Manipulating Gaussian and Non-Gaussian States of the Light : New Tools for Quantum Communications

Franck Ferreyrol [1], Marco Barbieri [1], Alexei Ourjoumtsev [1],
Jérome Wenger [2], Julien Laurat [3], Aurélien Dantan [4],
Simon Fossier [5], Eleni Diamanti [1], Thierry Debuisschert [5],
Rosa Tualle-Brouri [1], and Philippe Grangier [1]

1 Laboratoire Charles Fabry de l'Institut d'Optique, 91127 Palaiseau, France
2 : Institut Fresnel, Marseille 3 : LKB-ENS, Paris 4 : U. Aarhus, Denmark
5 : Thales Research and Technology, Palaiseau, France

IST / FET European Projects :
« COVAQIAL » & « COMPAS »

WP 1 Design of photonic components of CV quantum computing

T1.4 Investigating measurement-induced CV information processes
EXP: CNRS/IO TH: ULB, UP, POTSDAM
D1.5 (Y2) Measurement-induced nonlinear operations.

WP2 Design of atomic components of CV quantum computing

T2.3 Investigating alternative schemes for photonic and/or atomic quantum gates
EXP: CNRS/ENS, (CNRS/IO) TH: MPG, (USTAN)
D2.4 (Y2) Alternative methods using Kerr nonlinearity.

WP3 Demonstration of mesoscopic CV quantum processors

T3.2 Demonstrating CV quantum error correction
EXP: DTU TH: USTAN, (ULB), (UP)
D3.3 (Y2) Demonstration of CV quantum error correction.

WP 1 Design of photonic components of CV quantum computing

T1.4 Investigating measurement-induced CV information processes
EXP: CNRS/IO TH: ULB, UP, POTSDAM
D1.5 (Y2) Measurement-induced nonlinear operations.

The objective is to analyze the measurement-induced nonlinearity that may be attained by combining linear coupling, single-photon counting, homodyne detection, feedforward or conditioning. Such nonlinear operations are crucial to address universal CV quantum computation and CV entanglement purification.

Several CV information protocols will be realized in order to demonstrate this paradigm, which will then be exploited in WP3 for the realization of computing protocols (see, e.g., T3.1). A toolbox for process tomography will also need to be developed, for assessing the fidelity of the measurement-induced processes.

New ! : Implementation of a non-deterministic noiseless optical amplifier
Franck Ferreyrol, Marco Barbieri, Rémi Blandino, Simon Fossier,
Rosa Tualle-Brouri, & Philippe Grangier
Fits also in WP3 -> will be presented later

WP2 Design of atomic components of CV quantum computing

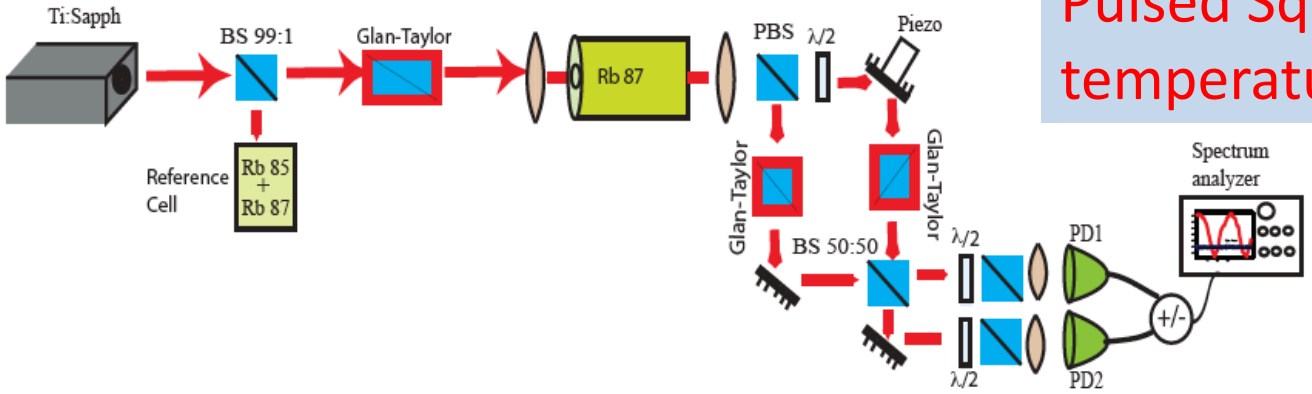
T2.3 Investigating alternative schemes for photonic and/or atomic quantum gates
EXP: CNRS/ENS, (CNRS/IO) TH: MPG, (USTAN)
D2.4 (Y2) Alternative methods using Kerr nonlinearity.

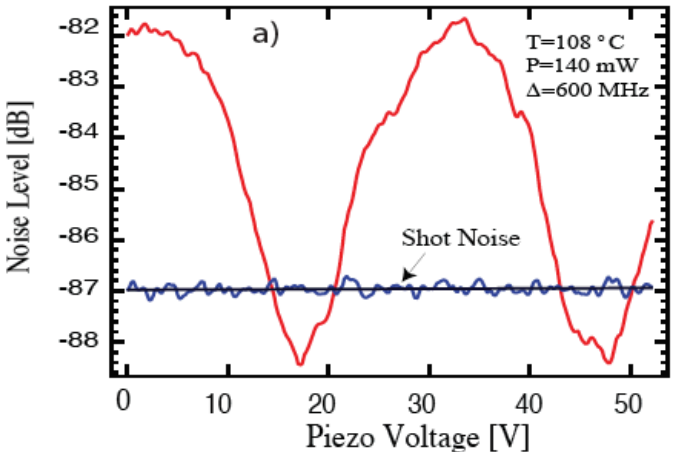
This task will explore novel effects that may potentially be exploited in order to get a very high nonlinear effect. In particular, we will investigate the cross-Kerr effect that arises in an Electromagnetically Induced Transparency-type interaction of light with an atomic system. It is anticipated that the strength of this nonlinear interaction may be orders of magnitude higher.

