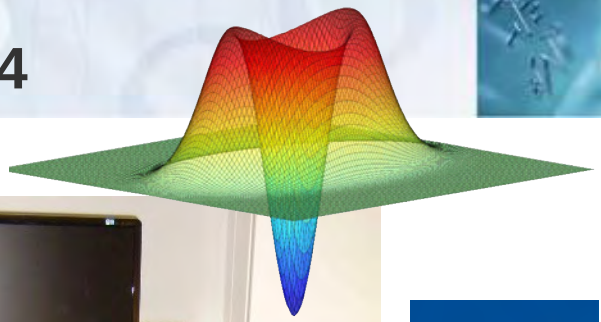
chist-era

Project Seminar
Istanbul
March 4-5, 2014



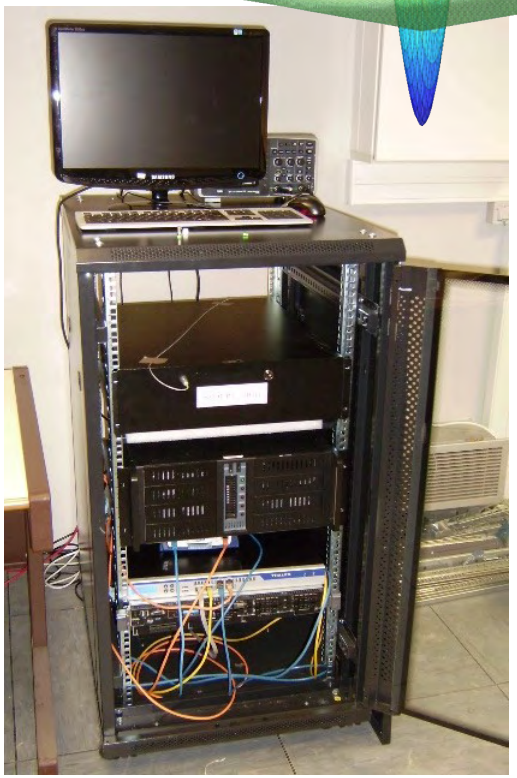
INSTITUT d'OPTIQUE GRADUATE SCHOOL

TELECOM ParisTech

ULB

HIPERCOM

High-Performance Coherent Quantum Communications



MPL

September 2011 – August 2014

Coordinated by Nicolas J. Cerf

THE UNIVERSITY of York

SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

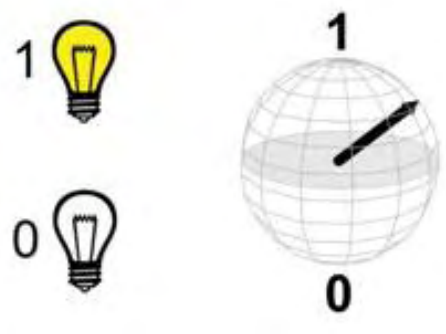
HIPERCOM CONSORTIUM

	Partner Number	Country	Institution/ Department	Name of the group leader	Other personnel participating in the project
Th	1 Coord.	Belgium	Université Libre de Bruxelles (**ULB**) / Centre for Quantum Information and Communication	Nicolas J. Cerf	Evgueni Karpov, Raul Garcia-Patron
Ex	2	France	Institut d'Optique Graduate School (**IO**) / Laboratoire Charles Fabry	Philippe Grangier	Rosa Tualle-Brouri, Rémi Blandino
Th-Ex	3	Germany	Max Planck Society / Max Planck Institute for the Science of Light (**MPL**)	Gerd Leuchs	Peter van Loock, Christoph Marquardt
Th	4	UK	University of York (**UY**) / Computer Science Department	Samuel L. Braunstein	Stefano Pirandola
Th-Ex	5	France	Telecom Paris Tech (**TPT**) / Laboratoire Traitement et Communication de l'Information	Eleni Diamanti	Damian Markham
Indus	6	France	SeQureNet (**SQN**)	Sebastien Kunz-Jacques	Paul Jouguet

ESSENCE OF HIPERCOM

Use of optical « **continuous variables** » instead of qubits

Bit Qubit

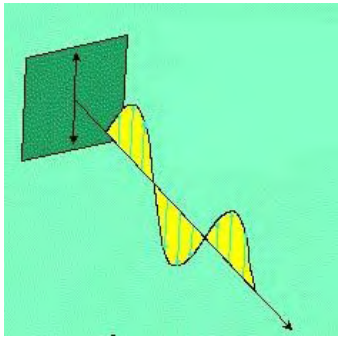


$$\alpha \cdot |0\rangle + \beta \cdot |1\rangle$$

… quantum superposition

The qubit has become the « cornerstone » of quantum information sciences
(most QIPC processes have been originally developed with qubits)

► **but several advantages of CV information carriers !**



amplitude

e.g., light field: A cos(ω t + φ)

… coherent communications

KEY CHALLENGE OF HIPERCOM

Develop ***coherent quantum communication*** in order to combine

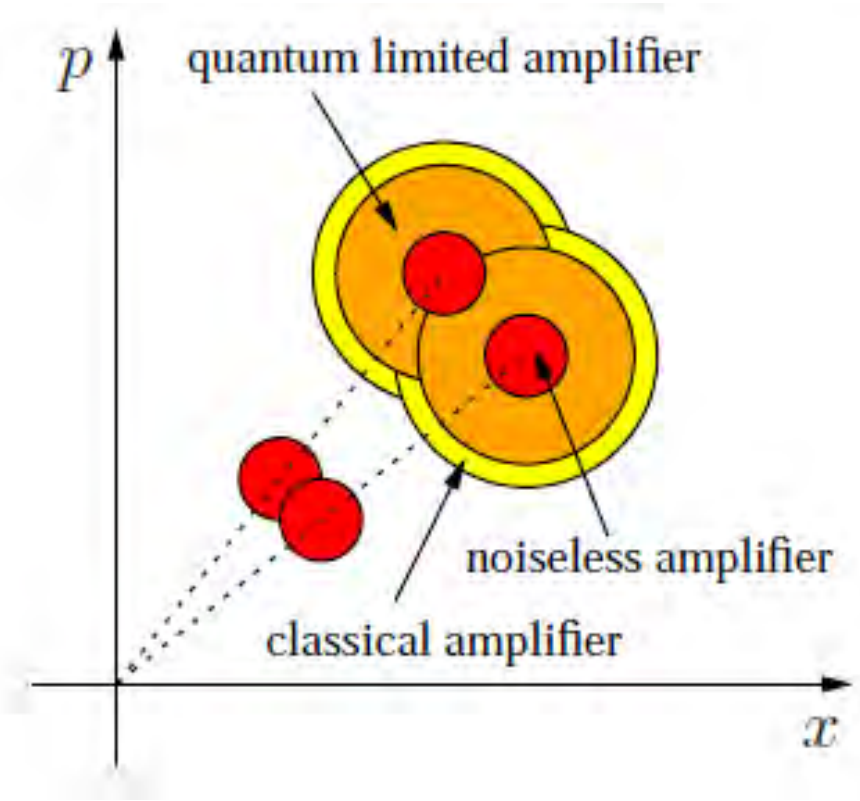
- the high bandwidth achievable by telecom components (e.g., homodyne detection)
- the fundamental benefits of quantum mechanics (e.g., unconditional security)

Fundamental problem : quantum optical amplifier cannot be used simply as a repeater because it is inherently limited by quantum noise.

The objective of HIPERCOM is to explore various techniques aiming at circumventing this problem and *enhancing the range* of coherent quantum communications

with a special emphasis on today's most developed platform towards applications, namely *CV Quantum Key Distribution*

[see Eleni Diamanti's talk]



METHODOLOGY OF HIPERCOM

Different strategies will be followed in order to approach
long-distance coherent CV quantum communications

ranging from the use of classical coding and other post-processing algorithms,
which is the most directly applicable solution in the short term,

to more elaborate techniques relying on specific quantum optical schemes
and ultimately on the use of quantum error-correcting codes.

In between these two extreme approaches, the potential solution offered by the noiseless linear amplifier or similar heralded operations will be investigated.

WP1 : Improve classical and optical post-processing
(e.g. classical coding, bidirectional protocols)

WP2 : Beyond classical coding but exper. accessible
(e.g. noiseless amplifier & other heralded proc.)

WP3 : Full quantum solution to range enhancement
(e.g. quantum coding, non-Gaussian CV codes)

applicable
with today's
techniques

longer-term
more theoretical
investigation

EXPECTED OUTCOMES OF HIPERCOM

Theoretical progresses on coherent quantum communications

quantum coding, Gaussian channel capacities, general security proofs of CV-QKD (incl. coherent attacks, side-channels, etc.)

