTSELECTION

Here we briefly introduce some basics of photon subtraction. In Alice's part of Fig. 1(a), photon subtraction is applied to the TMSV source. After the beamsplitter (BS1), with transmittance T, the mode B is splitted into modes B_1 and B_2, getting a tripartite state $\rho_{AB_1B_2}$. Then B_1 will be measured by a Positive Operator-Valued Measure (POVM) measurement $\{\hat{\Pi}_0, \hat{\Pi}_1\}$, and the modes A and B_2 will be kept only when the POVM element $\hat{\Pi}_1$ clicks. Different $\hat{\Pi}_1$ will lead to different type of photon subtraction. What we discuss here is subtracting k

*Corresponding author: hongguo@pku.edu.cn

photons, which refers to $\hat{\Pi}_1 = |k\rangle\langle k|$.

Because Alice's heterodyne detection and the POVM measurement $\{\hat{\Pi}_0, \hat{\Pi}_1\}$ are conducted on two different modes, they are commutable. Thus, Alice can perform the heterodyne detection on mode A first, and then the POVM measurement on mode B_1. It is known that heterodyne detection on one mode of TMSV state will project the other mode onto a coherent state. After BS1 the state of modes B_1 and B_2, given that Alice's heterodyne measurement results are $\{x_A, p_A\}$, is $\left|\varphi^{(x_A,p_A)}\right\rangle_{B_1B_2} = \left|\sqrt{1-T}\alpha\right\rangle_{B_1}\left|\sqrt{T}\alpha\right\rangle_{B_2}$, where $\alpha = \sqrt{2}\lambda\left(x_A - ip_A\right)/2$. The success probability of subtracting k photons will be the function of $\{x_A, p_A\}$, which is

$$\begin{aligned} &P^{\hat{\Pi}_1}\left(k|x_A,p_A\right) = \left|\left\langle k \mid \sqrt{1-T}\alpha\right\rangle\right|^2 \\ &= \exp\left[-\tfrac{(1-T)\lambda^2}{2}\left(x_A^2+p_A^2\right)\right]\cdot\left[\tfrac{(1-T)\lambda^2}{2}\left(x_A^2+p_A^2\right)\right]^k \Big/ k! \end{aligned} \tag{1}$$

Thus the mixed state output from Alice's station will be

$$\rho_{B_2}^{(k)} = \int dx_A dp_A \underbrace{\frac{P^{\hat{\Pi}_1}\left(k|x_A,p_A\right)}{P^{\hat{\Pi}_1}\left(k\right)}}_{\text{weighting function}} P_{x_A,p_A}\left|\sqrt{T}\alpha\right\rangle\left\langle\sqrt{T}\alpha\right|, \tag{2}$$

where $P_{x_A,p_A} = \frac{1}{\pi(V+1)}\exp\left(-\frac{x_A^2+p_A^2}{V+1}\right)$ is the Gaussian distribution of Alice's heterodyne measurement results, and $V = \left(1+\lambda^2\right)/\left(1-\lambda^2\right)$ is the variance of the TMSV state.

Comparing to the case where Alice does not use any kinds of photon subtraction operations, whose output mixed state is

$$\rho_B^{(G)} = \int dx_A dp_A P_{x_A,p_A}\left|\alpha\right\rangle\left\langle\alpha\right|, \tag{3}$$

there are two differences. The first is that there is an additional weighting function in Eq.(2) that $W = P^{\hat{\Pi}_1}\left(k|x_A,p_A\right)\Big/P^{\hat{\Pi}_1}\left(k\right)$, which leads to a filter function, or acceptance probability, of each pair of (x_A, p_A),

$$Q\left(\gamma,\lambda,T\right) = P^{\hat{\Pi}_1}\left(k\right)W = P^{\hat{\Pi}_1}\left(k|x_A,p_A\right). \tag{4}$$

The second is that the output coherent state needs to go through a BS with transmittance T, which can be emulated via generating a coherent state with a smaller mean value $\sqrt{T}\alpha$.