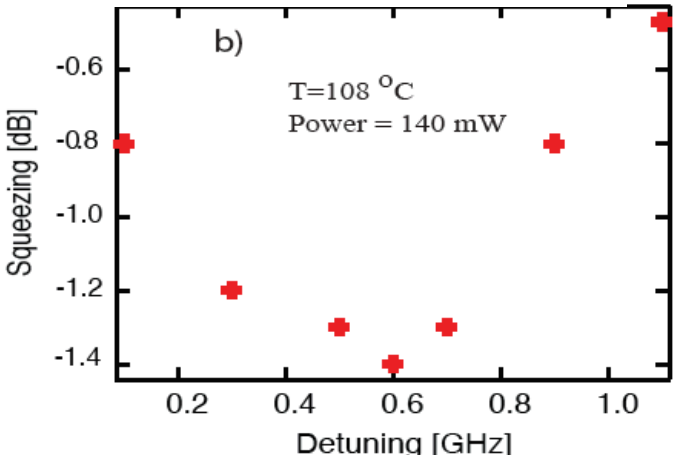
Another research avenue that will be pursued consists in exploring the possibilities offered by atoms trapped in optical lattices. These lattices could be used to create specific photonic states, useful for CV information processing. Alternatively, the photons could be used to detect atomic states. This may be a clever way to perform highly non-Gaussian operations.

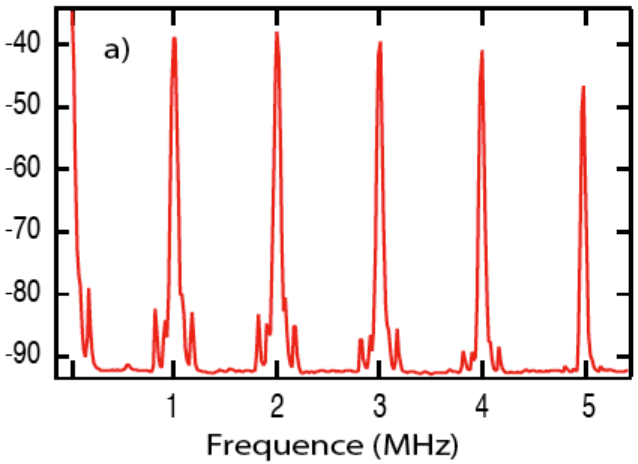
New! : Generation of continuous-wave and pulsed squeezed light with Rb87 vapor
Imad H. Agha, Gaetan Messin, and Philippe Grangier
arXiv:0911.2918, submitted to Optics Express

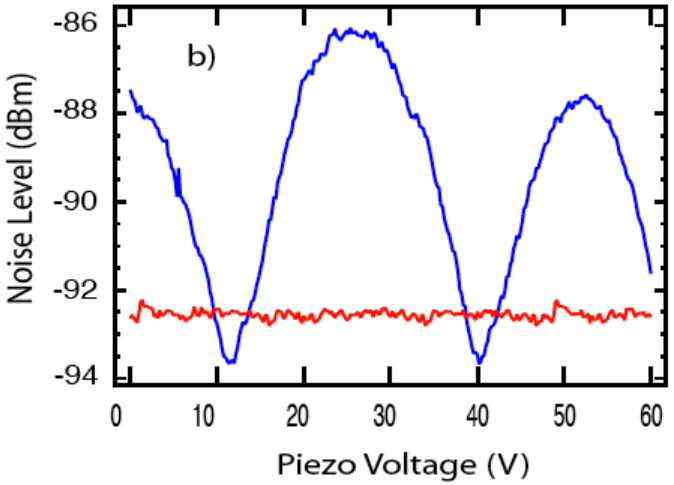
Pulsed Squeezing in a room-temperature Rubidium cell











Imad Agha, Gaëtan Messin, Ph. G. arXiv:0911.2918

CW Squeezing
@ 3 MHz
1.4 dB observed
2 dB corrected

Pulsed Squeezing
(in frequency space
@ 2.7 MHz)
Pulses 200 ns
Rep. rate 1 MHz

WP3 Demonstration of mesoscopic CV quantum processors

T3.2 Demonstrating CV quantum error correction

EXP: DTU TH: USTAN, (ULB), (UP)

D3.3 (Y2) Demonstration of CV quantum error correction (in a generalized sense…).

We will develop quantum protocols for the correction (or detection) of errors (or erasures) that are suitable to CV information carriers. These protocols, in which information is encoded into a CV multipartite entangled mesoscopic state, should be useful for circumventing the noise in distributed quantum computing networks. This issue is directly linked to the circuit-based model studied in T1.2.

*** Quantum repeaters with entangled coherent states** (theory)

Nicolas Sangouard, Christoph Simon, Nicolas Gisin, Julien Laurat, Rosa Tualle-Brouri, Philippe Grangier

Submitted to JOSA B Special Issue on Quantum Technologies (Eds : G. Morigi, A. Jordan, P. Grangier)

*** Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers** (theory)

S. Fossier, E. Diamanti, Th. Debuisschert, R. Tualle-Brouri, P. Grangier, J. Phys. B 42, 114014 (2009)

*** Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation** (theory)

Anthony Leverrier and Philippe Grangier, Phys. Rev. Lett. 102, 180504 (2009)