Experimental demonstrations of heralded non-Gaussian quantum processes

(noiseless linear amplifier & its application to CV-QKD)

Improved practical realizations of CV-QKD platform

working over longer distances and with stronger security assessment

- pave the way towards long-distance coherent CV quantum communications

- we are on a good track (all scheduled tasks as of Y2 were completed)

KNOWLEDGE DISSEMINATION

WP0 : Management & organization of annual topical workshops

e.g. Continuous-variable Quantum Information Processing workshop series

HIPERCOM kick-off meeting, Telecom ParisTech, Paris, September 26-27, 2011,
organized by Eleni Diamanti, widened to non-HIPERCOM invited speakers,
was turned into 8th workshop CV-QIP '11

9th workshop CV-QIP '12, Copenhagen, April 27-30, 2012
organized by Ulrik Andersen with ~ 25% of the attendance from HIPERCOM

HIPERCOM mid-term meeting, Jussieu, Paris, January 30 - February 1st, 2013,
organized by Julien Laurat (coupled to project QSCALE), widened to other experts,
was turned into 10th workshop CV-QIP '13

21th Central-European Workhop on Quantum Optics, Brussels, June 23-27, 2014
organized by Evgueni Karpov & Nicolas Cerf (~ 200 participants expected)
including special spessions for HIPERCOM ptoject & QSCALE project

21st Central European Workshop on Quantum Optics

Brussels, 23 – 27 June, 2014

Chair: Evgueni Karpov – ULB

Local organizing committee:

Edouard Brainis – UG
Nicolas Cerf (co-chair) – ULB
Serge Massar – ULB
Krassimir Panajotov – VUB
Hugo Thienpont - VUB

Vrije Universiteit Brussel

ULB UNIVERSITÉ LIBRE DE BRUXELLES

UNIVERSITEIT GENT

SCIENTIFIC WORKPACKAGES

WP1 + 2 + 3 : rest of this talk

2 selected results in connection with NLA & CV-QKD

- Noiseless linear amplifier

  Further progresses on theoretical understanding of noiseless amplification of non-Gaussian states

  (ULB) [this talk]

- CV-QKD experimental platform

  Further progresses on optical implementation

  (TNT & SQN) [Eleni Diamanti's talk]

Noiseless Linear Amplifier (NLA)

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

Physical approximation to the unphysical target operation

$$|\alpha\rangle \rightarrow |g\,\alpha\rangle \qquad g>1$$

Quantum filter diagonal in Fock basis:

$$\hat{G}=g^{\hat{n}} \qquad |n\rangle \rightarrow g^{n}|n\rangle \qquad |\alpha\rangle \rightarrow g^{\hat{n}}|\alpha\rangle \propto \mathrm{e}^{(g^2-1)|\alpha|^2/2}|g\,\alpha\rangle$$

Applications:

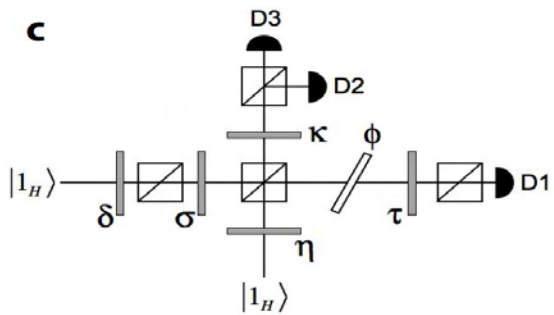
- High-fidelity probabilistic cloning / phase estimation
- Filtration of high-entangled pures states (entanglement concentration)
- Phase-insensitive (universal) squeezing
- Breeding of Schrödinger-cat states
- ***Compensation of optical losses in quantum communication and quantum key distribution (IO, ULB)***

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

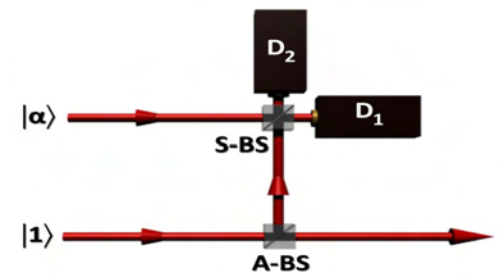
G. Y. Xiang[1], T. C. Ralph[2], A. P. Lund[1,2], N. Walk[2] and G. J. Pryde[1]*



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

Implementation of a Nondeterministic Optical Noiseless Amplifier

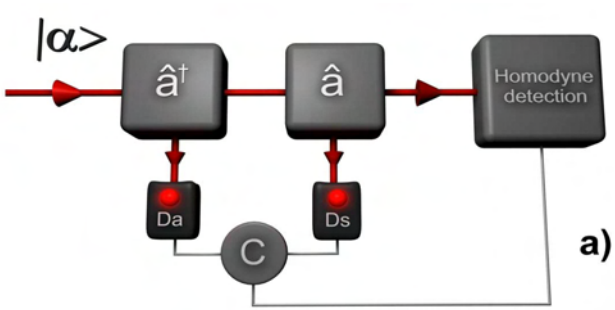
Franck Ferreyrol, Marco Barbieri, Rémi Blandino, Simon Fossier, Rosa Tualle-Brouri, and Philippe Grangier
Groupe d'Optique Quantique, Laboratoire Charles Fabry, Institut d'Optique, CNRS, Université Paris-Sud, Campus Polytechnique, RD 128, 91127 Palaiseau cedex, France
(Received 10 December 2009; published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

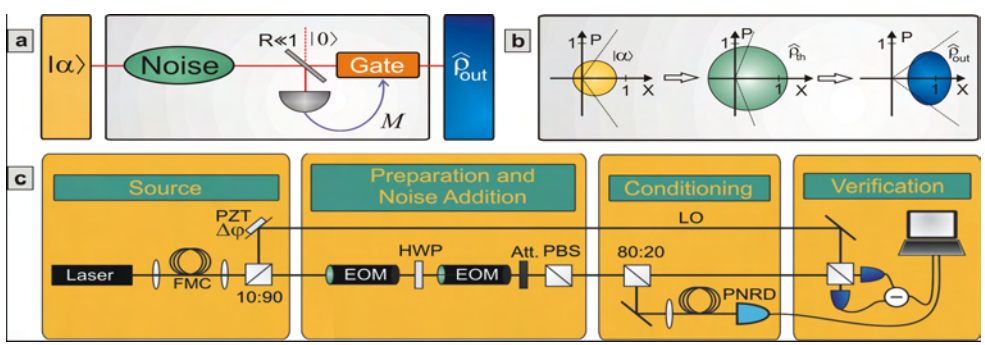
A. Zavatta[1,2], J. Fiurášek[3] and M. Bellini[1,2]*



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

Noise-powered probabilistic concentration of phase information

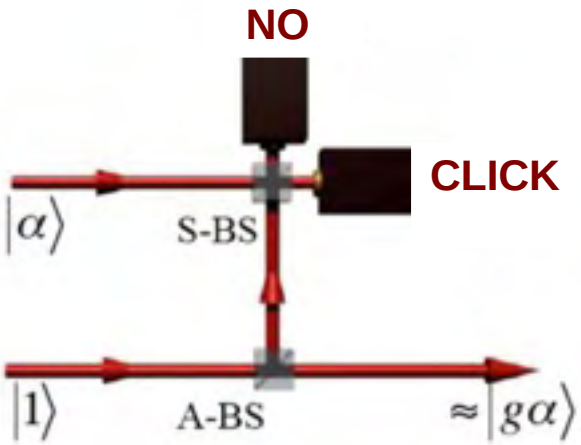
Mario A. Usuga[1,2†], Christian R. Müller[1,3†], Christoffer Wittmann[1,3], Petr Marek[4], Radim Filip[4], Christoph Marquardt[1,3], Gerd Leuchs[1,3] and Ulrik L. Andersen[2]*

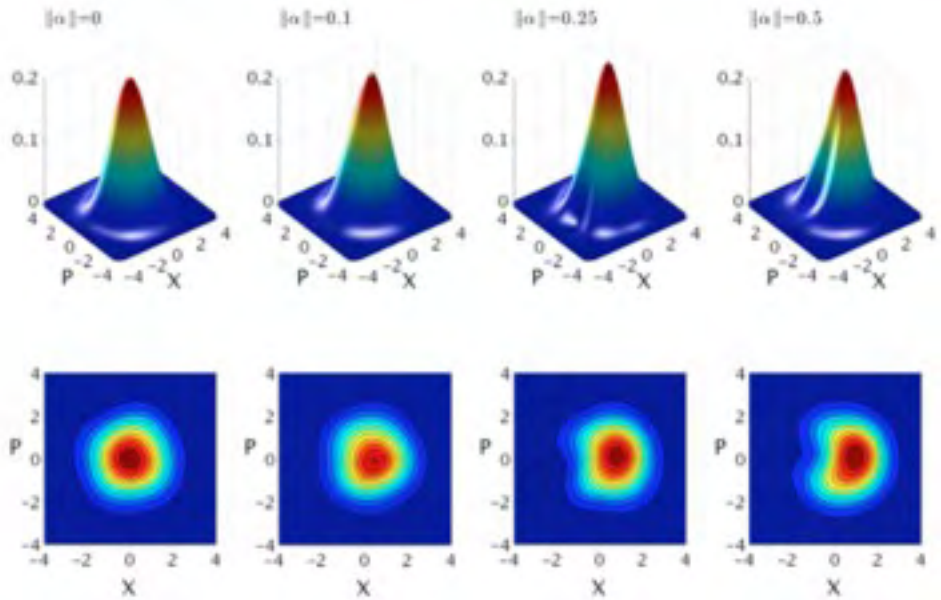


NLA of coherent states by quantum scissors (Palaiseau)

