Unidimensional continuous-variable quantum key distribution

Vladyslav C. Usenko[*]
Department of Optics, Palacký University, 17. listopadu 50, 772 07 Olomouc, Czech Republic and
Bogolyubov Institute for Theoretical Physics of National Academy of Sciences, Metrolohichna st. 14-b, 03680, Kiev, Ukraine

Frédéric Grosshans[†]
Laboratoire de Photonique Quantique et Moléculaire, ENS Cachan, UMR CNRS 8537, F-94235 Cachan, France and
Laboratoire Aimé Cotton, CNRS, Université Paris-Sud and ENS Cachan, F-91405 Orsay, France

We propose the continuous-variable quantum key distribution protocol based on the Gaussian modulation of a single quadrature of the coherent states of light, which is aimed to provide simplified implementation compared to the symmetrically modulated Gaussian coherent-state protocols. The protocol waives the necessity in phase quadrature modulation and the corresponding channel transmittance estimation. The security of the protocol against collective attacks in a generally phase-sensitive Gaussian channels is analyzed and is shown achievable upon certain conditions. Robustness of the protocol to channel imperfections is compared to that of the symmetrical coherent-state protocol. The simplified unidimensional protocol is shown possible at a reasonable quantitative cost in terms of key rate and of tolerable channel excess noise.

Technical paper : arXiv:1504.07093

I. INTRODUCTION

Quantum key distribution (QKD) ensures the security of a secret key through the very nature of quantum states distributed between trusted parties. Recent developments in this field are concerned with the continuous-variables (CV) coding of key bits, [1–11] in particular, the Gaussian modulation of coherent states of light [6–10] is promising experimentally [9, 10]. The main goal of the present paper is to propose a further simplification of these coherent state protocols.

In particular, almost all published coherent-state protocols suppose a symmetrical amplitude and phase quadrature modulation. In the present paper we propose the unidimensional (UD) CV QKD protocol based on the Gaussian single-quadrature modulation, which reduces the experimental needs of the emitter to a single intensity modulator, instead of both a phase and an intensity modulator. Our paper thus continues the tendency of technical simplification of the QKD protocols which was started in [12], where low cost and compact discrete variable QKD system was proposed.

II. UNIDIMENSIONAL PROTOCOL

The central idea of the protocol is to modulate a single quadrature of coherent states. This should provide simplified implementation, at the price of slightly degraded performances, as we show below. One of the trusted sides, Alice, produces coherent states, and then modulates one of the quadratures (x), displacing each coherent state according to a random Gaussian variable of variance V_M. The mixture of the modulated states thus forms a "sausage" on a phase-space [see Fig. 1 (a)]. The states are then sent to the remote trusted party Bob through a generally phase-sensitive channel. Bob performs homodyne measurement of the modulated quadrature, measuring most of the time the x-quadrature, and sometimes measuring the p-quadrature. After sufficient number of runs, Alice and Bob analyze the security from both quadrature statistics and extract a secret key from the x-quadrature data.

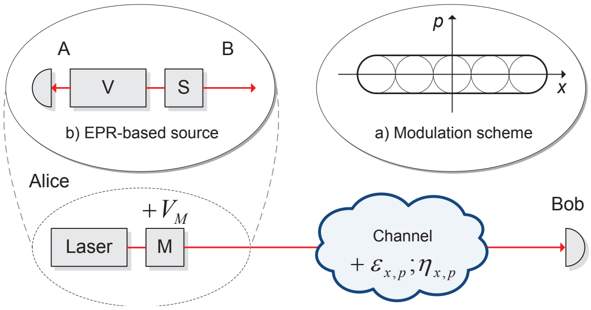

FIG. 1. (Color online) Scheme of the UD coherent-state protocol. Alice prepares a coherent state using a laser source and displaces it along the x-quadrature using modulator M. The states travel through an untrusted, generally phase-sensitive, channel to a remote party Bob, who performs homodyne measurement of the x-quadrature. (a) Mixture of modulated coherent states on a phase-space. (b) Equivalent entanglement-based scheme using a two-mode squeezed vacuum source, mode A is measured by Alice using a homodyne detector, mode B is squeezed on the squeezer S and sent to channel.

