Proof-of-principle test of continuous-variable quantum key distribution in free-space atmospheric channel

Vladyslav C. Usenko,[1,*] Christian Peuntinger,[2,3] Ivan Derkach,[1] Bettina Heim,[2,3,4] Christoph Marquardt,[2,3,4] Radim Filip,[1] and Gerd Leuchs[2,3,4]

[1]*Department of Optics, Palacký University, 17. listopadu 50, 772 07 Olomouc, Czech Republic*
[2]*Max Planck Institute for the Science of Light, Günther-Scharowsky-Str. 1 / Bldg 24, 91058 Erlangen, Germany*
[3]*Institute of Optics, Information and Photonics, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Staudtstr. 7/B2, 91058 Erlangen, Germany*
[4]*Erlangen Graduate School in Advanced Optical Technologies (SAOT), FAU, Paul-Gordan-Str. 6, 91052 Erlangen, Germany*

We study the applicability of the continuous-variable quantum key distribution (CV QKD) protocol based on the Gaussian modulation of coherent states of light in the free-space atmospheric channels. We show that the transmittance fluctuations (also referred to as fading) result in the excess noise, which must be considered untrusted and therefore limits the security. We show that such excess noise due to fading depends on the variance of the modulated signal and so the modulation must be optimized in the free-space implementations of CV QKD. We then split the overall transmittance distribution to sub-channels with relatively stable transmittance and suggest the method of sub-channels post-selection so that only the data from particular highly transmitting and properly estimated sub-channels contribute to the key rate. We show that such method enables the coherent-state CV QKD in the strongly fluctuating free-space channels, but must be optimized taking into account the success probability. We also study and confirm the stability of the method with respect to the finite-size effects and imperfect channel estimation. Finally, we report the proof-of-principle test of coherent-state CV QKD in the mid-range free-space atmospheric channel and confirm the positive role of sub-channel post-selection, which improves the secure key rate of the protocol. Our result is promising for the future free-space realizations of CV QKD including extra-terrestrial long-distance satellite links.

PACS numbers:

I. INTRODUCTION

Quantum key distribution (QKD) [1] is well known to have it's goal in the development of methods (protocols) allowing two legitimate users to share a secure key, which could be lately used for confidential communication using methods of classical cryptography (such as one-time pad cryptosystem). After being first proposed and realized on the basis of single qubits (represented by photons or weak coherent pulses) or entangled qubit pairs, QKD was lately extended to the realm of continuous-variable (CV) states defined on the infinite-dimensional Hilbert spaces and realized by multiphoton quantum states or entangled two-mode states of light.

Two main families of CV QKD protocols were proposed and realized based on squeezed [2] or coherent [3] states and Gaussian modulation so that security against optimal Gaussian collective attacks is accessible due to extremality of Gaussian states [4]. It was a particularly important step in the development of CV QKD, when the coherent-state protocol was shown secure upon any fixed channel attenuation and the use of reverse information reconciliation [3]. However, in the free-space atmospheric channels fixed attenuation is practically never the case since atmospheric effects such as turbulence lead to the fluctuations of the transmission coefficient. At the same time such channels are of the particular importance as they waive the requirement on the existing communication infrastructure and require only the line of sight between the trusted stations. Moreover, the free-space channels are the key element of the truly long-distance extra-terrestrial quantum communication through a satellite. Thus in the current work we report the study of the security of Gaussian CV QKD protocols and the stability of Gaussian entanglement over the fluctuating channels, which are also referred to as the fading channels. We show the threat to security due to the transmittance fluctuations but also suggest the solution based on the post-selection of sub-channels with lower fluctuations of transmittance. We also report the proof-of-principle test of Gaussian-modulated coherent-state CV QKD over a real fluctuating free-space channel and show that sub-channel post-selection enables the security of the protocol in such a link.

II. FREE-SPACE CV QUANTUM COMMUNICATION

We first consider the scheme of CV quantum communication where the trusted sender (Alice) uses the quadrature-entangled source with variance V and measures one of the modes with a heterodyne detector thus conditionally preparing the displaced coherent state. This is equivalent to the use of the laser source to which Alice applies Gaussian quadrature modulation by displacing the states on the phase space with modulation variance $\sigma = V - 1$. The modulated state travels through the fluctuating channel, described by a probability distribution of transmittance values $p_i(\eta_i)$, to the remote trusted party (Bob) who performs the homodyne measurement of the signal with an excess noise χ (which can be either trusted or untrusted). Thus, the scheme consists in the distribution and detection of a two-mode entangled state through

*Electronic address: usenko@optics.upol.cz

a fluctuating channel.

The Gaussian states can be explicitly described by the first and second moments of the quadratures of the respective modes, in particular by the covariance matrix of quadratures. The covariance matrix of the state transmitted through a fluctuating channel is governed by the mean values of transmittance, particularly $\langle\sqrt{\eta}\rangle$, which scales down the correlation terms, and $\langle\eta\rangle$, which defines the variance of the transmitted mode as $V\langle\sqrt{\eta}\rangle + 1 - \langle\sqrt{\eta}\rangle + \chi$. The channel is thus becoming equivalent to the fixed-type channel with transmittance $\langle\sqrt{\eta}\rangle^2$ and the modulation-dependent excess noise caused by transmittance fluctuations $\epsilon_f = Var(\sqrt{\eta})(V-1)$, where $Var(\sqrt{\eta}) \equiv \langle\eta\rangle - \langle\sqrt{\eta}\rangle^2$.