Truncation to space spanned by vacuum and single-photon state

$$|\alpha\rangle \simeq |0\rangle + \alpha|1\rangle \;\rightarrow\; |0\rangle + g\,\alpha|1\rangle$$

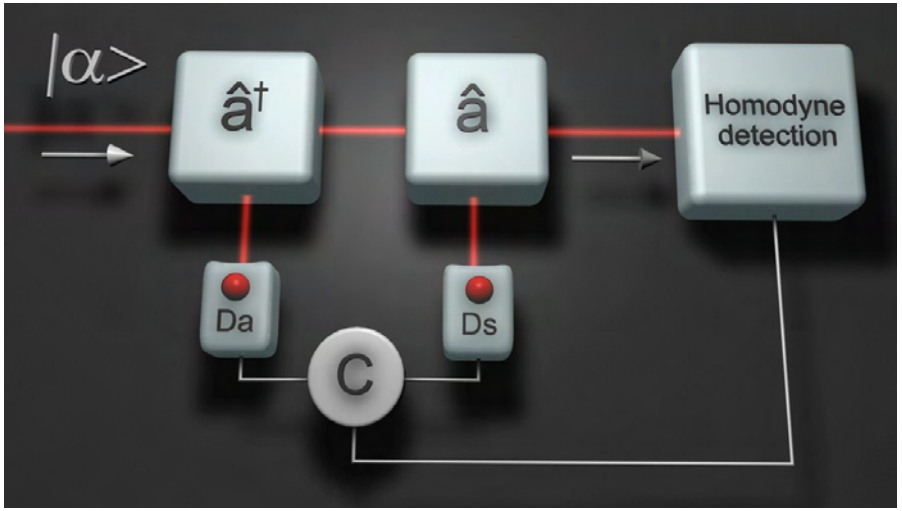


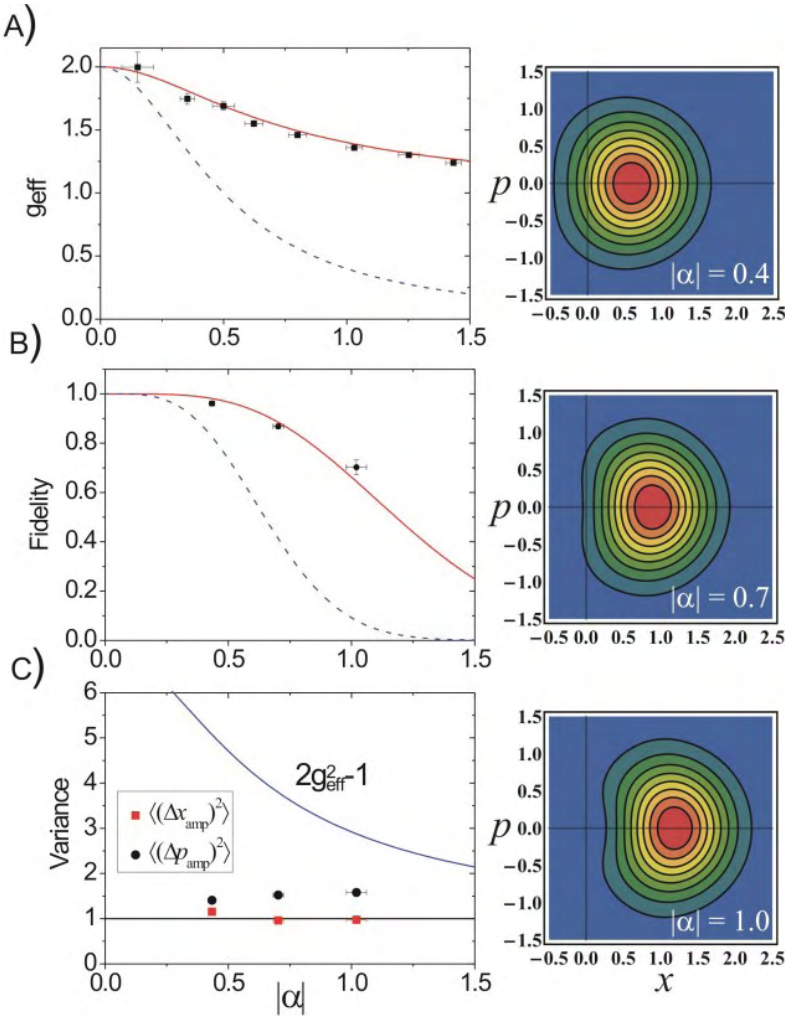


$$\left(t|1\rangle_T|0\rangle_R + r|0\rangle_T|1\rangle_R \right) \left(|0\rangle_{\text{in}} + \alpha|1\rangle_{\text{in}} \right) \;\rightarrow\; r|0\rangle_T + t\,\alpha|1\rangle_T \propto |0\rangle_T + g\,\alpha|1\rangle_T$$

... choose $t/r = g$

NLA by photon addition / subtraction (Florence)





$$g^{\hat{n}} \approx \sum_{k=0}^{N} \frac{d^k}{k!} \hat{n}^k$$

keep only 1st order

$$g^{\hat{n}} \approx (g-1)\hat{n}+1 = (g-2)\hat{a}^+\hat{a}+\hat{a}\hat{a}^+$$

choose $g=2$

$$\hat{G}_{g=2} = \hat{a}\hat{a}^+$$

... very crude approximation,
works well only for weak coherent states

$$\hat{a}\hat{a}^+\left(|0\rangle+\alpha|1\rangle\right) = \hat{a}\left(|1\rangle+\sqrt{2}\alpha|2\rangle\right) = |0\rangle+2\alpha|2\rangle$$

Noiseless amplification & CV QKD

Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier

Rémi Blandino,[1,*] Anthony Leverrier,[2] Marco Barbieri,[1,†]
Jean Etesse,[1] Philippe Grangier,[1] and Rosa Tualle-Brouri[1,3]

ArXiv:1205.0959; Phys. Rev. A **86**, 012327 (2012).

(IO)

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

Jaromír Fiurášek[1] and Nicolas J. Cerf[2]

ArXiv:1205.6933, Phys. Rev. A **86**, 060302(R) (2012).

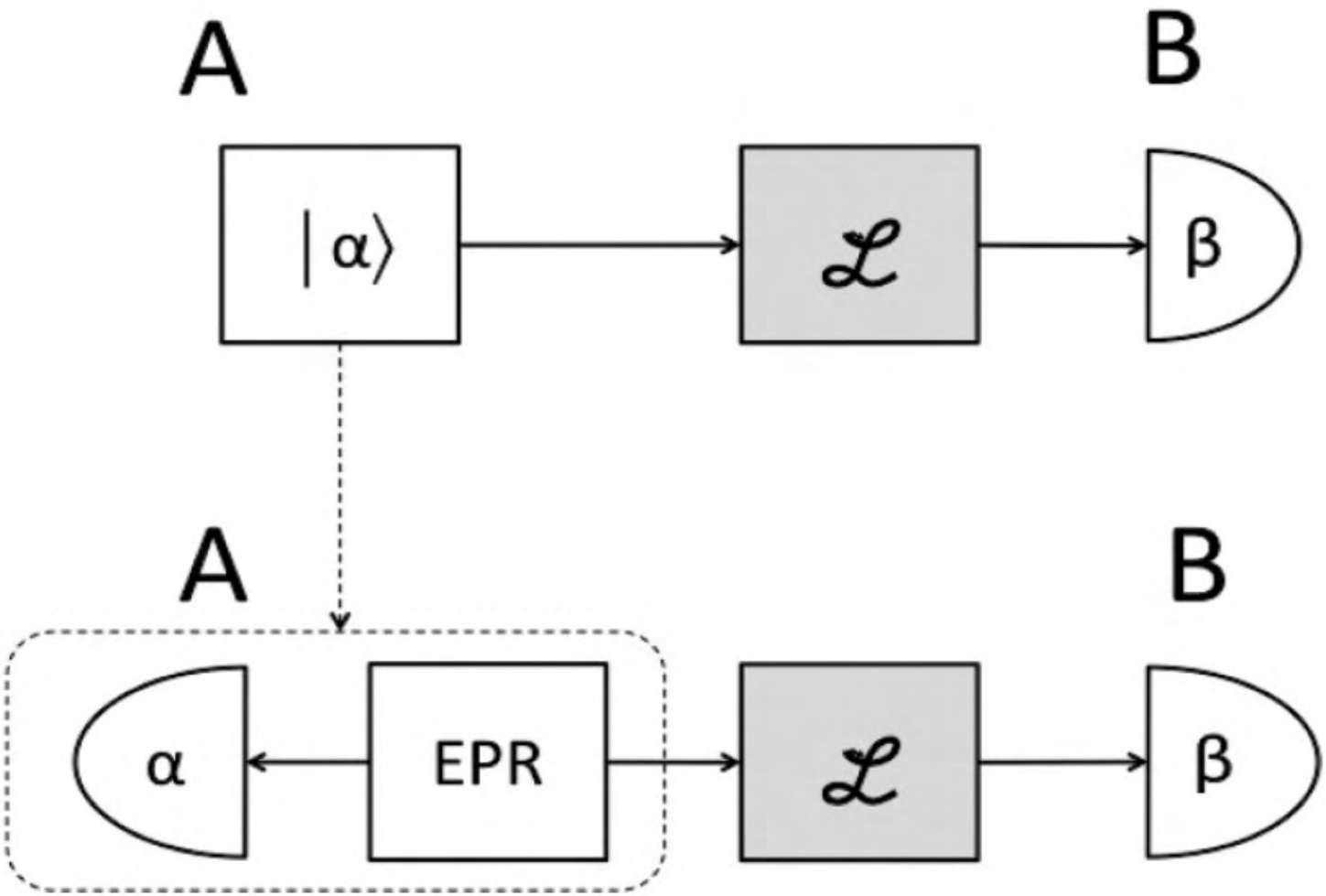
(ULB)