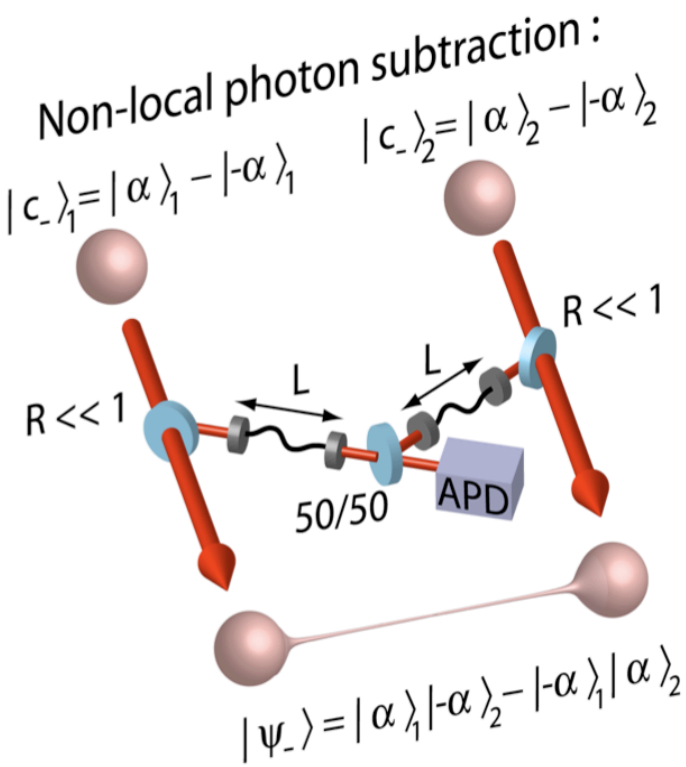
*** Implementation of a non-deterministic noiseless optical amplifier** (exp.)

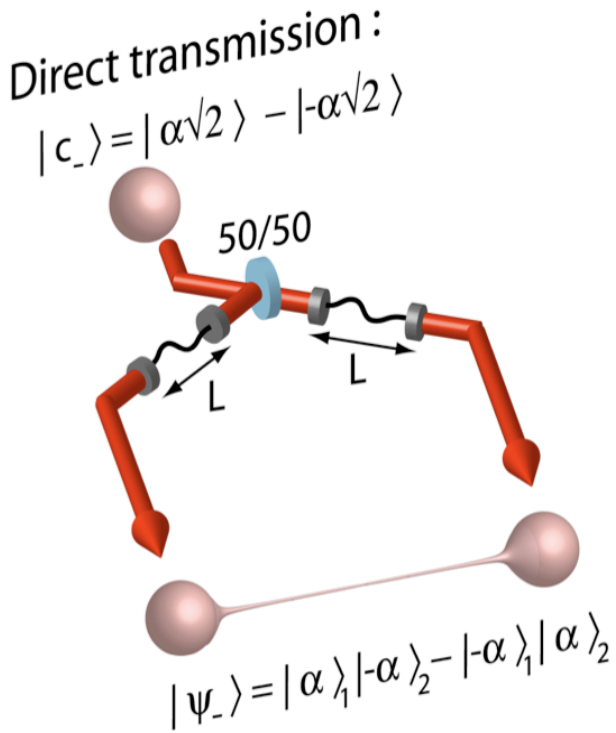
F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, P. Grangier

Quantum repeaters with entangled coherent states

Y1 of COMPAS : new method for remote entanglement of cat states

Main advantage of this scheme : **almost insensitive to transmission losses !**
(the non-local cats are never transmitted in the line)