First we study the effect of fading on the Gaussian entanglement in terms of logarithmic negativity [5], and derive the bounds for the entanglement-breaking fluctuating channel. Then we consider security against individual and collective Gaussian attacks and show that fading channels can break the security of the Gaussian CV QKD already in case of individual attacks due to the modulation-dependent excess noise, resulting from transmission fluctuations. The states with the higher variance (i.e. stronger initial entanglement) appear to be more sensitive to the fluctuations of transmittance. We also assume the particular type of fluctuations caused by beam-wandering, which is the typical effect of turbulence in the mid-range free-space channels [6], where transmittance distribution is governed by the Weibull statistics, and perform the security analysis in this particular case. We show that the negative effect of fading can be partly compensated by increasing the ratio of the beam spot to the aperture size. This improvement is achieved by the cost of increasing the mean channel loss. Alternatively the transmittance fluctuations can be compensated in the general case using the post-selection of sub-channels.

III. POST-SELECTION OF SUB-CHANNELS

The post-selection of sub-channels is based on the possibility to estimate the channel and transmit at least one signal state during the stability window of a fluctuating channel. This is achievable when repetition rate of the source and detectors is much (orders of magnitude) higher than the frequency of transmittance changes. In particular, this is achievable with the current CV technology and the relatively slow atmospheric turbulence. The post-selection of sub-channels within a certain range is shown to be able to restore or improve the entanglement and security properties of Gaussian CV states due to the effective reduction of the transmittance fluctuations.

In the simplest case the sub-channel with the highest possible transmittance is post-selected at the cost of the very low probability of success. If however the probability of success is taken into account and the resulting key rate is weighted by such probability, the post-selection must be optimized to provide the highest key rate. Then a certain set of sub-channels should be post-selected [7].

We also address the finite-size effects in the CV QKD protocols, possibly caused by the data ensemble size reduction due to post-selection, and show the stability of our result upon the achievable sampling rates. In addition we show that the method is stable against the imperfect channel estimation.

IV. PROOF-OF-PRINCIPLE TEST

The proof-of-principle test of coherent-state CV QKD over the free-space atmospheric channel was performed at the Max-Planck Institute for the Science of Light in Erlangen, using the setup of free-space quantum communication with continuous variables [8], which was also recently used to distribute squeezed states through an atmospheric link [9]. The coherent states were produced by a laser system, modulated in amplitude and phase quadratures according to the Gaussian distributions with three different modulation variances, verified locally using heterodyne measurement, and then sent though the 1.6 km free-space atmospheric channel. On the remote side of the link the states were measured using another heterodyne detector, while the channel transmittance was monitored using the intensity measurements. On the data analysis stage, the covariance matrices of the states prepared by Alice and measured by Bob were reconstructed and the channel noise was estimated. The security analysis was performed using purification of the channel noise using the entangling cloner model to assess the upper bound on the information leakage, while the mutual information between the trusted parties was calculated directly on the measured data. The transmittance window was cut to the sub-channels with relatively stable loss and noise in each sub-channel was estimated, being lower than the noise in the overall dataset due to stabilization of channel fading. The lower bound on secure key rate was then obtained for the whole dataset (showing no QKD possible) as well as for the particular sets of sub-channels (showing the positive lower bound on the key rate for some of the sub-channels), and the optimal post-selection was found. It was shown that post-selection indeed restores and improves the security of the protocol and enables CV QKD with coherent states over the real mid-range atmospheric channel.

V. SUMMARY

In our work we consider the distribution of Gaussian entanglement and the Gaussian continuous-variable quantum key distribution over the fluctuating channels. We show that transmittance fluctuations reduce the entanglement and may lead to the security break. We suggest the method of sub-channels post-selection and show that it is able to restore the entanglement and the security properties of the Gaussian states. We also report the proof-of-principle experimental test which confirms the possibility to implement CV QKD in fluctuating free-space links and shows the improvement from the method of sub-channel post-selection. Our result thus opens a pathway towards implementation of long-distance CV QKD in free space including satellite links.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002); V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, Dušek M, N. Lütkenhaus and M. Peev, Rev. Mod. Phys. **81** 1301 (2009)

[2] M. Hillery, Phys. Rev. A **61** 022309 (2000); N. J. Cerf, M. Lèvy and G. Van Assche, Phys. Rev. A **63** 052311 (2001); L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, U. L. Andersen, Nature Communications **3**, 1083 (2012)

[3] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003); P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier and E. Diamanti, Nature Photonics **7**, 378 (2013)

[4] M. Navascués, F. Grosshans, and A. Acin, Phys. Rev. Lett. **97**, 190502 (2006); R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006)

[5] G. Vidal and R. F. Werner, Phys. Rev. A **65**, 032314 (2002)

[6] D. Y. Vasylyev, A. A. Semenov and W. Vogel, Phys. Rev. Lett. **108** 220501 (2012)

[7] V. C. Usenko, B. Heim, C. Peuntinger, C. Wittmann, C. Marquardt, G. Leuchs and R. Filip, New J. Phys. **14**, 093048 (2012)

[8] B. Heim, D. Elser, T. Bartley, M. Sabuncu, C. Wittmann, D. Sych, C. Marquardt, and G. Leuchs, Appl. Phys. B **98**, 635 (2010); B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, Ch. Marquardt, and G Leuchs, New J. Phys. **16**, 113018 (2014)

[9] C. Peuntinger, B. Heim, C. R. Müller, C. Gabriel, C. Marquardt, G. Leuchs, Phys. Rev. Lett. **113**, 060502 (2014)