Virtual noiseless amplification and Gaussian post-selection in continuous-variable quantum key distribution

Jaromír Fiurášek and Nicolas J. Cerf

Department of Optics, Palacký University, 17. listopadu 12, 77146 Olomouc, Czech Republic
QUIC, Ecole Polytechnique, CP 165/59, Universit\'e Libre de Bruxelles, 1050 Brussels, Belgium

european social fund in the czech republic
EUROPEAN UNION
MINISTRY OF EDUCATION, YOUTH AND SPORTS
OP Education for Competitiveness
INVESTMENTS IN EDUCATION DEVELOPMENT

Heralded probabilistic noiseless amplifier

Physical approximation to the unphysical target operation

$$|\alpha\rangle \rightarrow |g\alpha\rangle$$

Quantum filter diagonal in Fock basis:

$$\hat{G} = g^{\hat{n}} \qquad |n\rangle \rightarrow g^{n}|n\rangle \qquad g^{\hat{n}}|\alpha\rangle \propto |g\alpha\rangle$$

Motivation:

- Improved estimation and cloning of coherent states
- Entanglement distillation and concentration
- Breeding of Schrodinger cat-like states
- ***Compensation of losses in quantum communication***

T. C. Ralph and A. P. Lund, arXiv:0809.0326 (2008).

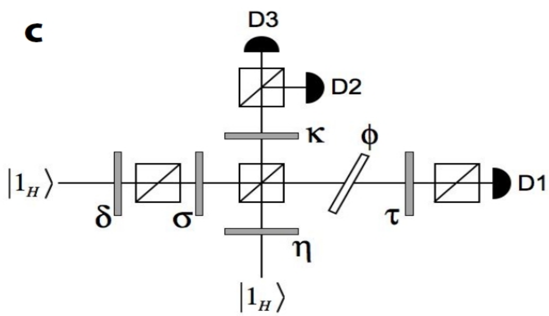
Experimental noiseless amplification

LETTERS
PUBLISHED ONLINE: 28 MARCH 2010 | DOI: 10.1038/NPHOTON.2010.35
nature photonics

Heralded noiseless linear amplification and distillation of entanglement

G. Y. Xiang[1], T. C. Ralph[2], A. P. Lund[1,2], N. Walk[2] and G. J. Pryde[1]*

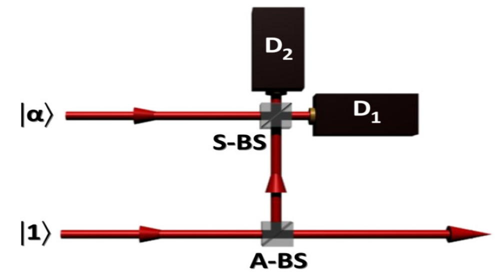
c



PRL 104, 123603 (2010) PHYSICAL REVIEW LETTERS week ending 26 MARCH 2010

Implementation of a Nondeterministic Optical Noiseless Amplifier

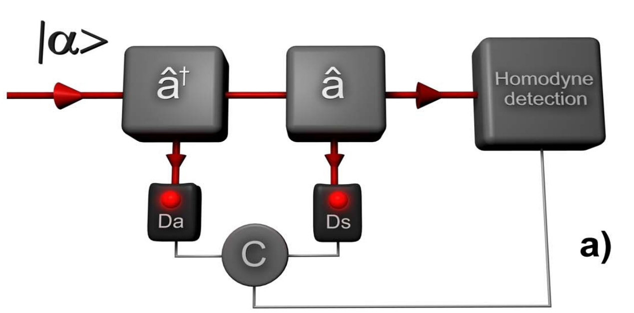
Franck Ferreyrol, Marco Barbieri, Rémi Blandino, Simon Fossier, Rosa Tualle-Brouri, and Philippe Grangier
Groupe d'Optique Quantique, Laboratoire Charles Fabry, Institut d'Optique, CNRS, Université Paris-Sud, Campus Polytechnique, RD 128, 91127 Palaiseau cedex, France
(Received 10 December 2009; published 24 March 2010)



nature photonics
ARTICLES
PUBLISHED ONLINE: XX XX 2010 | DOI: 10.1038/NPHOTON.2010.260

A high-fidelity noiseless amplifier for quantum light states

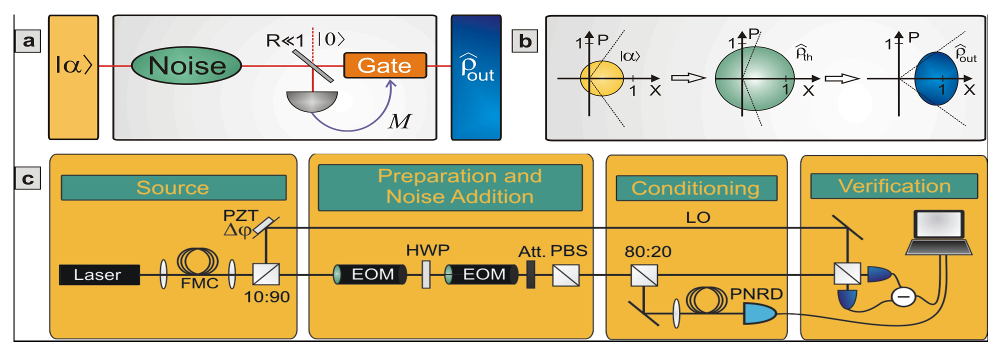
A. Zavatta[1,2], J. Fiurášek[3] and M. Bellini[1,2]*