III. SECURITY OF THE PROTOCOL

We compute the asymptotic secret key rate of our protocol against collective attacks. The optimality of Gaussian attacks [14, 15] allows us to use well known formulas to compute the secret key rate from the covariance matrix.

To analyze the security of the protocol we switch to the equivalent entanglement-based (EPR) scheme. For the UD protocol such scheme can be built, by taking a two-mode

[*] usenko@optics.upol.cz
[†] frederic.grosshans@u-psud.fr

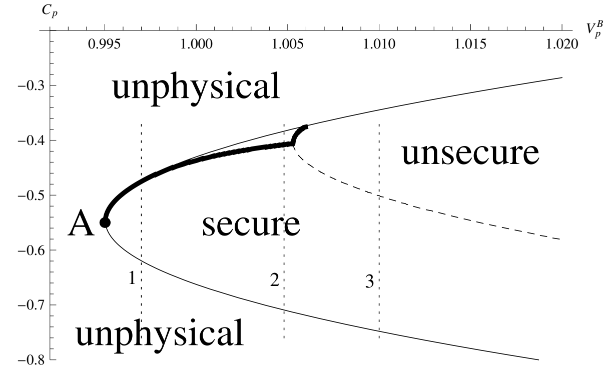

FIG. 2. Physicality (solid line) and security (dashed line) regions of the UD protocol. The pessimistic value of C_p, which minimizes the key rate, is given as a bold solid line. Modulation variance $V_M = 10$, channel transmittance in x: $\eta_x = 0.1$, noise in x: $\epsilon_x = 5\%$ SNR. A is the vertex of the parabola. The lines 1, 2 and 3 correspond to the key rate dependencies given in Fig. 3.

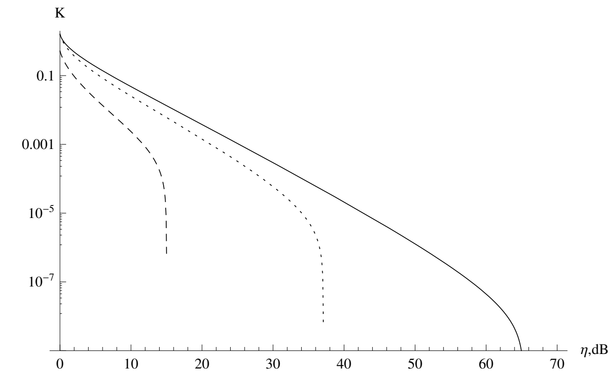

FIG. 4. Typical dependence of the key rate on loss (in dB scale) upon symmetric channel excess noise $\epsilon = 5\%$ SNU. Solid line: symmetrical coherent protocol; dashed-line: UD protocol with correlation estimation in p; dotted line: UD protocol without correlation estimation in p. Modulation variance $V_M = 100$.

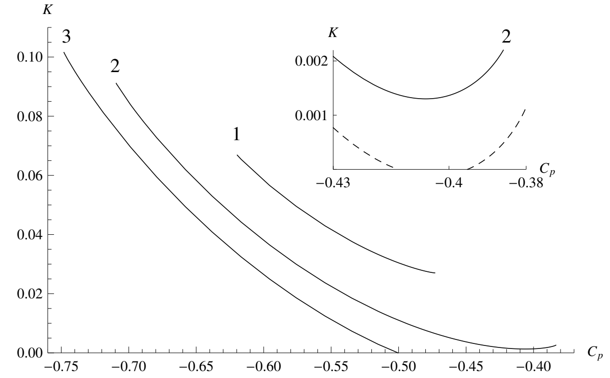

FIG. 3. Key rate secure against collective attacks versus correlation C_p for different values of variance V_p^B, corresponding to the lines 1, 2 and 3 in Fig. 2. Inset demonstrates the dependence of line 2 in the smaller scale. For comparison the line corresponding to $V_p^B = 1.00535$ is given as dashed, demonstrating the particular case when the security is lost and then restored.

squeezed vacuum state of variance V and squeezing one of its modes with the squeezing parameter $-\log\sqrt{V}$, giving us an initial covariance matrix.