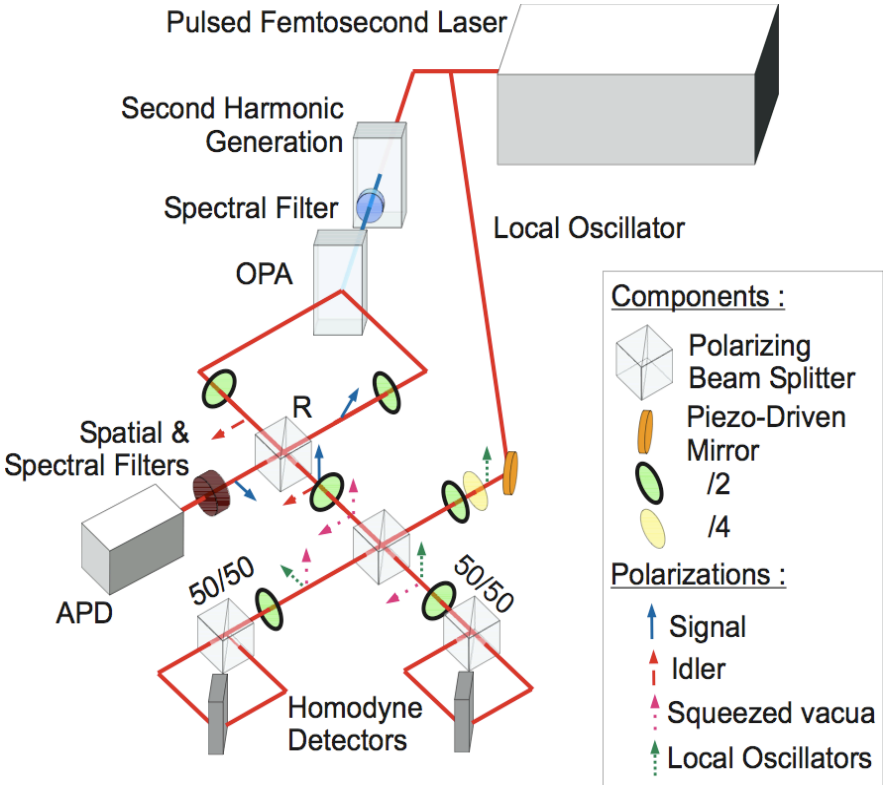


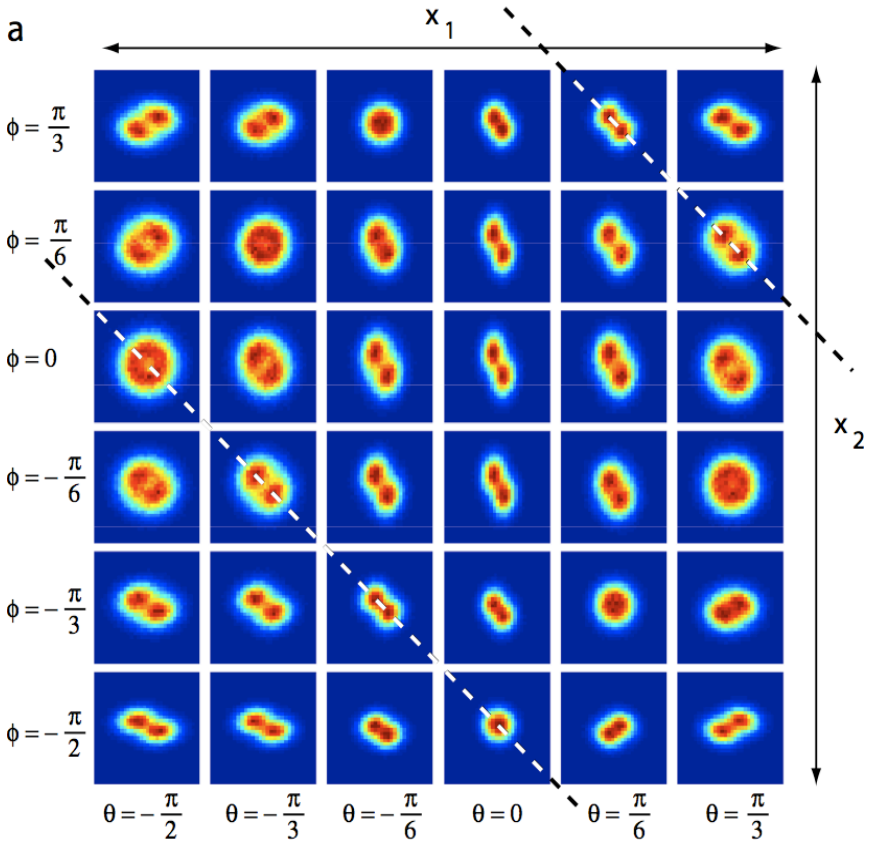


Fidelity for 10 dB losses : **F = 0.4** **F = 0.003**

Experiment

A. Ourjoumtsev et al, Nature Physics, 5, 189, 2009





Experimental set-up

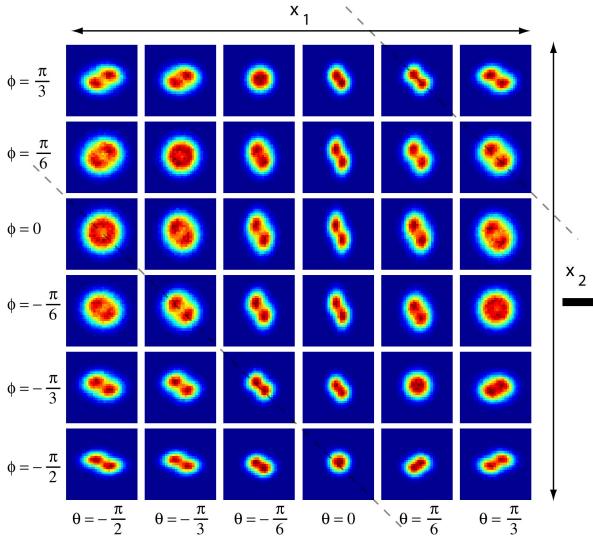
Two-mode probability distributions (two phases ϕ and θ...)

Results

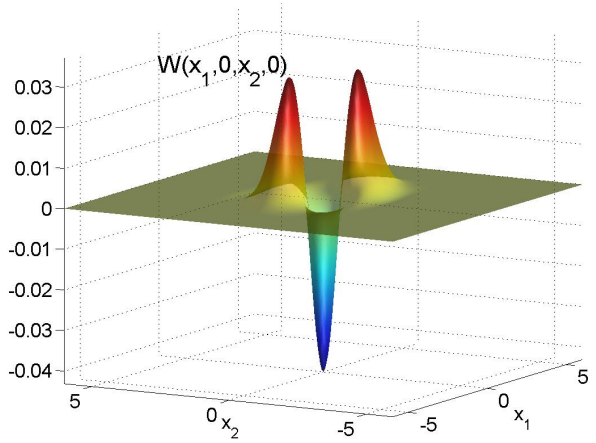
A. Ourjoumtsev et al, Nature Physics, 5, 189, 2009

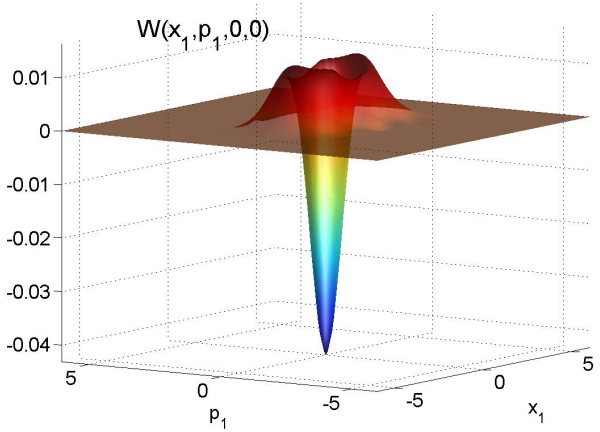
Full two-mode tomography :

$P(x_{1,\theta}, x_{2,\varphi})$



Cuts of the experimental 4D Wigner function, corrected for homodyne losses

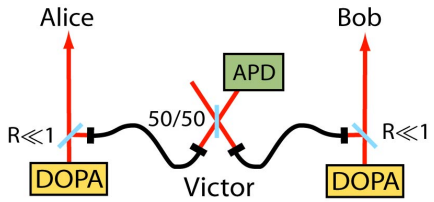




Entanglement : $N = 0{,}25 \pm 0{,}04$

Almost insensitive to losses in the quantum channel !

… but still far from a quantum repeater !