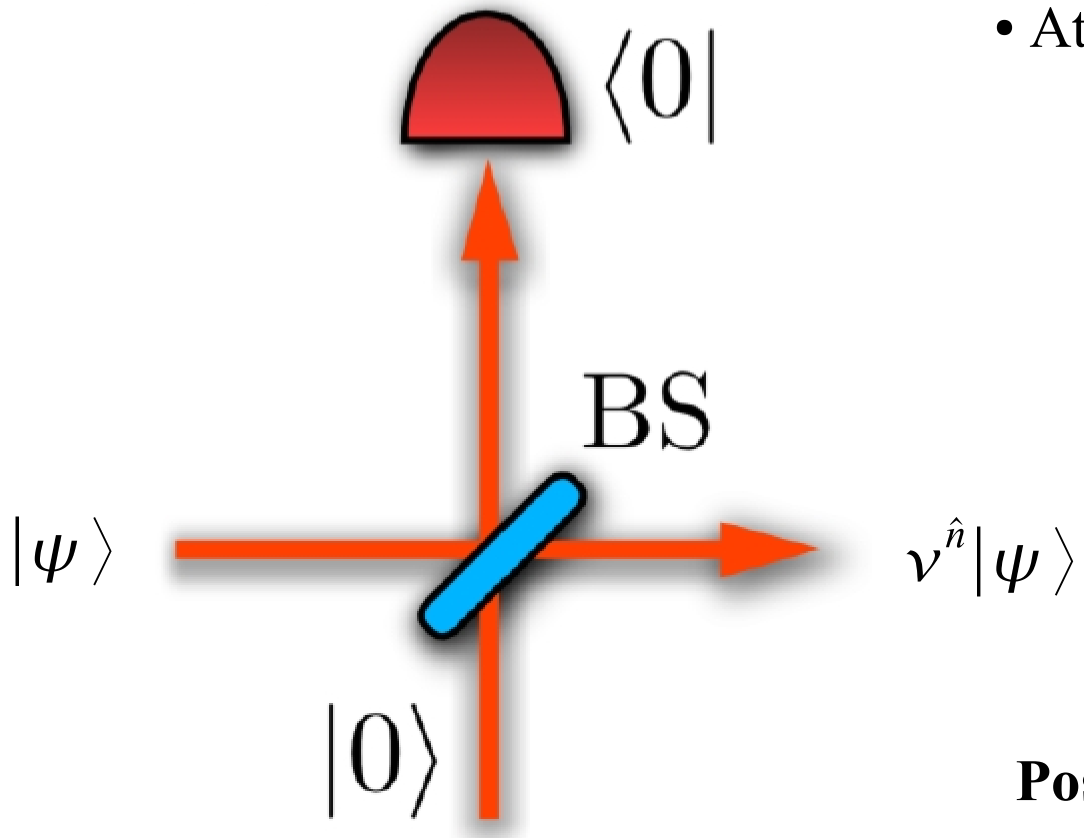
nature physics
LETTERS
PUBLISHED ONLINE: XX MONTH XXXX | DOI: 10.1038/NPHYS1743

Noise-powered probabilistic concentration of phase information

Mario A. Usuga[1,2†], Christian R. Müller[1,3†], Christoffer Wittmann[1,3], Petr Marek[4], Radim Filip[4], Christoph Marquardt[1,3], Gerd Leuchs[1,3] and Ulrik L. Andersen[2]*



Noiseless attenuation



- Quantum filter
- Attenuation of Fock state amplitudes

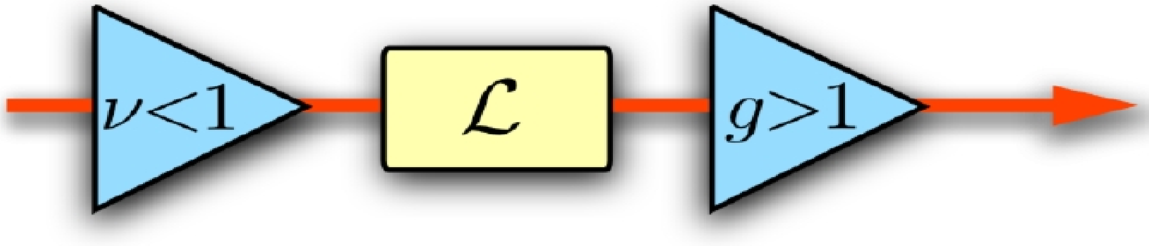
$$|n\rangle \rightarrow \nu^{n}|n\rangle \qquad \nu < 1$$

Possible implementation:

- Beam splitter with transmittance ν^2
- Projection onto vacuum

Suppression of losses in direct state transmission

$|\psi\rangle$



Input state in subspace spanned by vacuum and single-photon states:

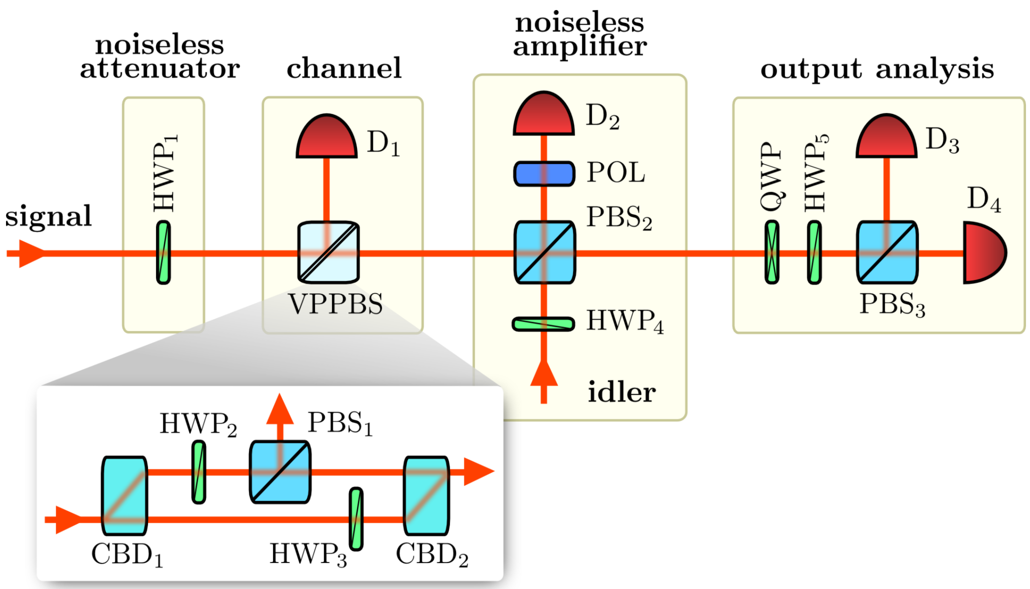
$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle$$