Gaussian Post-selection for Continuous Variable Quantum Cryptography

Nathan Walk[*] and Timothy C. Ralph
Thomas Symul and Ping Koy Lam

ArXiv:1206.0936, Phys. Rev. A **87**, 020303 (2013).

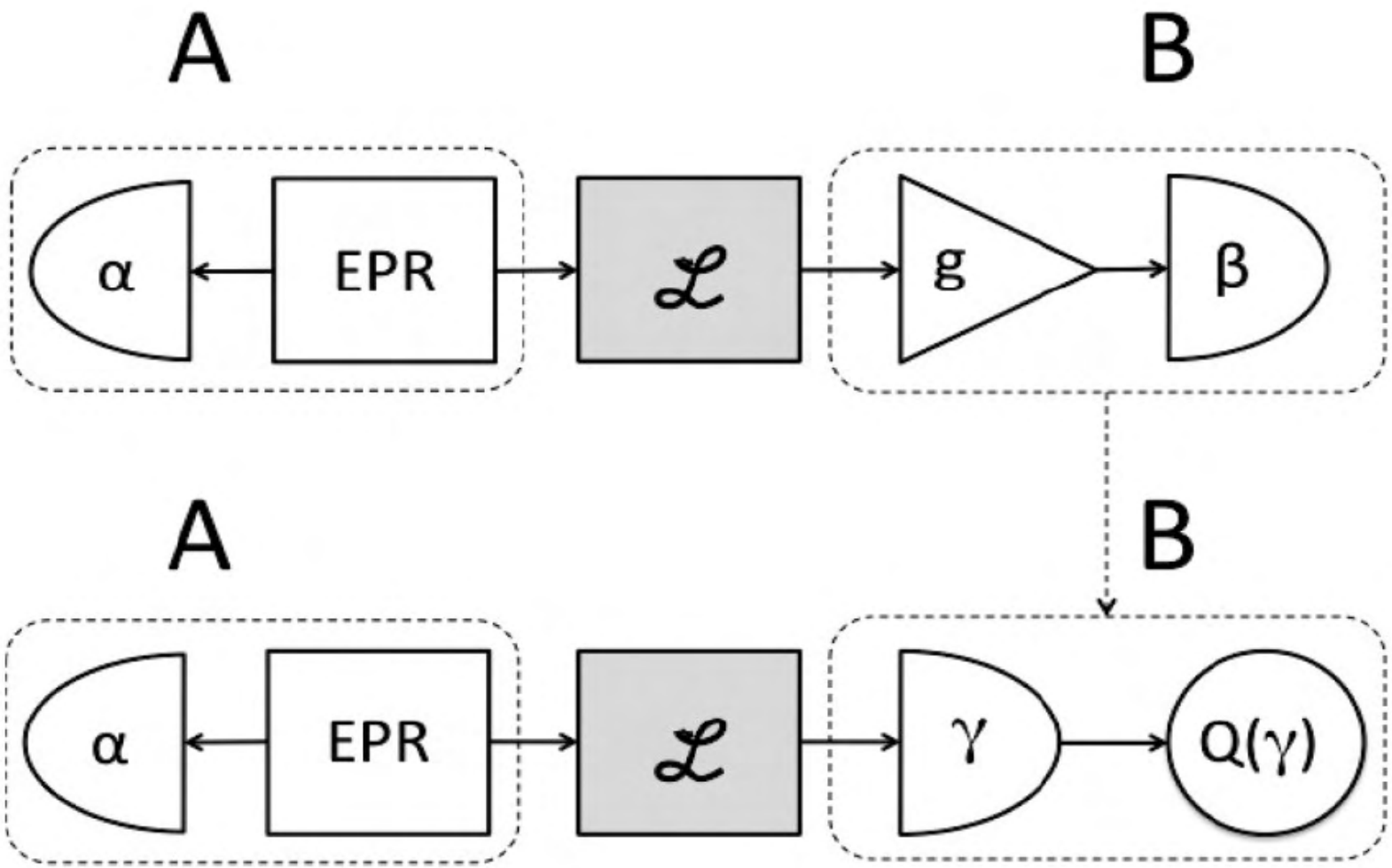
CV QKD with heterodyne detection



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 amplification can be emulated on Bob's measured data.

Emulation of noiseless amplification by postselection

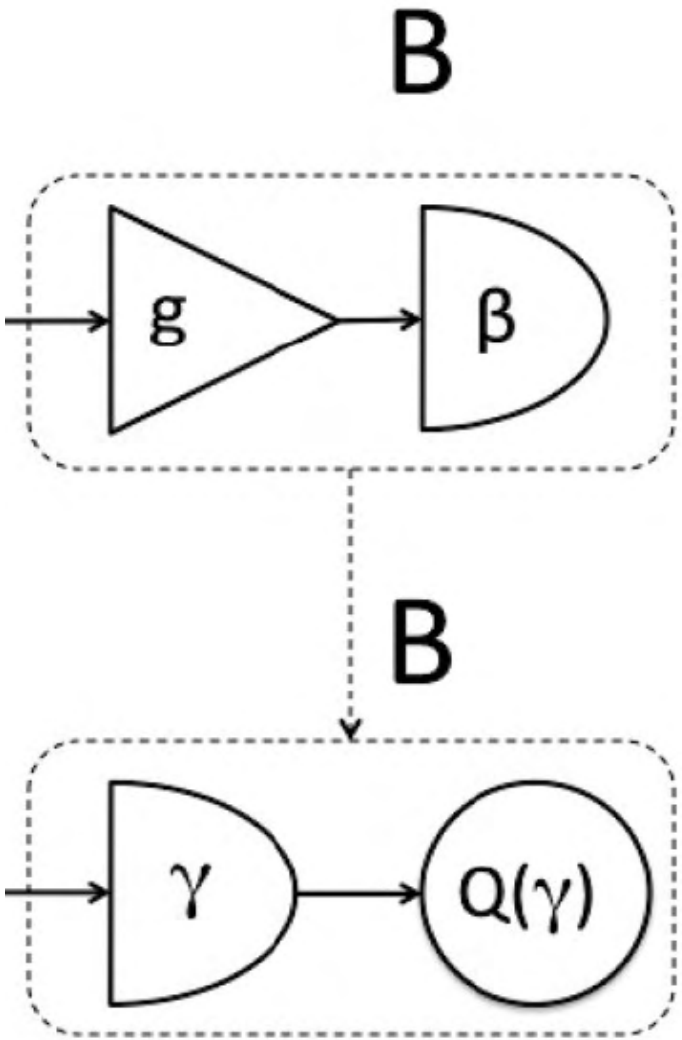
$$P(\beta) \propto \langle \beta | g^n \rho_B g^n | \beta \rangle$$