$T_{\text{filters \& APD}} \sim 10\%$:

~ 100 km optical fiber

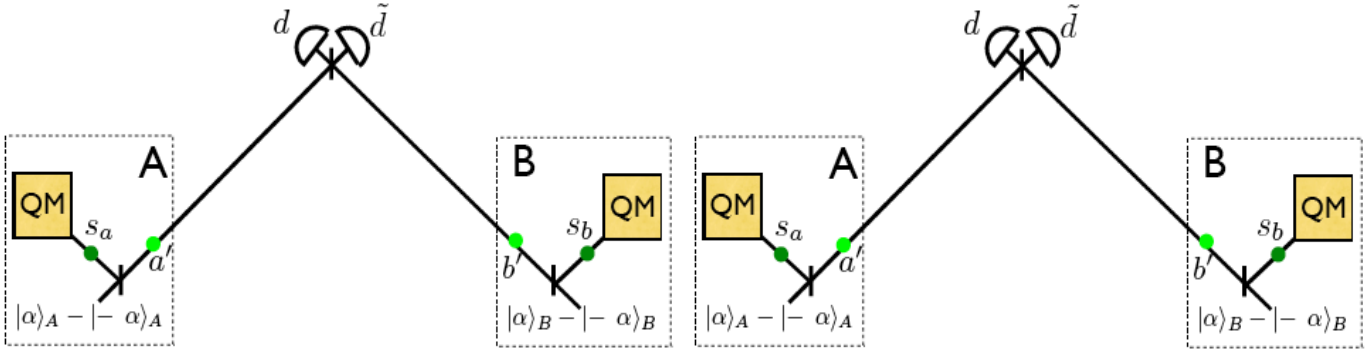
Quantum repeaters with entangled cats ?

coll. with N. Sangouard, C. Simon, N. Gisin

Institut d'Optique

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

QIPC



Bell measurements are deterministic for entangled cats using only BS and photon counters !

$$|\phi_\pm\rangle_{AB} = \frac{1}{\sqrt{M_\pm}}(|\alpha\rangle_A|\alpha\rangle_B \pm |-\alpha\rangle_A|-\alpha\rangle_B)$$
$$|\psi_\pm\rangle_{AB} = \frac{1}{\sqrt{M_\pm}}(|\alpha\rangle_A|-\alpha\rangle_B \pm |\alpha\rangle_A|-\alpha\rangle_B)$$

BS →

$$|\phi_+\rangle \rightarrow |\text{even}\rangle_{\text{out1}}|0\rangle_{\text{out2}},$$
$$|\phi_-\rangle \rightarrow |\text{odd}\rangle_{\text{out1}}|0\rangle_{\text{out2}},$$
$$|\psi_+\rangle \rightarrow |0\rangle_{\text{out1}}|\text{even}\rangle_{\text{out2}},$$
$$|\psi_-\rangle \rightarrow |0\rangle_{\text{out1}}|\text{odd}\rangle_{\text{out2}},$$

But parity measurements (even / odd) are extremely sensitive to losses…

-> To avoid errors one has to use kittens rather than cats

-> Increase of the « failure » probability (getting 0 0)

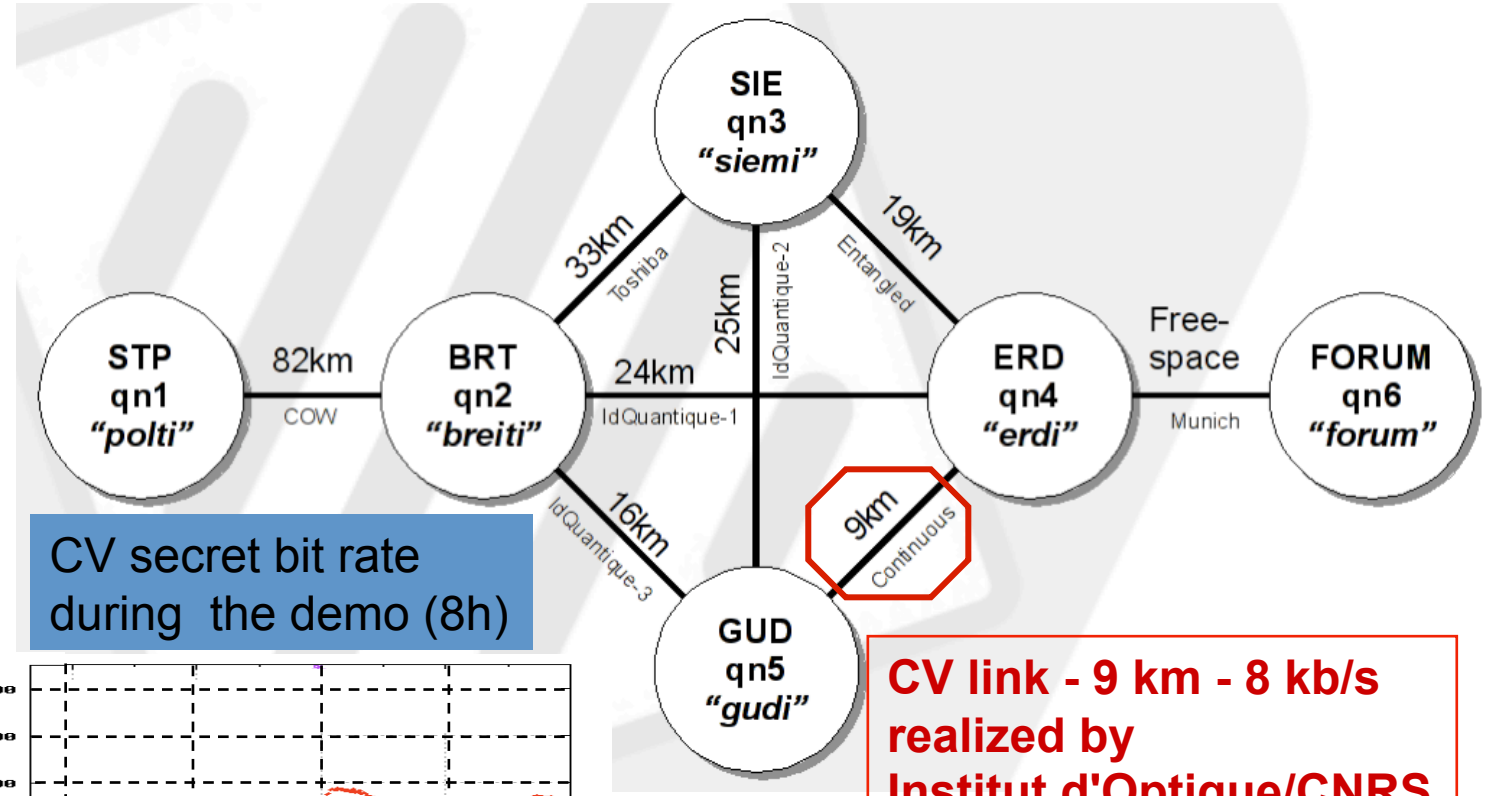
-> Overall not significantly better than using entangled photons :-((