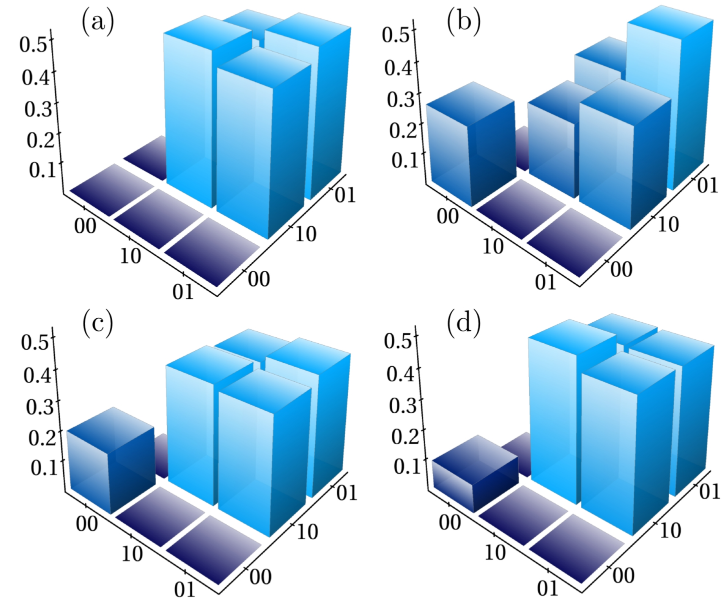
Lossy channel combined with noiseless attenuation and amplifcation, g=1/(ντ):

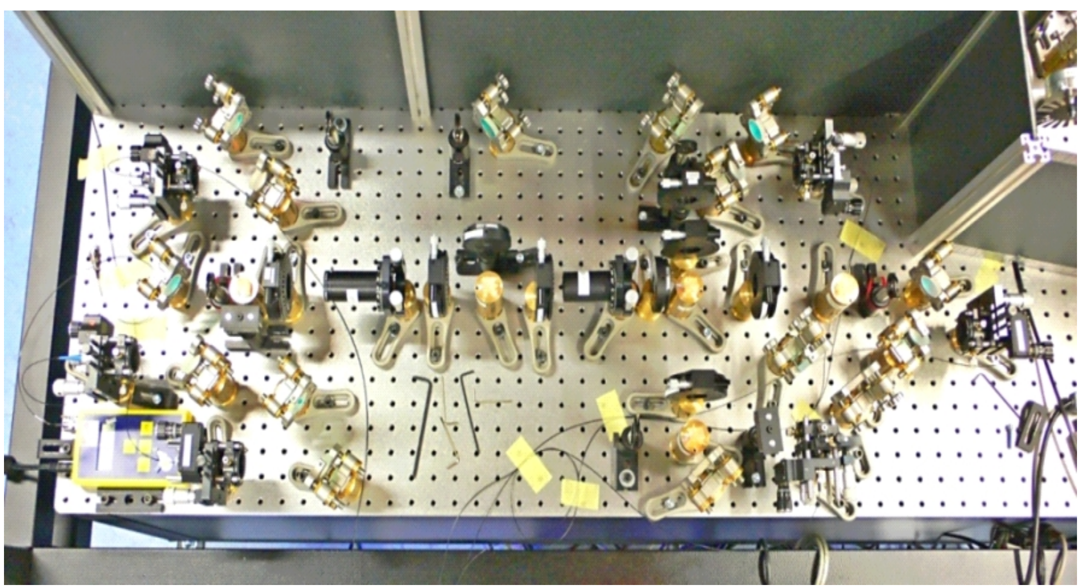
$$\rho = |\psi\rangle\langle\psi| + (1-\tau^2)\nu^2|c_1|^2|0\rangle\langle 0|$$

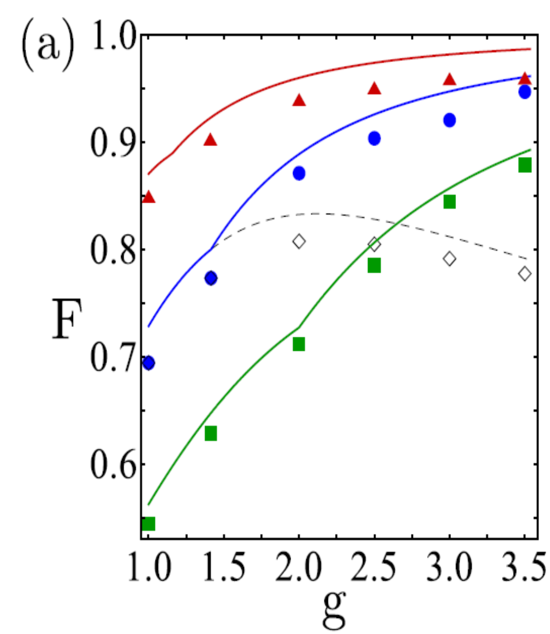
M. Mičuda, I. Straka, M. Miková, M. Dušek, N. J. Cerf, J. Fiurášek, and M. Ježek,
Noiseless Loss Suppression in Quantum Optical Communication, Phys. Rev. Lett. 109, 180503 (2012).