Thus, after changing the way to look at the protocol by exchanging Alice's two commutable measurements, we get the equivalent *virtual* photon subtraction via postselection of Alice's heterodyne results and scaling the mean value of output coherent state by a factor $\sqrt{T}$. The postselection filter function is Eq.(4). Since Alice reveals her decision of accepting each data or not after Bob's measurement, the discarded part can be seen as the decoy states, as in another non-Gaussian protocol [7].

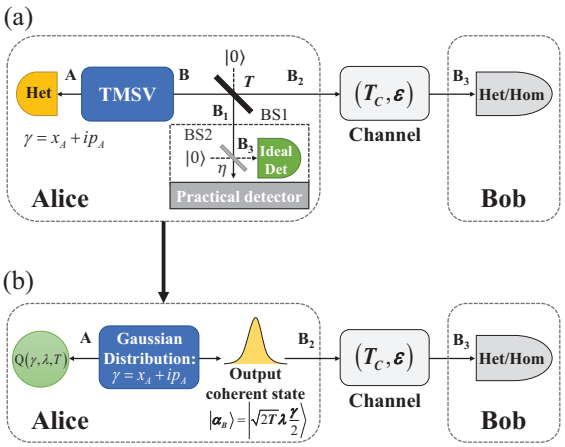


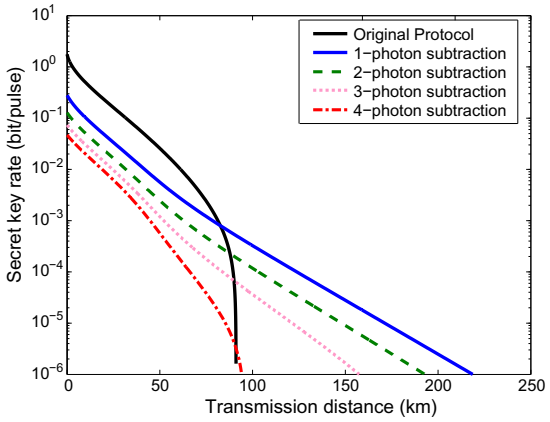
FIG. 1: (color online)(a) Entanglement-based (EB) scheme of CV QKD with photon subtraction. (b) Prepare-and-measure (PM) scheme of CV QKD with *virtual* photon subtraction. Other notations: Het: heterodyne detection. Hom: homodyne detection. BS1(2): beamsplitter. γ: Alice's measurement result. λ: parameter of TMSV. $Q\left(\gamma,\lambda,T\right)$: postselection filter function. $T(\eta)$: transmittance of BS1(2). T_C, ε: channel parameters

III. PERFORMANCE OF THE PROTOCOLS

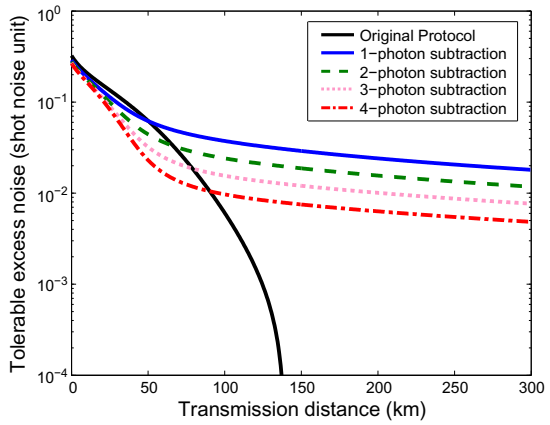
For simplicity, we only consider the asymptotic rate here. Although the state $\rho_{AB_3}^{\hat{\Pi}_1}$ is non-Gaussian, according to Gaussian optimality theorem [8], its secret key rate is no less than a Gaussian state $\rho_{AB_3}^{G}$ who has the same covariance matrix with it, that $K(\rho_{AB_3}^{\hat{\Pi}_1}) \geq K(\rho_{AB_3}^{G})$. Thus we will use $\rho_{AB_3}^{G}$ to do the security analysis for the rest of the paper. Besides, the success probability of Alice's POVM measurement $P^{\hat{\Pi}_1}$ should also be taken into account.