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

$$\propto Q(\gamma) \langle \gamma | \rho_B | \gamma \rangle$$

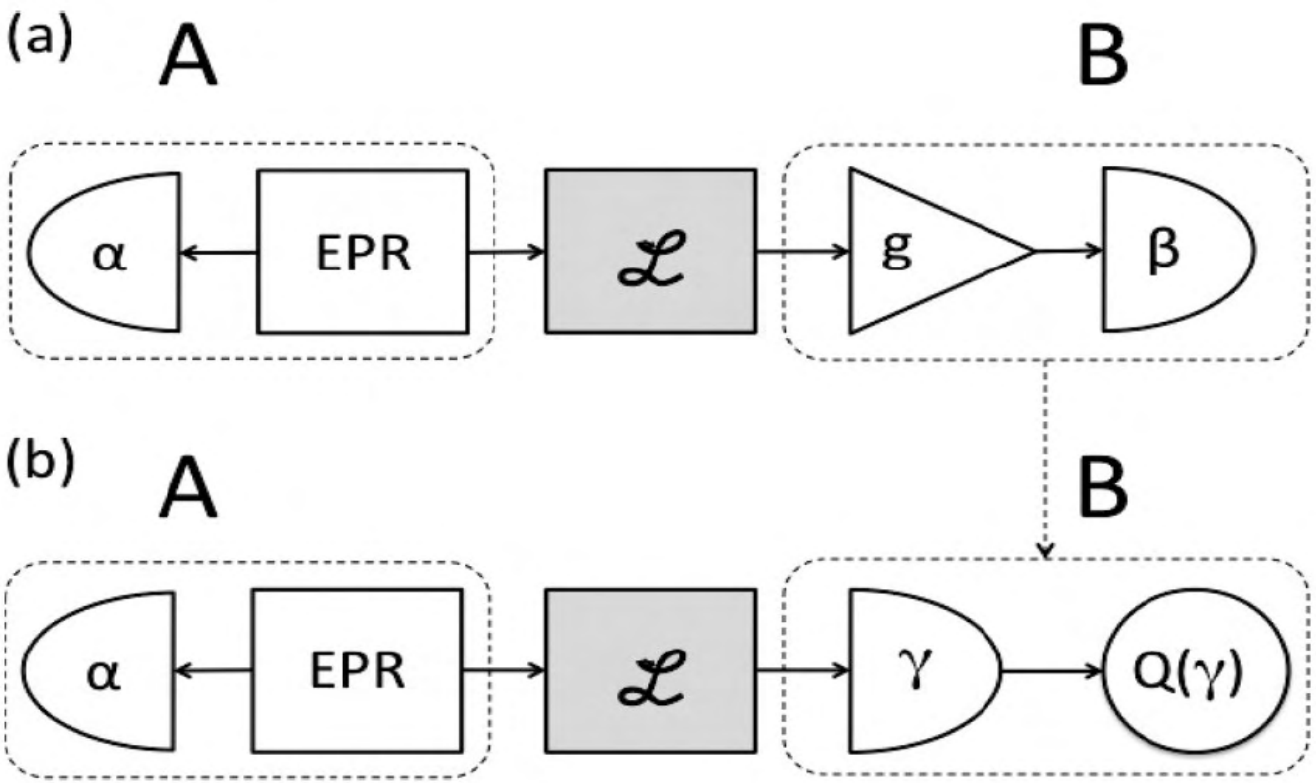
$$\beta = \frac{\gamma}{g} \qquad (g > 1)$$

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



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

Security properties of protocol with post-selection



The protocol is completely equivalent to the following sequence:

(i) probabilistic entanglement concentration by local noiseless amplification
(ii) standard deterministic entanglement-based CV QKD protocol

The security properties of our scheme with postselection are thus the same as the security properties of the standard deterministic protocol.

Lossy channel and noiseless amplification

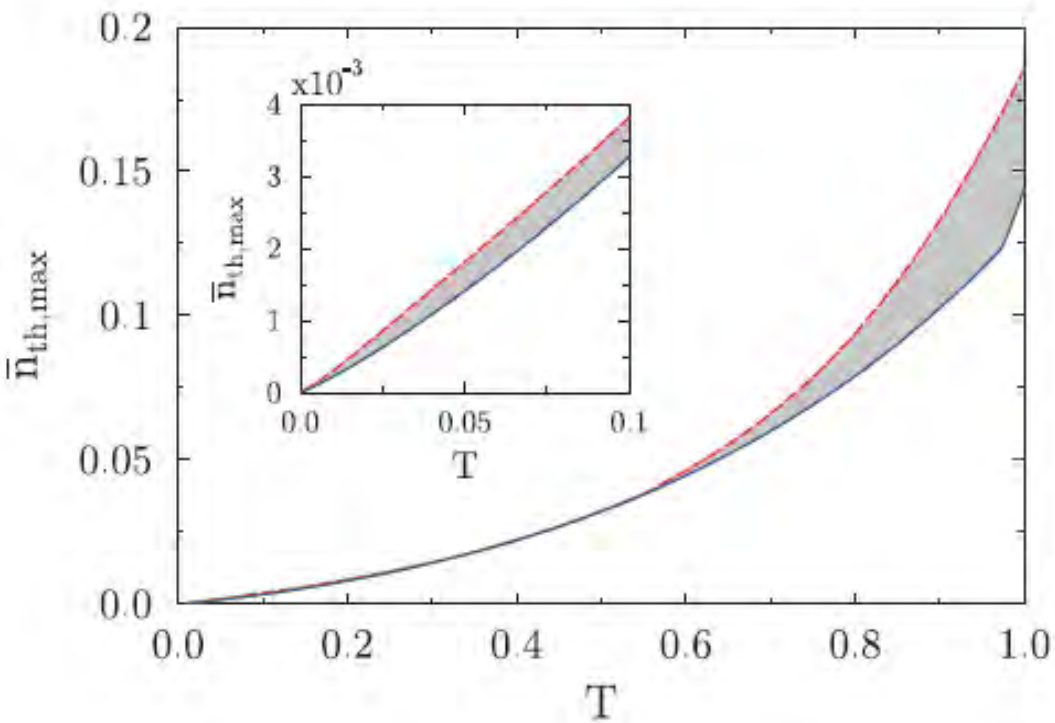


FIG. 3. (Color online) CV QKD over a lossy channel of transmittance T and output excess thermal noise $\bar{n}_{th}$. The maximum tolerable noise $\bar{n}_{th,max}$ decreases for decreasing T. A secret key can be generated if $\bar{n}_{th} < \bar{n}_{th,max}$, shown with the blue solid line (standard 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, $T \leqslant 0.1$.

$$a_{out} = \sqrt{T}\, a_{in} + \sqrt{1-T}\, a_{th}$$

$$\langle a_{th}^{\dagger} a_{th} \rangle = \frac{\bar{n}_{th}}{1-T}$$

Achievable secret key rates

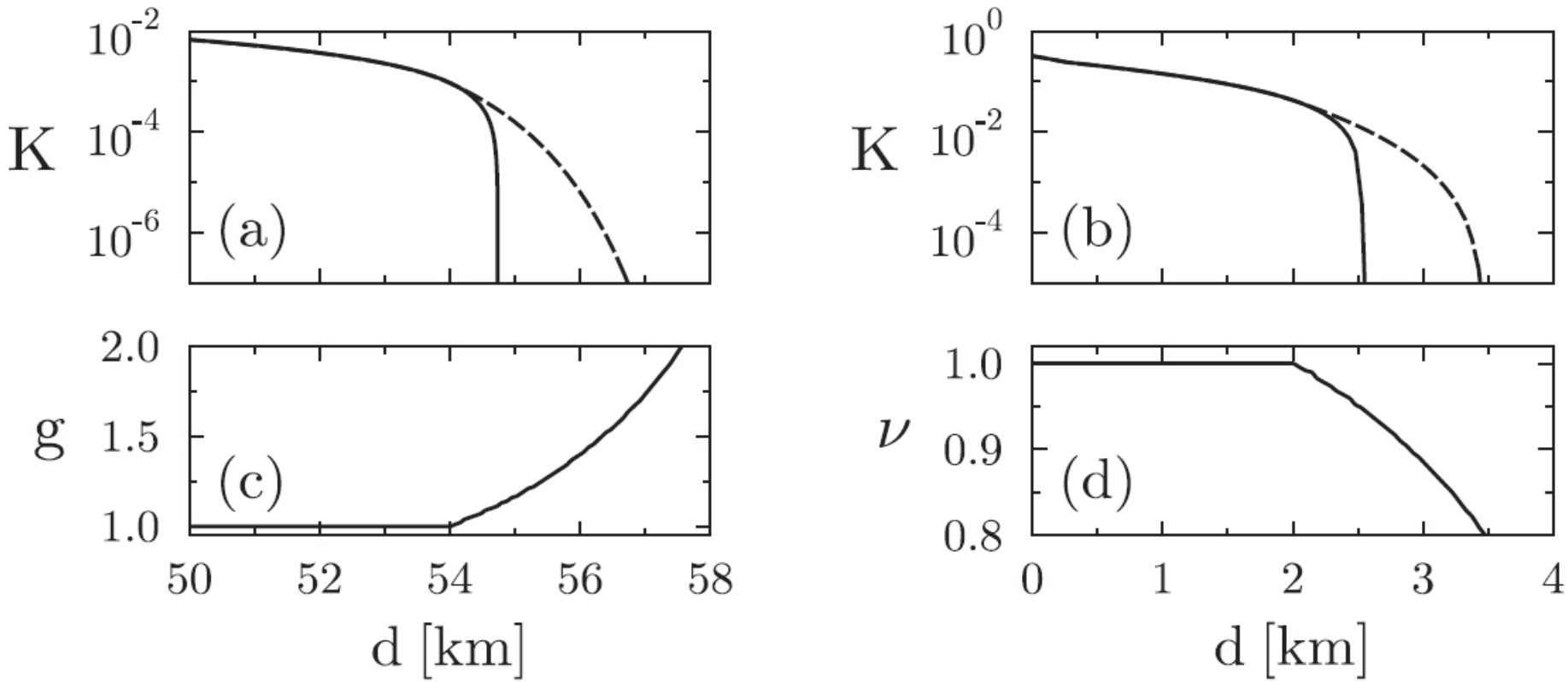


FIG. 4. Achievable secret key rate K in CV QKD over a lossy channel with 0.2 dB loss per km. (a) Comparison of the protocol without Gaussian postselection (solid line) and with optimal noiseless amplification (dashed line), $n_{\text{th}} = 2.5 \times 10^{-3}$, $\gamma_M = 3\sqrt{V_\gamma}$. (b) Comparison of the protocol without Gaussian postselection (solid line) and with optimal noiseless attenuation (dashed line), $n_{\text{th}} = 0.1$. 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.