The experiment

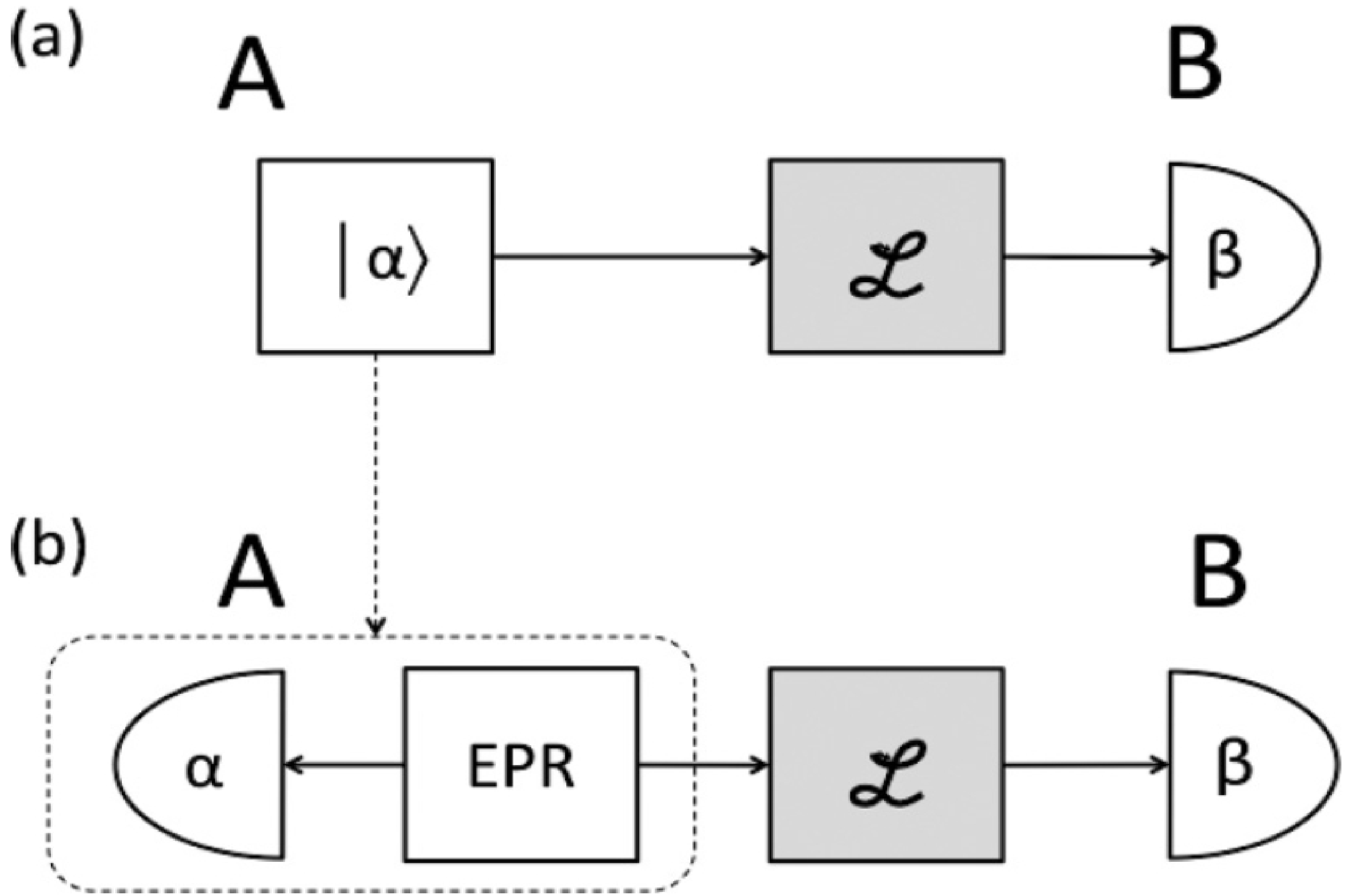








CV QKD with heterodyne detection

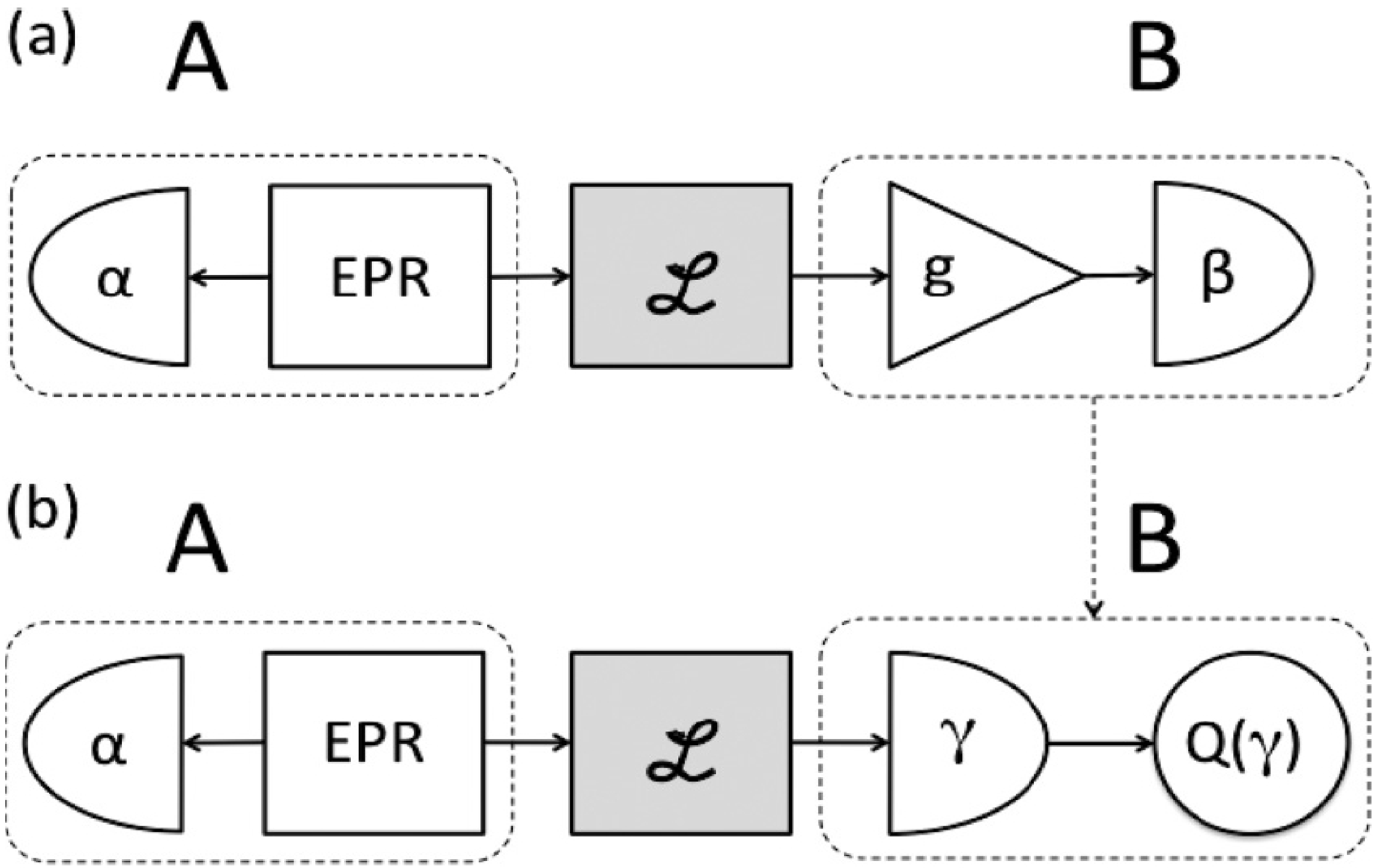


Alice prepares coherent states

Bob performs projection onto coherent states

$$|\Psi_{EPR}\rangle = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n |n\rangle|n\rangle$$