Better hardware needed ! (here : deterministic parity measurement)

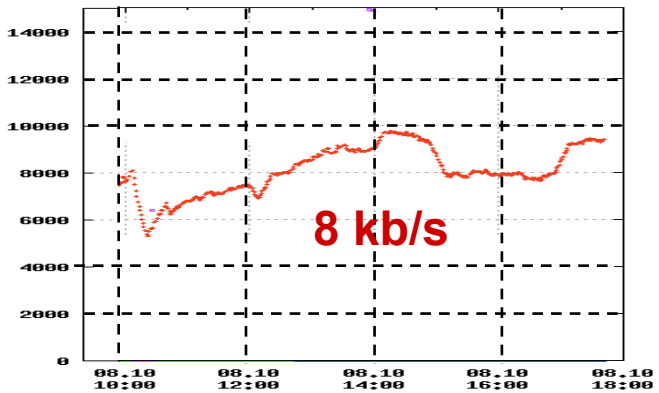
The SECOQC Quantum Back Bone

Real-size demonstration of a **secure quantum cryptography network**

by the European Integrated Project SECOQC, Vienna, 8 october 2008

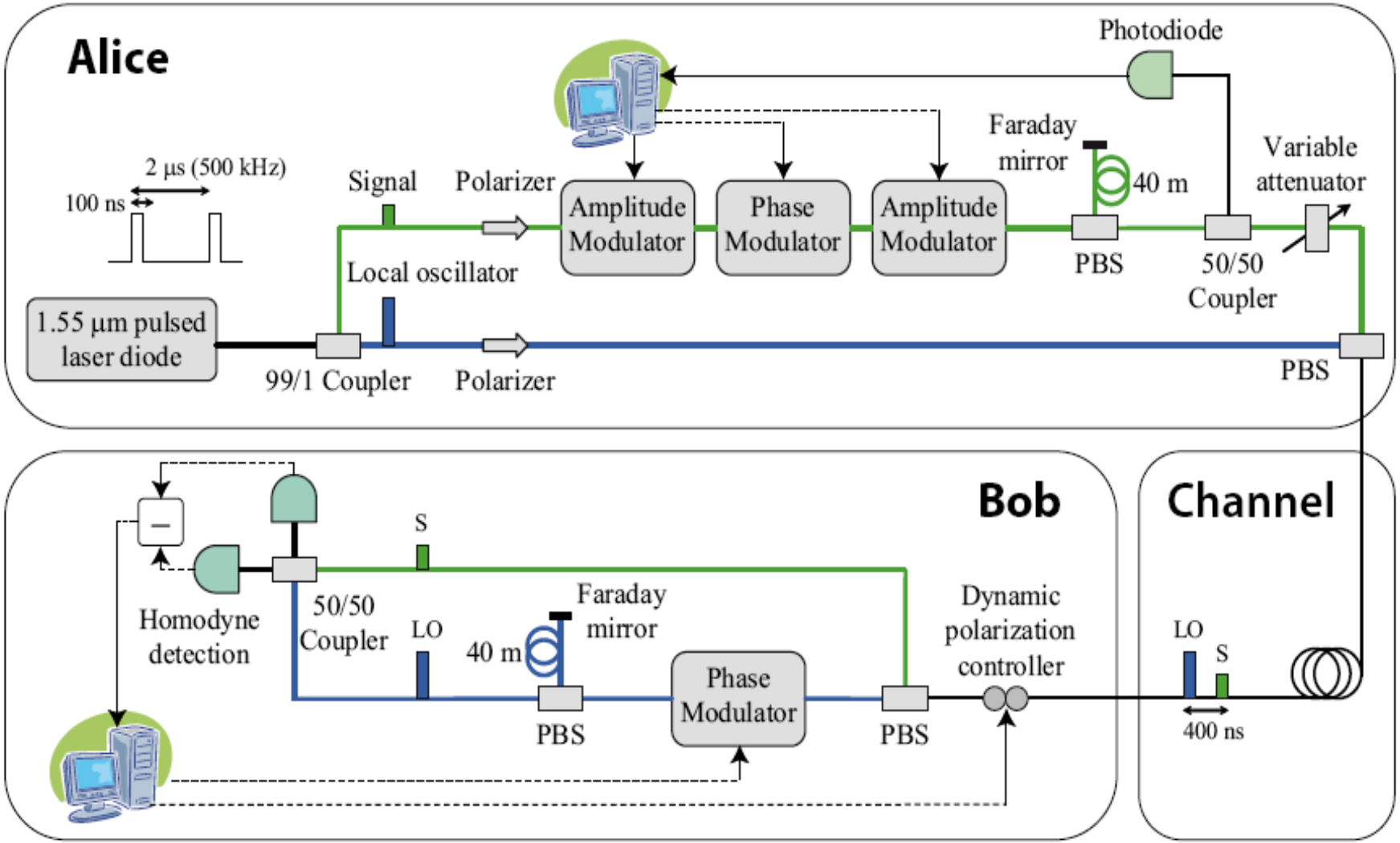


CV secret bit rate during the demo (8h)



CV link - 9 km - 8 kb/s realized by Institut d'Optique/CNRS and Thales (proven fully secure !)