For the *virtual* k-photon subtraction, the transmittance T of Alice's BS can be chosen arbitrarily from 0 to 1, which will result in different secret key rates. Thus, there exists an optimal choice of T for each distance. In Fig. 2, (a) shows the maximal secret key rate at each distance, and (b) shows the maximal tolerable excess noise at each distance, for all possible T. Fig. 2 suggests that by using photon subtraction the performance will outperform the original protocol at long distance range, which implies the advantage of extending the maximal transmission distance. Fig. 2 also shows that the 1-photon subtraction has the longest transmission distance than other cases. Besides, when channel is more clean, all four photon subtraction operations will expand the maximal transmission distance more than 200km.

Another thing one may concern about is that, when implementing photon subtraction, whether the information reconciliation step would still remain a relatively high efficiency as for the Gaussian data. We have carried a preliminary test on the performance of multi-dimensional reconciliation method, proposed in [9], on both using 1-



(a)



(b)

FIG. 2: (a) The maximal secret key rate and (b) the maximal tolerable excess noise at each transmission distance when changing the transmittance T of Alice's BS, in which the original GG02 protocol (black solid line), and 1-photon subtraction (blue solid line), 2-photon subtraction (green dashed line), 3-photon subtraction (pink dotted line), and 4-photon subtraction (red dash-dotted line) photons, respectively. Other simulation parameters are: the variance of TMSV state is $V = 20$, channel loss is 0.2dB/km, excess noise is 0.01, and reconciliation efficiency is $\beta = 0.95$.

photon subtraction and not using any photon subtraction cases (non-Gaussian and Gaussian cases, respectively) with simulated data, assuming Binary Input Additive White Gaussian Noise Channel (BIAWGNC). Table I shows that the multi-dimensional reconciliation method shows a similar performance on both non-Gaussian and Gaussian cases, given the same signal-to-noise ratio (SNR). From Table I, when considering a high reconciliation efficiency like 0.95, the 0.02 rate check matrix still shows a relatively high successful decoding probability, i.e., more than 60%. This implies the feasibility of practically implementing this equivalent *virtual* photon subtraction method we proposed here.

	SNR	β	Type	S/T	AIN
R=0.1	0.1626	92.02%	Gaussian	39/40	103
			Non-Gaussian	40/40	82
	0.1613	92.71%	Gaussian	33/40	134
			Non-Gaussian	40/40	102
	0.1600	93.40%	Gaussian	20/40	151
			Non-Gaussian	34/40	130
R=0.02	0.0301	93.37%	Gaussian	47/48	111
			Non-Gaussian	47/48	101
	0.0296	94.97%	Gaussian	37/48	190
			Non-Gaussian	37/48	174
	0.0293	95.94%	Gaussian	18/48	157
			Non-Gaussian	33/48	178

TABLE I: Performance comparison of multi-dimensional reconciliation method between Gaussian and non-Gaussian data. R: the rate of sparse check matrix. SNR: signal-to-noise ratio. β: reconciliation efficiency. Type: the type of tested data. S/T: the number of successfully decoded data blocks/the number of total tested data block. AIN: average iteration number when decoding process succeeds.

IV. ACKNOWLEDGEMENT

This work is supported by the National Science Fund for Distinguished Young Scholars of China (Grant No. 61225003), the National Hi-Tech Research and Development (863) Program.

[1] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[2] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[3] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photonics **7**, 378 (2013).
[4] T. C. Ralph and A. P. Lund, arXiv: 0809.0326 (2008).
[5] C. Navarrete-Benlloch, R. García-Patrón, J. H. Shapiro, and N. J. Cerf, Phys. Rev. A **86**, 012328 (2012).
[6] P. Huang, G. He, J. Fang, and G. Zeng, Phys. Rev. A **87**, 012317 (2013).
[7] A. Leverrier and P. Grangier, Phys. Rev. A **83**, 042312 (2011).
[8] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[9] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, Phys. Rev. A **77**, 042325 (2008).