CV QKD augmented with noiseless amplification



Noiseless attenuation at the input is equivalent to a suitable choice of λ.

Noiseless amplification can be emulated on the measured data.

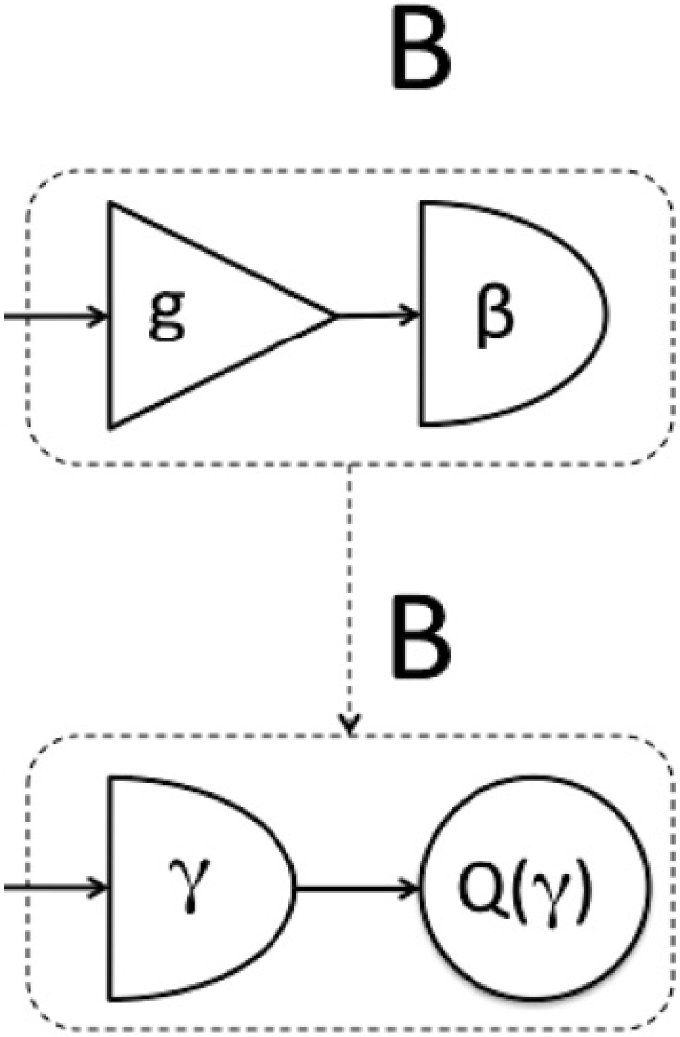
Emulation of noiseless amplification by postselection