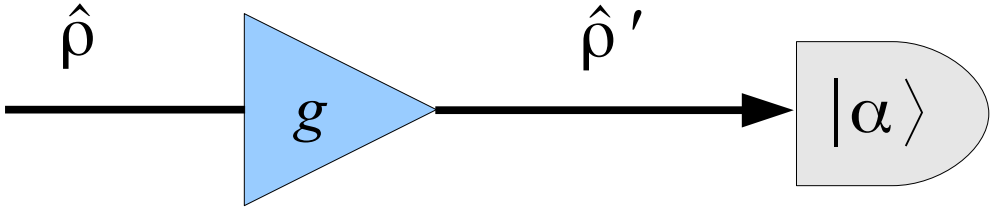
Noiseless amplification of non-Gaussian states

C.N. Gagatsos, J. Fiurasek, A. Zavatta, M. Bellini, N.J. Cerf, preprint (2013).

- Description in phase space (using Husimi Q-function)
- Counterintuitive action on the mean field amplitude
- Proposal for the experimental verification of mean field amplification by noiseless attenuation

Description of NLA in phase-space representation

In terms of Husimi Q-function: $Q(\alpha) = \frac{1}{\pi} \langle \alpha | \hat{\rho} | \alpha \rangle$



with $g > 1$

$$Q'(\alpha) \propto \frac{1}{\pi} \langle \alpha | \overbrace{g^{\hat{n}}\, \hat{\rho}\, g^{\hat{n}}}^{\hat{\rho}\,'} | \alpha \rangle$$

use $g^{\hat{n}} |\alpha\rangle = e^{(g^2-1)|\alpha|^2/2} |g\alpha\rangle$

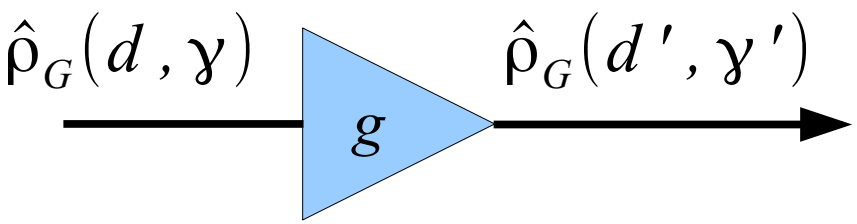
$$\propto \frac{1}{\pi}\, e^{(g^2-1)|\alpha|^2} \langle g\alpha | \hat{\rho} | g\alpha \rangle$$

$$\boxed{Q'(\alpha) \propto e^{(g^2-1)|\alpha|^2}\, Q(g\alpha)}$$

J. Fiurasek and N.J. Cerf,
PRA 86, 060302(R) (2012)

… we can track the noiseless amplification of an **arbitrary state**

Noiseless amplification of arbitrary Gaussian state



$$\begin{cases} d = \text{ displacement vector (mean field)} \\ \gamma = \text{ covariance matrix} \end{cases}$$

$$Q(\alpha) = \frac{2}{\sqrt{\pi^2 \det(\gamma + I)}} \exp\left[-(r-d)^T(\gamma+I)^{-1}(r-d)\right]$$

with $r = \left(\Re(\alpha), \Im(\alpha)\right)^T$

$$\gamma' = \left[g^2(\gamma+I)^{-1} - \frac{g^2-1}{2} I\right]^{-1} - I$$

$$d' = \left[I - \frac{g^2-1}{2}(\gamma - I)\right]^{-1} g\, d$$

… we can follow the evolution of (d,γ) of an **any Gaussian state**

Evolution of mean field amplitude of Gaussian states

take $\gamma = \begin{pmatrix} \sigma_x^2 & 0 \\ 0 & \sigma_p^2 \end{pmatrix}$

effective gain G_{eff} depends on σ_i^2

$$d_i' = \overbrace{\frac{2g}{(1+\sigma_i^2)+g^2(1-\sigma_i^2)}}^{G_{\text{eff}}} d_i$$

with $i = \text{x or p}$

$$1 < G_{\text{eff}}(\sigma^2<1) < g < G_{\text{eff}}(\sigma^2>1)$$

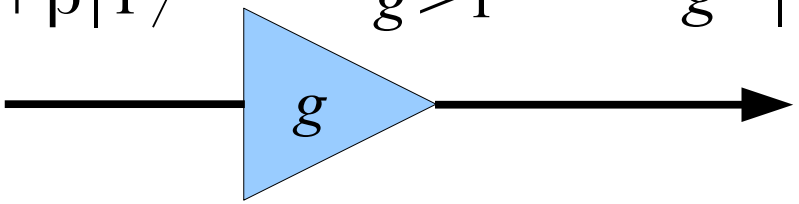
sublinear gain **superlinear gain**

…noiseless amplification of an **arbitrary Gaussian state** can only **increase the mean field amplitude**

Counterintuitive behavior for non-Gaussian states

example

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad g>1 \qquad g^{\hat{n}}|\psi\rangle = \alpha|0\rangle + g\beta|1\rangle|n\rangle$$



$$\langle \hat{a} \rangle_{\psi} = \alpha^* \beta \qquad \langle \hat{a} \rangle_{\psi'} = \frac{\alpha^* g \beta}{|\alpha|^2 + g^2|\beta|^2}$$

$$G_{\text{eff}} = \frac{\langle \hat{a} \rangle_{\psi'}}{\langle \hat{a} \rangle_{\psi}} = \frac{g}{1+(g^2-1)|\beta|^2} < 1 \quad \text{if} \quad |\beta|^2 > \frac{1}{g+1}$$

… the single-photon component $g\beta$ increases when g increases, so we tend to $|1\rangle$ with a mean field tending to 0.

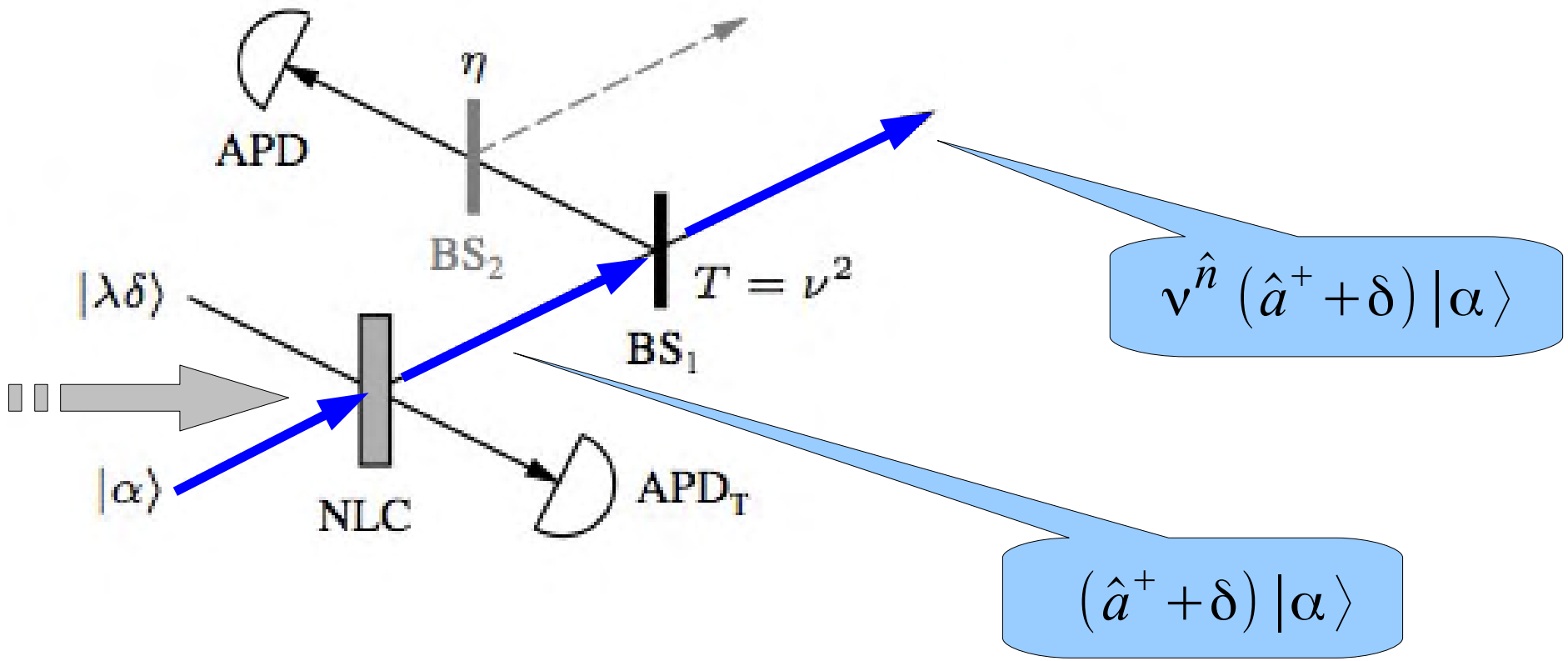
… noiseless amplification may **decrease the mean field amplitude !**