All-fibered CVQKD @ 1550 nm



Field test of a continuous-variable quantum key distribution prototype
S Fossier, E Diamanti, T Debuisschert, A Villing, R Tualle-Brouri and P Grangier
New J. Phys. 11 No 4, 04502 (April 2009)

Security of coherent state CV-QKD protocol

- Security initially proven against (arbitrary) individual attacks :

  F. Grosshans et al, Nature 421, 238 (2003)
  F. Grosshans and N. J. Cerf, Phys. Rev. Lett. 92, 047905 (2004)

- Then security proven against arbitrary collective attacks :

  F. Grosshans, Phys. Rev. Lett. 94, 020504 (2005)
  M. Navasqués and A. Acin, Phys. Rev. Lett. 94, 020505 (2005)

- For both individual and collective attacks Gaussian attacks are optimal
  → Alice and Bob consider Eve's attacks Gaussian and estimate her information using the Shannon quantity I_{BE} or the Holevo quantity χ_{BE}

  M. Navasqués et al, Phys. Rev. Lett. 97, 190502 (2006)
  R. García-Patrón et al, Phys. Rev. Lett. 97, 190503 (2006)

- Very recently proofs of unconditional security (against coherent attacks)
  coherent attacks are not better than collective attacks.

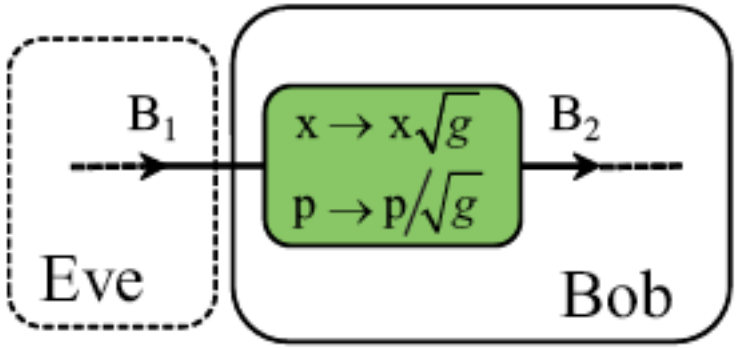
  R. Renner and J. I. Cirac, quant-ph/0809.2243 (september 2008) + PRL 2009

… but maximum distance for secret key distribution limited by « reconciliation efficiency »
(even very good error correcting codes like LDPC do not reach Shannon limit !)

Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers

Simon Fossier, Eleni Diamanti, Thierry Debuisschert, Rosa Tualle-Brouri, Philippe Grangier

J. Phys. B 42, 114014 (2009)



Old trick : using a parametric amplifier can « erase » the imperfections of Bob's detector !

Bob knows the quadrature that he wants to measure : noiseless amplification !

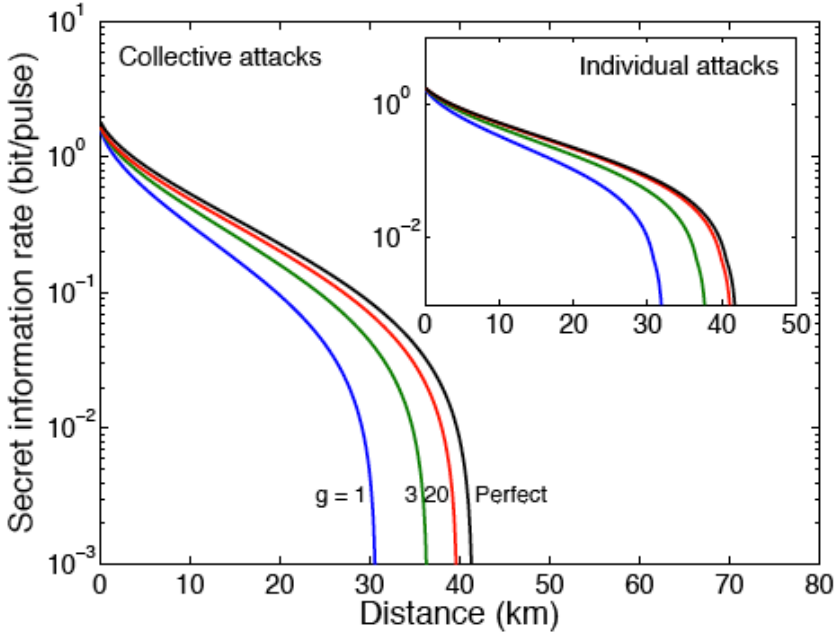


FIG. 3: Secret key generation rate as a function of distance for a protocol with *homodyne detection* and a *phase-sensitive amplifier*, in the case of collective (main figure) and individual (inset) eavesdropping attacks. The 'perfect' curve corresponds to a perfect homodyne detector ($\eta = 1$, $v_{el} = 0$) and no amplifier.

Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation

Anthony Leverrier and Philippe Grangier, Phys. Rev. Lett. 102, 180504 (2009)

Idea : use a discrete modulation with 4 coherent states only

For small amplitude very close to gaussian : security theorems do apply !

But the error correcting codes work much better with discrete modulation !

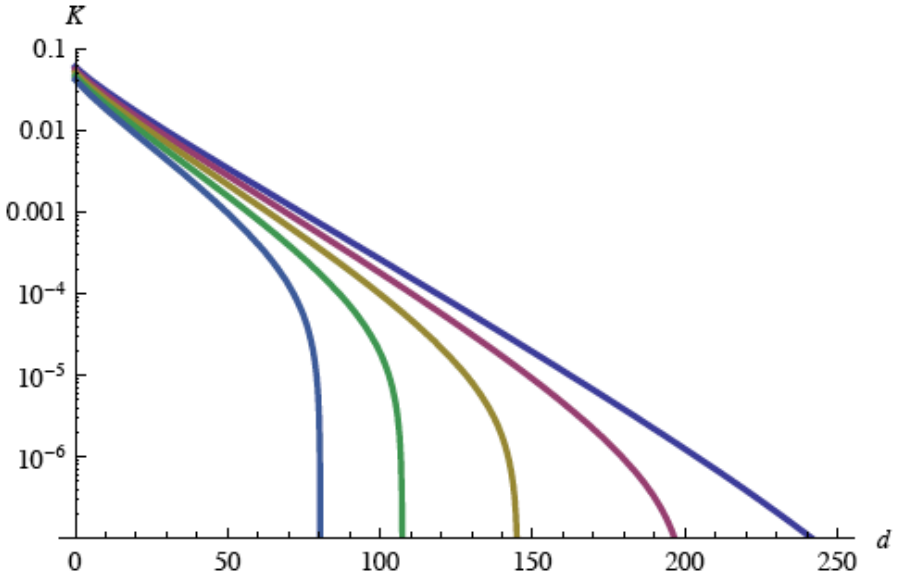
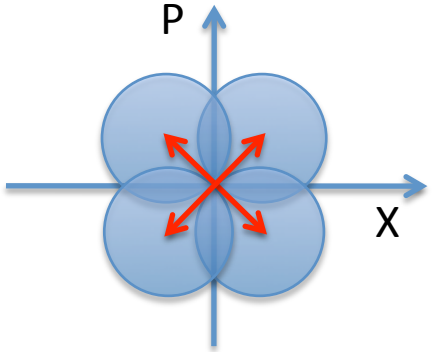