$$P(\beta) = \langle \beta | g^n \rho_B g^n | \beta \rangle$$

$$P(\beta) = e^{(g^2-1)|\beta|^2} \langle g\beta | \rho_B | g\beta \rangle$$

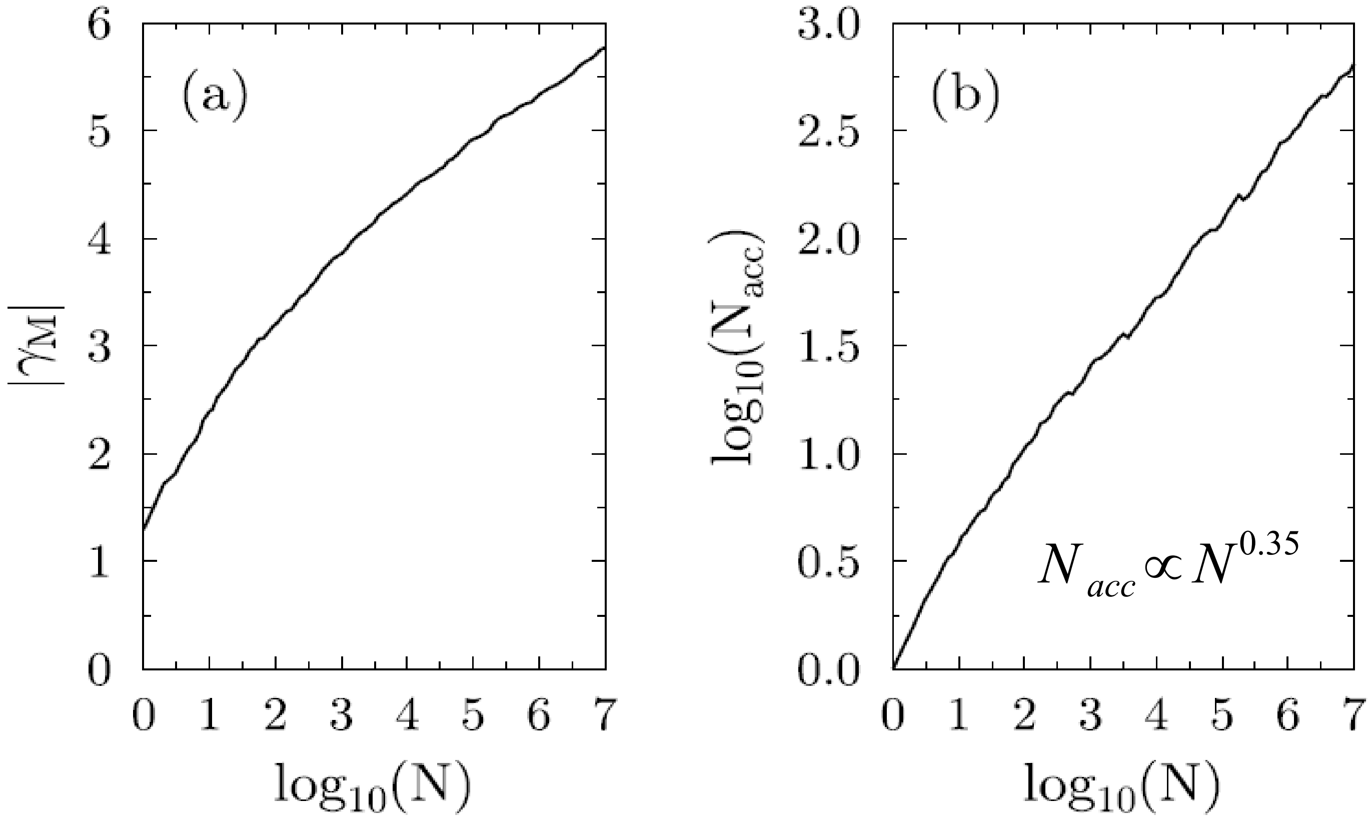
$$\beta = \frac{\gamma}{g}$$

$$Q(\gamma) = \exp\left[(1-g^{-2})|\gamma|^2\right]$$



Post-selection: the data is accepted with probability proportional to Q(γ).

Success rate of the post-selection



$$Q(\gamma) = \exp\left[-(1-g^{-2})(|\gamma_M|^2 - |\gamma|^2)\right] \leqslant 1 \qquad |\gamma_M| = max_j |\gamma_j|$$

Exact emulation of noiseless amplification.

The number of accepted data scales sublinearly with N – inefficient procedure.

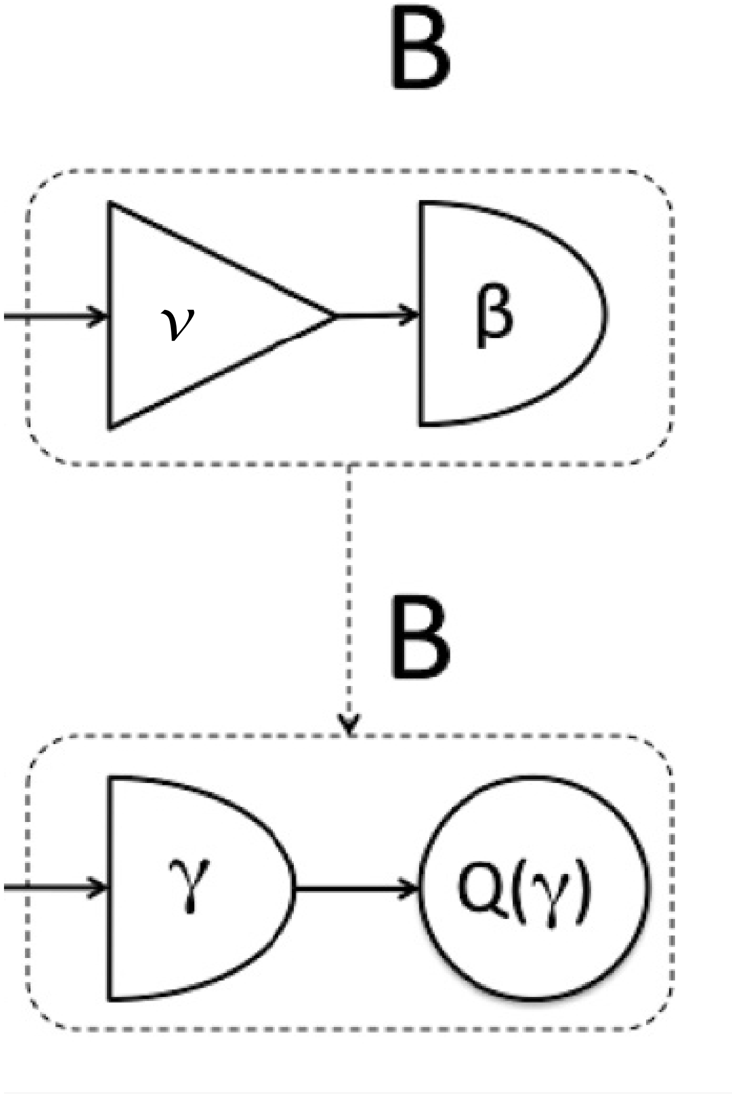
Emulation of noiseless attenuation by postselection

$$P(\beta) \propto \langle \beta | \nu^n \rho_B \nu^n | \beta \rangle$$

$$P(\beta) \propto e^{-(1-\nu^2)|\beta|^2} \langle \nu \beta | \rho_B | \nu \beta \rangle$$

$$\beta = \frac{\gamma}{\nu}$$

$$Q(\gamma) = \exp\left[-(\nu^{-2} - 1) |\gamma|^2 \right]$$



Efficient emulation is possible because Q(γ)<1.

Secret key calculation

• Virtual entanglement picture is employed

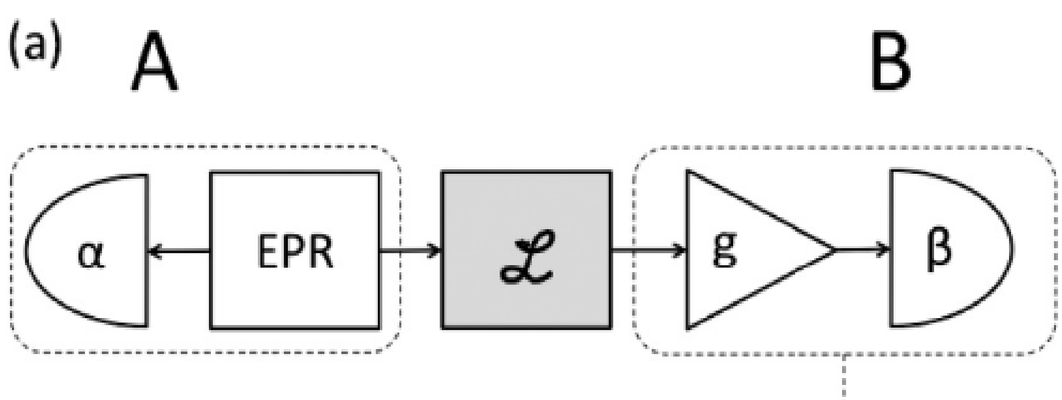
• The effective entangled Gaussian state shared by Alice and Bob after noiseless amplification/ noiseless attenuation is determined

$$\rho_{AB,out} = \frac{1}{N} g^{n_B} \rho_{AB} g^{n_B} \qquad \rho_{AB,out} = \frac{1}{N} \nu^{n_B} \rho_{AB} \nu^{n_B}$$