As the states travels through the untrusted channel, the covariance matrix is transformed. However, since there is no modulation in the p quadrature, the correlation in p cannot be estimated. Bob only measures the variance V_p of the channel output in p, and the parameter $C_p = \langle p_A p_B \rangle$ of the covariance matrix is unknown, which prevents a direct computation of the key rate K.

However, this unknown parameter is bounded by the Heisenberg uncertainty principle, which bounds the possible covariance matrices [13]. It therefore imposes physical constraints on C_p; the only allowed values being inside a parabola in the $\{V_p^B, C_p\}$ plane. One can also analytically derive the lower bound on the key rate and find the security bounds in terms of unknown correlation C_p upon given (measured) V_p^B. The corresponding physicality and security regions in terms of C_p are shown on Fig. 2.

It is evident from the graph, that there exists a region of V_p^B, where the protocol is secure for any C_p. In this region, no physically valid collective attack can break the security. For higher values of V_p^B the protocol cannot be implemented, since it would only be secure for some values of C_p, but Alice and Bob cannot estimate the latter quantity. Such a behavior can be clearly observed at the graphs in Fig. 3. When the channel excess noise $\epsilon_x > 0$ increases, the physicality region expands, which allows Eve to perform stronger attacks.

Counter-intuitively, the key rate is not always a monotonous function of the correlation $|C_p|$. Indeed, it can be seen from Fig. 3 that upon certain values of variance V_p^B the lower bound on the key rate can have a local minimum within the security region. Moreover, the security can be even lost and restored (see the dashed line at the inset in Fig. 3).

However, when the channel excess noise in p is small, the key rate is a monotonous function of the correlation $|C_p|$ (as can be also seen in Fig. 3) in most of the physicality region, and the pessimistic value for C_p is typically the highest physically valid negative value $C_p^{\max}$.

As the noise increases, the pessimistic value of C_p gets lower than $C_p^{\max}$ and must be found numerically. It is given as bold line in Fig. 2. In this case, a key rate computed at $C_p^{\max}$ is greater than the lower bound on the real key rate and is therefore too optimistic. However, even when the pessimistic value of C_p is inside the parabola, This upper bound, which can be computed analytically, is often a good approximation.

IV. PERFORMANCE FOR SYMMETRIC CHANNELS

In typical communication channels, one expects values of loss and excess noise in both quadratures to be symmetric. In the limit of strong modulation this bound on the key rate becomes

$$K^{\text{sym}}_{\substack{V_M\to\infty\\ \eta\ll 1}} \lesssim \left(\tfrac{1}{3} - \sqrt{2\epsilon}\right)\eta\log e$$

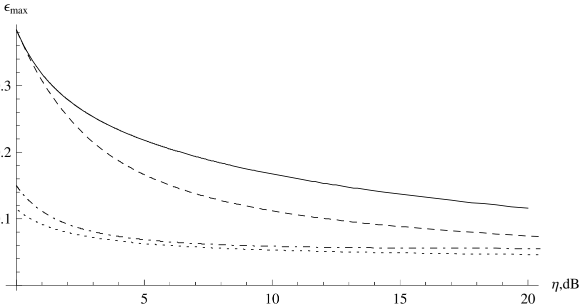

FIG. 5. Typical profile of the security region in terms of maximal tolerable channel excess noise ϵ versus channel loss (in dB scale). Solid line: symmetrical coherent protocol; dashed-line: UD protocol with channel estimation in p; dotted line: UD protocol without channel estimation in p; dot-dashed line: optimistic evaluation of UD protocol without channel estimation in p assuming $C_p = C_p^{max}$. Modulation variance $V_M = 100$.