Experimental proposal for probing this paradox

C.N. Gagatsos, J. Fiurasek, A. Zavatta, M. Bellini, N.J. Cerf, preprint (2013)

Use noiseless attenuator with gain $\nu < 1$ (exact map is physical)

Non-Gaussian state made with coherently-displaced single-photon addition on a coherent state (PDC in a nonlinear crystal + weak auxiliary coherent beam)



Noiseless attenuation of single-photon added coherent state

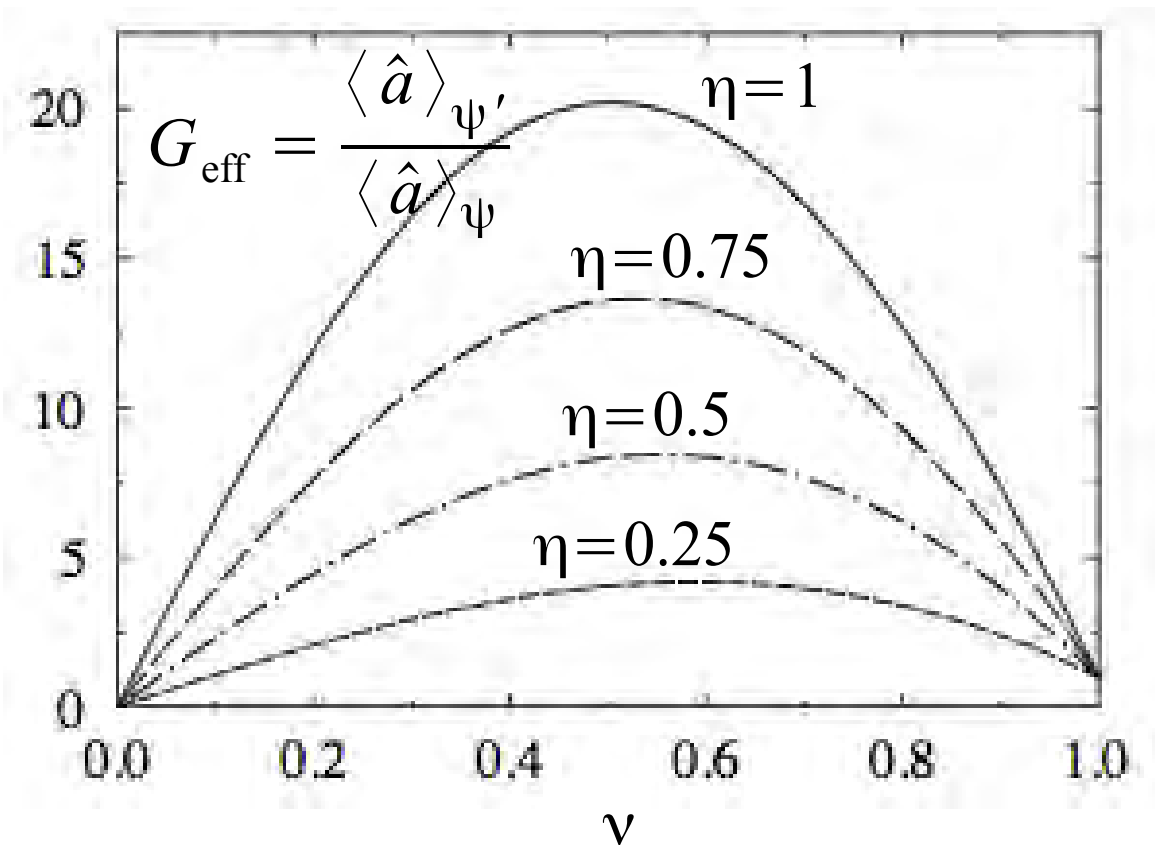
$$|\psi\rangle \propto (\hat{a}^+ + \delta)\,|\alpha\rangle$$

$$|\psi'\rangle \propto \nu^{\hat{n}}\,(\hat{a}^+ + \delta)\,|\alpha\rangle$$

$$= (\nu\,\hat{a}^+ + \delta)\,\underbrace{\nu^{\hat{n}}\,|\alpha\rangle}$$

$$\propto (\hat{a}^+ + \delta/\nu)\;\;|\nu\,\alpha\rangle$$

use $\nu^{\hat{n}}\,\hat{a}^+ = \hat{a}^+\,\nu^{\hat{n}+1}$



robust against inefficient single-photon detection

$\eta = 0.25$

and imperfect state prepar.

purity $p = 0.75$

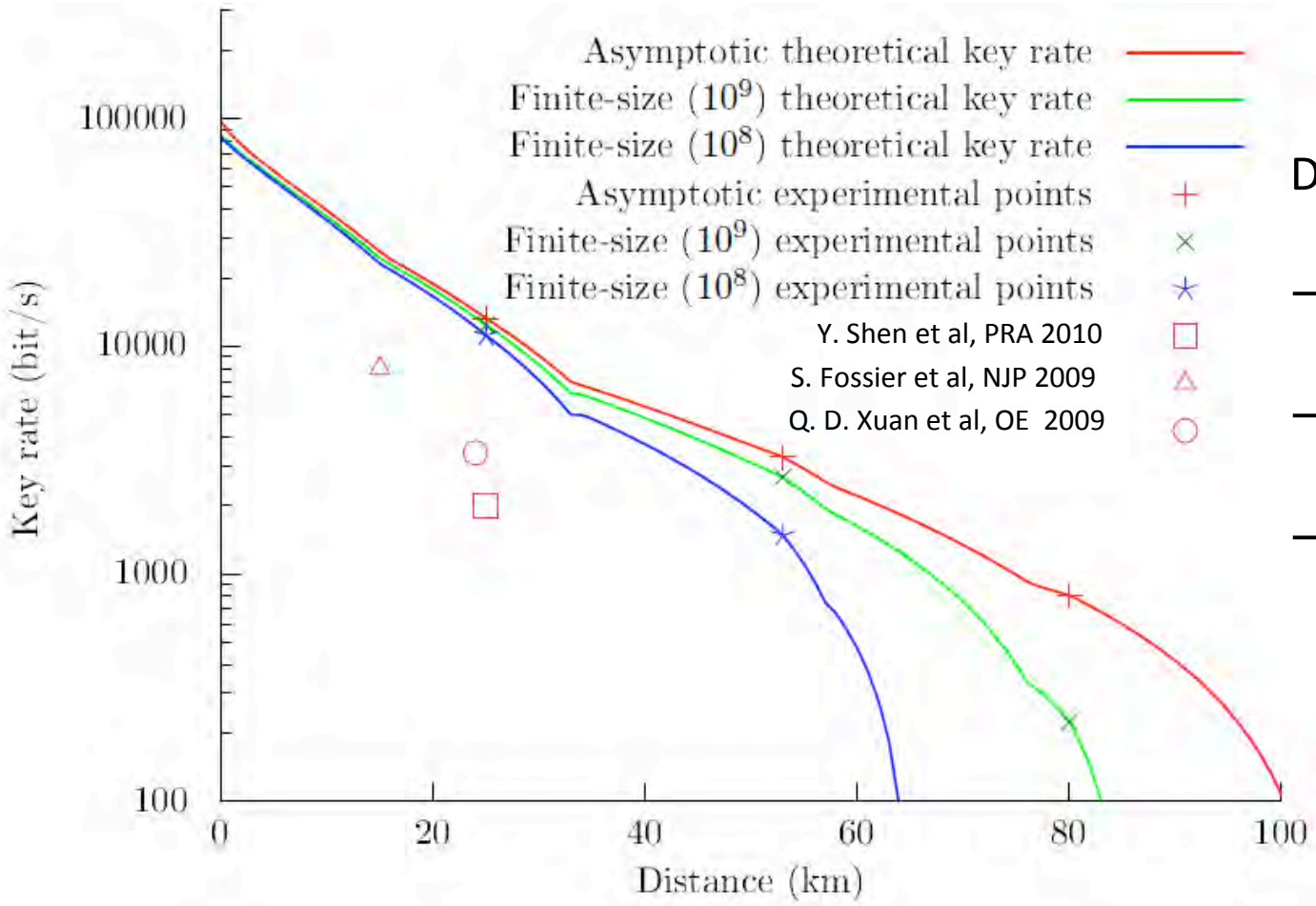
HIPERCOM experimental results on Quantum Key Distribution

Hipercom **objectives** for continuous-variable QKD

- Improve performance in terms of **rate and distance in both fiber optic and free space implementations**