•Secret key against collective attacks is calculated:

$$K = \max(\eta I_{AB} - \chi_{AE}, \eta I_{AB} - \chi_{BE})$$

• The key rate is maximized by optimizing Alice's modulation strength λ



Lossy channel and noiseless amplification

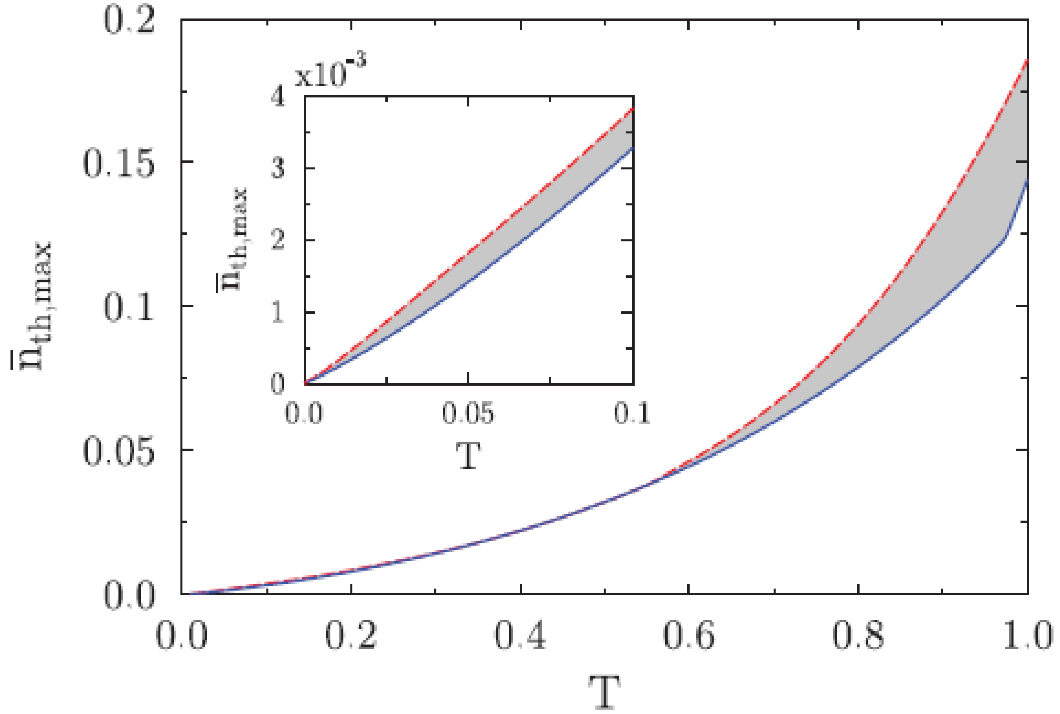


FIG. 3. (Color online) CV QKD over a lossy channel of transmittance T and output excess thermal noise $\bar{n}_{\mathrm{th}}$. The maximum tolerable noise $\bar{n}_{\mathrm{th,max}}$ decreases for decreasing T. A secret key can be generated if $\bar{n}_{\mathrm{th}} < \bar{n}_{\mathrm{th,max}}$, shown with the blue solid line (standard protocol) or red dashed line (protocol augmented with virtual noiseless amplification). The gray area indicates the class of channels for which noiseless amplification is beneficial. We optimize over Alice's modulation variance V and Bob's amplification gain g, and we assume $\eta = 0.9$. The inset shows a zoom-in of the region of high losses, $T \leqslant 0.1$.