This equation describes well the the key rate if the losses or noise in the channel are low, otherwise providing a rough upper bound.

We now compare the UD CV QKD protocol with the standard symmetrical modulation protocol GG02 [6, 7, 14, 15] used over the same channel. We first assume a noiseless lossy channel, where $\epsilon = 0$. In this case, C_p is known, and the exact key rate for our protocol can be computed. For $V_M \to \infty$, in the low transmission limit rate is $\frac{\eta}{3}\log e$, slightly smaller than the key rate of the standard coherent-state protocol ($\frac{\eta}{2}\log e$) [16].

In the general case, however, the channel noise reduces the security of the protocol. The results of the calculations in this case are given in Fig. 4 in terms of key rate upon fixed channel excess noise and in Fig. 5 in terms of the maximum tolerable channel excess noise versus channel loss. Evidently, the UD protocol demonstrates higher sensitivity to channel excess noise, which is the cost of technical simplification, but still provides a reasonable security region in terms of channel excess noise. The approximation $C_p := C_p^{max}$ is given as the dot-dashed line in Fig. 5.

For the sake of comparison we also analyzed the protocol, in which no information is extracted from p-quadrature, but some modulation and measurement is performed to estimate the channel the correlation in p. This intermediate protocol lays in between the symmetrical and completely asymmetrical counterparts, but requires modulation in both quadratures. It main interest it theoretical, since it allows to split the origin of the performance degradation of our protocol compared to GG02 between the degradation due to the asymmetric modulation and the one due to incomplete channel estimation.

V. SUMMARY AND CONCLUSIONS

We have proposed and investigated the unidimensional continuous-variable quantum key distribution protocol based on the Gaussian modulation of a single quadrature of coherent states of light, in which physicality bounds enable to limit the eavesdropping attacks and assess the security region. The protocol allows simpler technical realization with no need of phase quadrature modulation and full channel estimation at the cost of lower key rate and higher sensitivity to channel excess noise, compared to symmetrical coherent-state protocol. However, the performance of the protocol is still comparable to that of the symmetrical counterpart and allows for the practical implementation.

ACKNOWLEDGMENTS

The work of VCU was supported by the Project No. 13-27533J of the Czech Science Foundation and by the EU FP7 Project BRISQ2 under Grant Agreement No. 308803, co-financed by MSMTČR (7E13032). The work of FG was supported by the ANR-NSERC ANR-09-BLAN-0410-02 FReQueNCy project.

[1] C. Weedbrook *et al.*, Rev. Mod. Phys. **84**, 621 (2012).
[2] F. Furrer, *et al.*, Phys. Rev. Lett. **109**, 100502 (2012).
[3] F. Furrer, Phys. Rev. A 90, 042325 (2014).
[4] L. S. Madsen, *et al.*, Nature Communication **3**, 1083 (2012).
[5] T. Gehring, *et al.*, arXiv:1406.6174.
[6] F. Grosshans and Ph. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[7] F. Grosshans and Ph. Grangier, Proceedings of QCMC 6 arXiv.org:quant-ph/0204127 (2002).
[8] A. M. Lance, *et al.*, Phys. Rev. Lett. **95**, 180503 (2005)
[9] P. Jouguet, *et al.*, Nat. Photonics 7, 378 (2013)
[10] P. Jouguet, D. Elkouss, and S. Kunz-Jacques, Phys. Rev. A **90**, 042329 (2014)
[11] Y.-B. Zhao, M. Heid, J., and N. Lütkenhaus
[12] J. L. Duligall, *et al.*, New J. Phys. **8**, 249 (2006)
[13] A Serafini, J. Opt. B, 7, R19 (2005)
[14] M. Navascues, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006)
[15] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006)
[16] F. Grosshans, Phys. Rev. Lett. **94**, 020504 (2005)