- Improve **practical security** of CV-QKD systems

Long-distance CV-QKD results in Paris



Distance limitation removed

→ new error-correcting codes

→ improved optical stability

→ security against collective attacks including finite-size effects

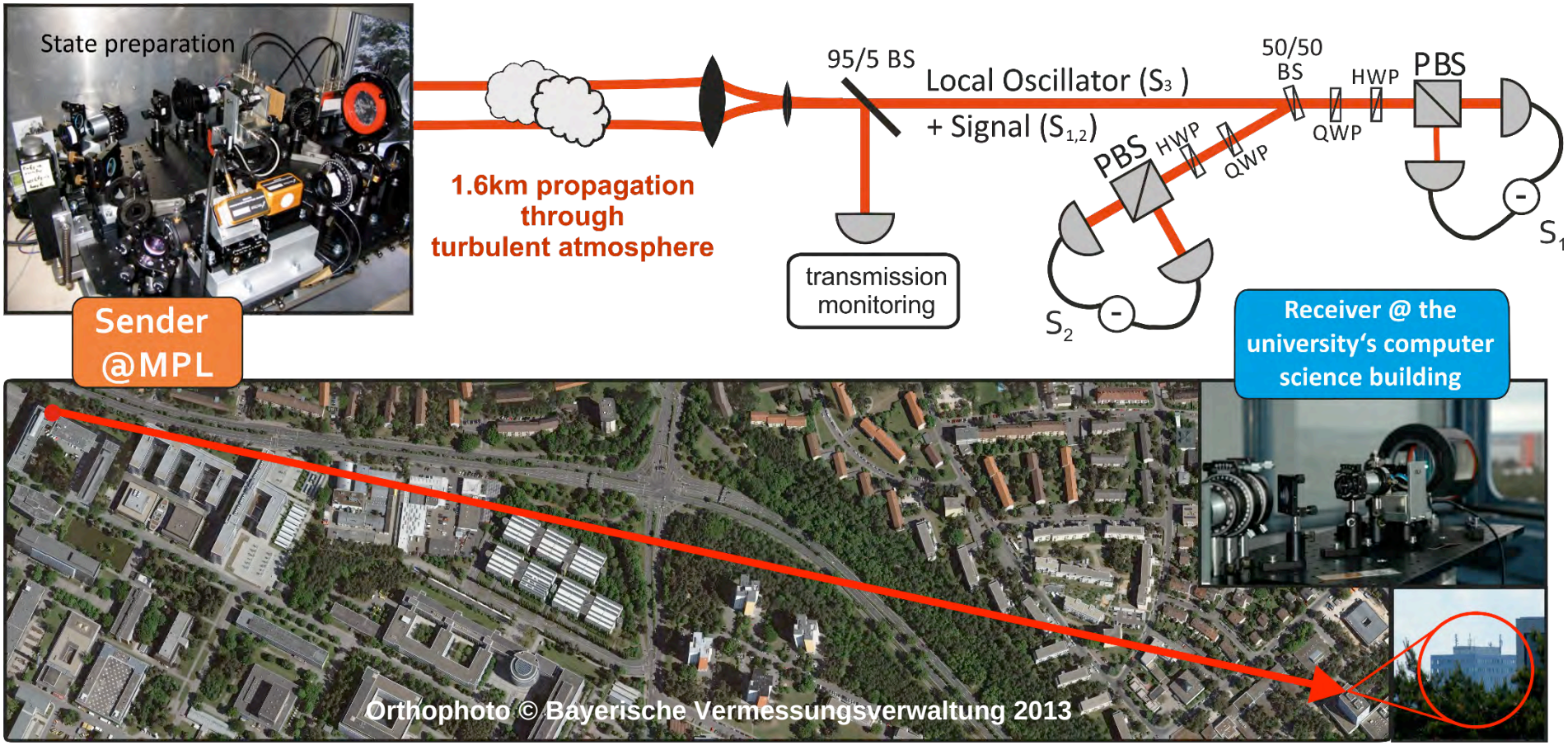
P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti, Nature Photonics 2013

CV-QKD commercial system : Cygnus

Courtesy: SeQureNet

Free-space experiments in Erlangen

Intra-city point-to point link of 1.6 km
Free space implementation → polarization encoding → immune to wavefront distortions
Stokes measurement of intense light modes → homodyne detection



Practical security assurance

- Deviations of security proof assumptions from real implementations open the way to hacking
- Hacking helps improve the practical security of QKD

- Side channel attack based on ubiquitous calibration procedures

  → countermeasure: **real-time shot noise evaluation**

  P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A 2013

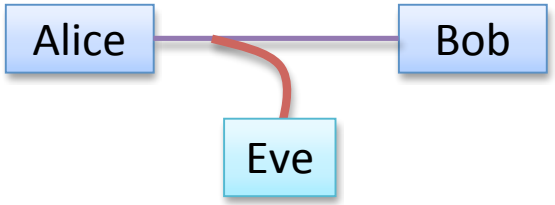
  - Trojan horse-type of attack on commercial CV-QKD system

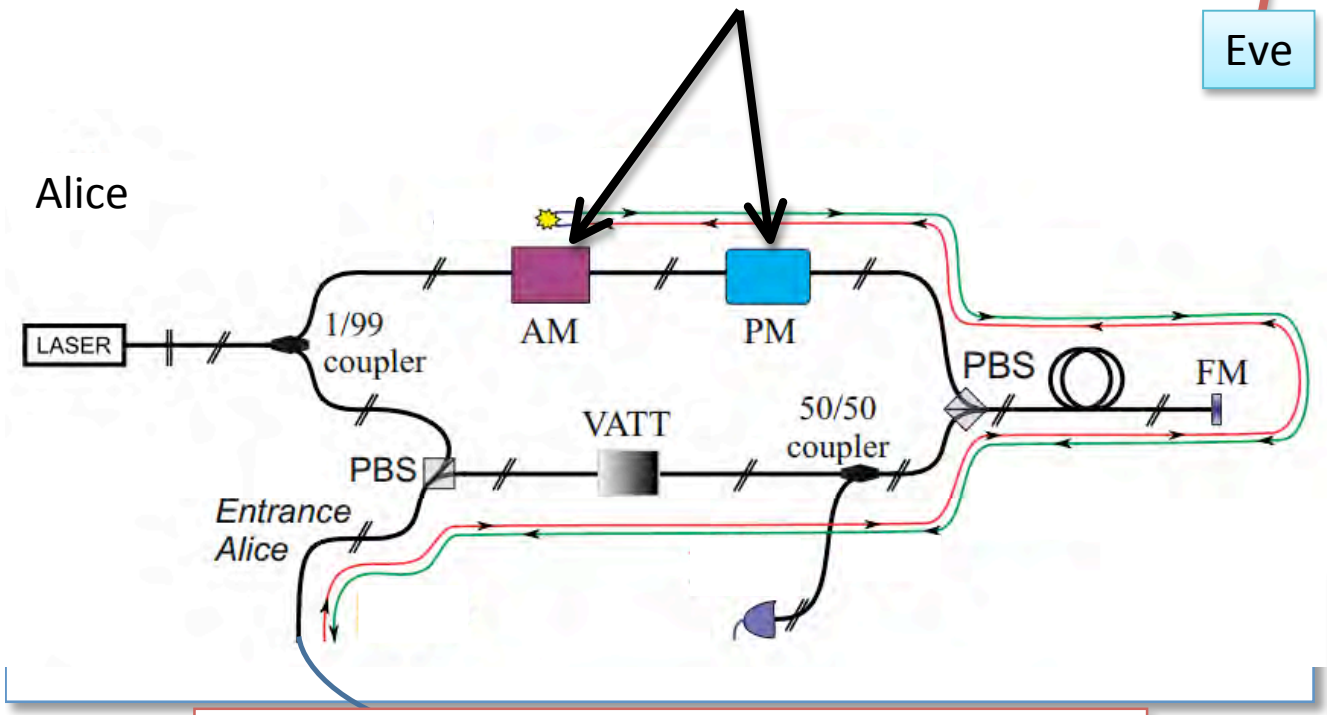
    HIPERCOM collaboration: Paris – Erlangen

Trojan horse attack on commercial CV-QKD system

Objective of the eavesdropper Eve

•read out the state of Alice's modulators



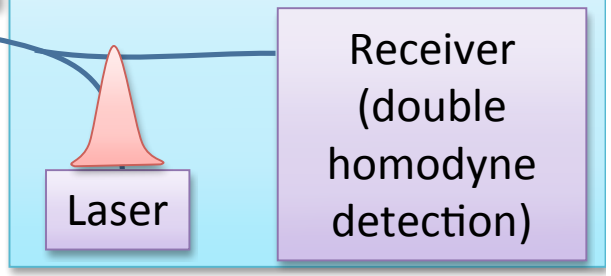


Eve's required knowledge

•temporal information

•attenuation of components inside the system

Eve's portable attack setup



Current progress

•Building Eve's attack apparatus

•Theoretical analysis of information Eve may obtain from the Trojan horse pulse which contains Alice's modulator setting