Amplifying channel and noiseless attenuation

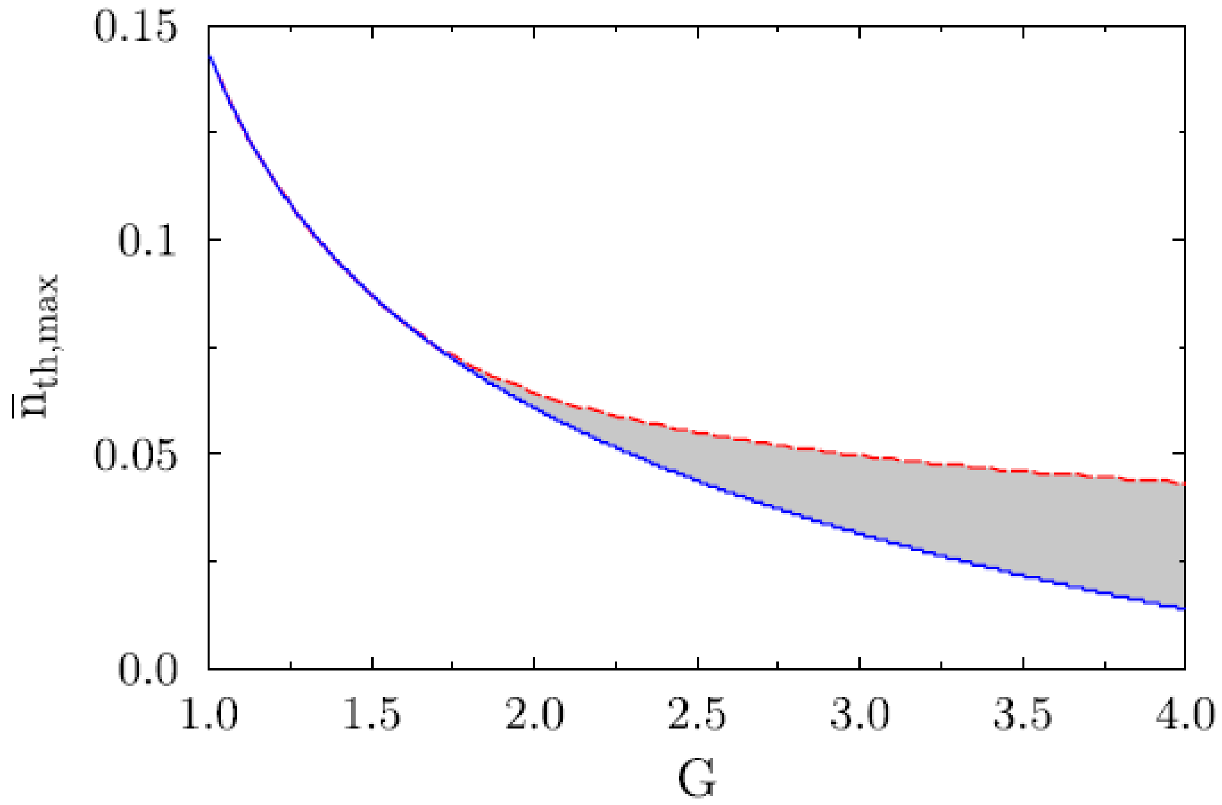


FIG. S.2: CV QKD over an amplifying channel of gain G and output excess thermal noise $\bar{n}_{\mathrm{th}}$. The maximum tolerable noise $\bar{n}_{\mathrm{th,max}}$ decreases for increasing G. A secret key can be generated if $\bar{n}_{\mathrm{th}} < \bar{n}_{\mathrm{th,max}}$, shown with the blue solid line (standard protocol) or red dashed line (protocol augmented with virtual noiseless attenuation). The grey area indicates the class of channels for which virtual noiseless attenuation is beneficial. We optimize over Alice's modulation variance V and Bob's attenuation ν, and assume $\eta = 0.9$.

Achievable secret key rates

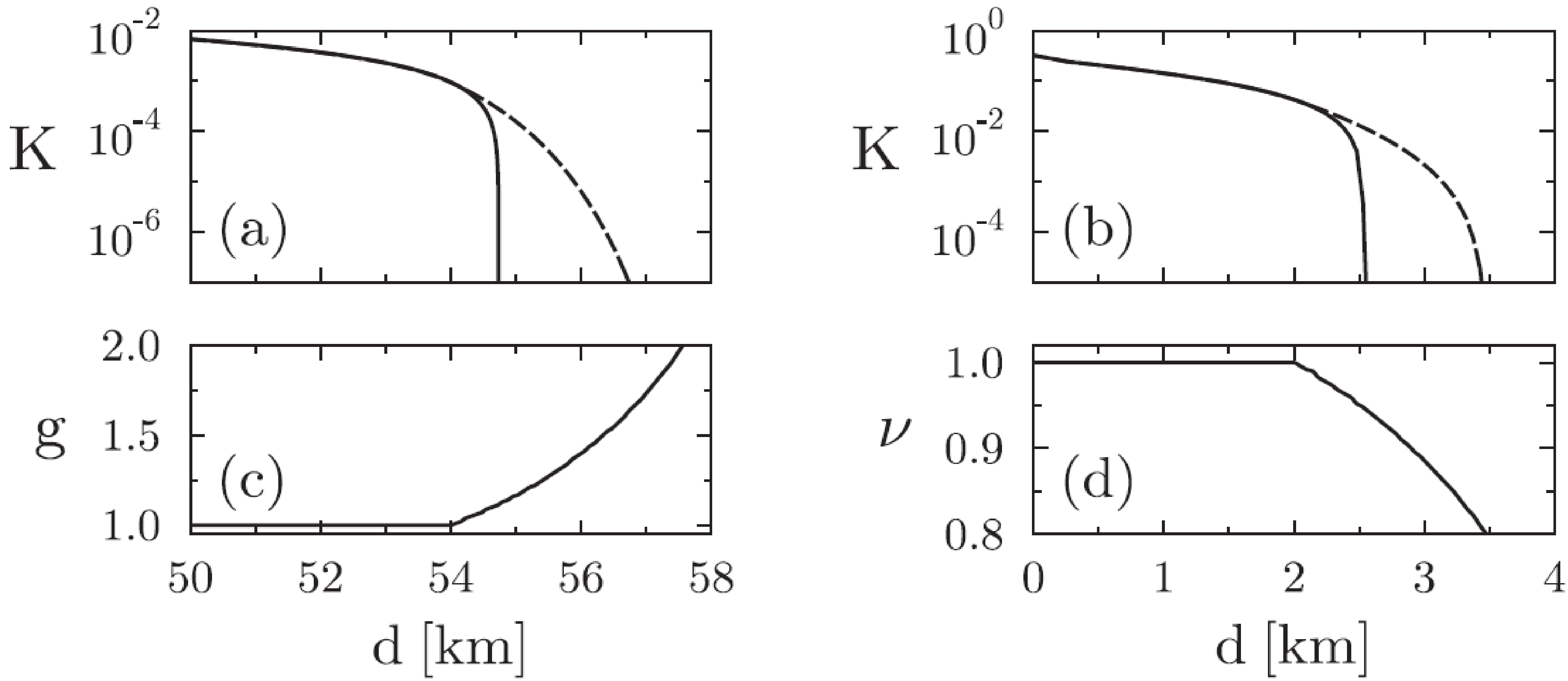


FIG. 4. Achievable secret key rate K in CV QKD over a lossy channel with 0.2 dB loss per km. (a) Comparison of the protocol without Gaussian postselection (solid line) and with optimal noiseless amplification (dashed line), $n_{\mathrm{th}} = 2.5 \times 10^{-3}$, $\gamma_M = 3\sqrt{V_\gamma}$. (b) Comparison of the protocol without Gaussian postselection (solid line) and with optimal noiseless attenuation (dashed line), $n_{\mathrm{th}} = 0.1$. We assume $\eta = 0.9$, and the parameters V, g, and ν were optimized for each d so as to maximize K. The resulting optimal g and ν are plotted in panels (c) and (d), respectively.

Thank you for your attention!