Figure 6: (Color online.) Secret key rate of the four-state protocol for a imperfect, realistic reconciliation efficiency of 80% and a quantum efficiency of Bob's detection equal to 0.6. From top to bottom, excess noise is 0.002, 0.004, 0.006, 0.008 and 0.01. The modulation variance (in number of photons) is 0.125, that is $V_A = 0.25$.



Long distances can be reached with realistic values (both for the quantum encoding and the classical decoding)

Expt under way…

Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation

Anthony Leverrier and Philippe Grangier Phys. Rev. Lett. 102, 180504 (2009)

Idea : use a discrete modulation with 4 coherent states only
For small amplitude very close to gaussian : security theorems do apply
But the error correcting codes work much better with discrete modulation !

$$|\Phi_4\rangle = \frac{1}{2}\left(|\psi_0\rangle|\beta\rangle + |\psi_1\rangle|-\beta^*\rangle + |\psi_2\rangle|-\beta\rangle + |\psi_3\rangle|\beta^*\rangle\right)$$

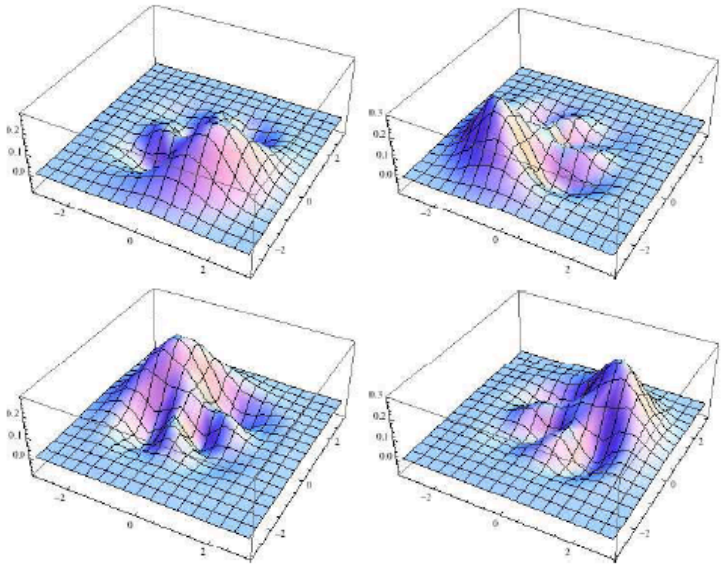


Figure 1: (Color online.) States $|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle$ and $|\psi_3\rangle$ for $\alpha^2 = 0.5$ unit of shot noise.

Actually it is a quantum code :

* 4 non-orthogonal (gaussian) coherent states at Bob's side

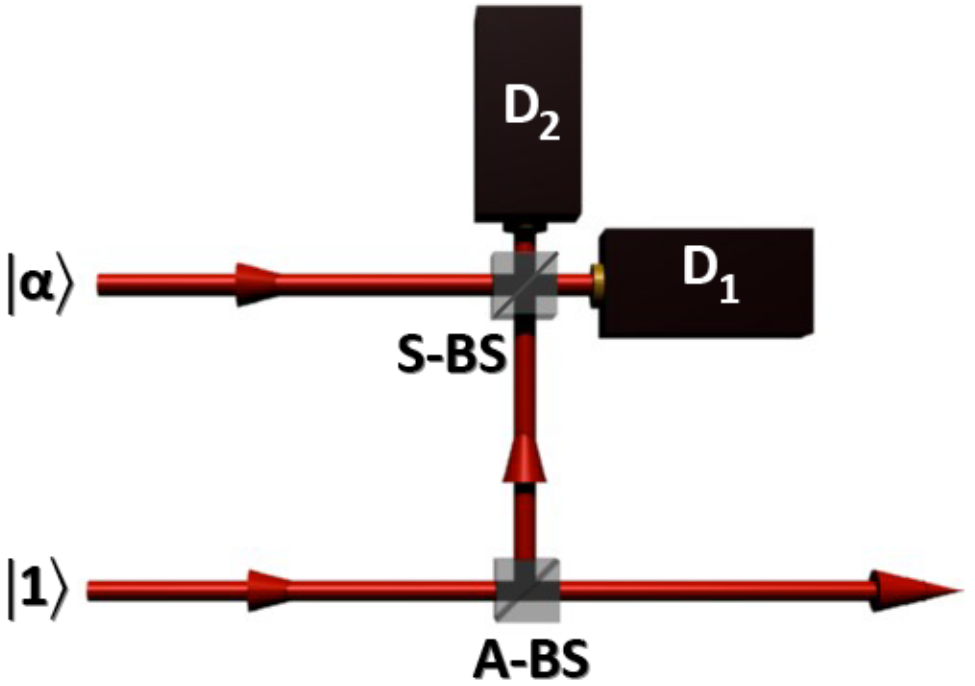
entangled with

* 4 orthogonal (non-gaussian) quantum states at Alice's site !

This entangled state is required to calculate the secret bit rate (using Holevo information)

Implementation of a non-deterministic noiseless optical amplifier

T.C Ralph and A.P. Lund,
Nondeterministic Noiseless Linear Amplification of Quantum Systems,
arXiv:0809.0326 (2008).



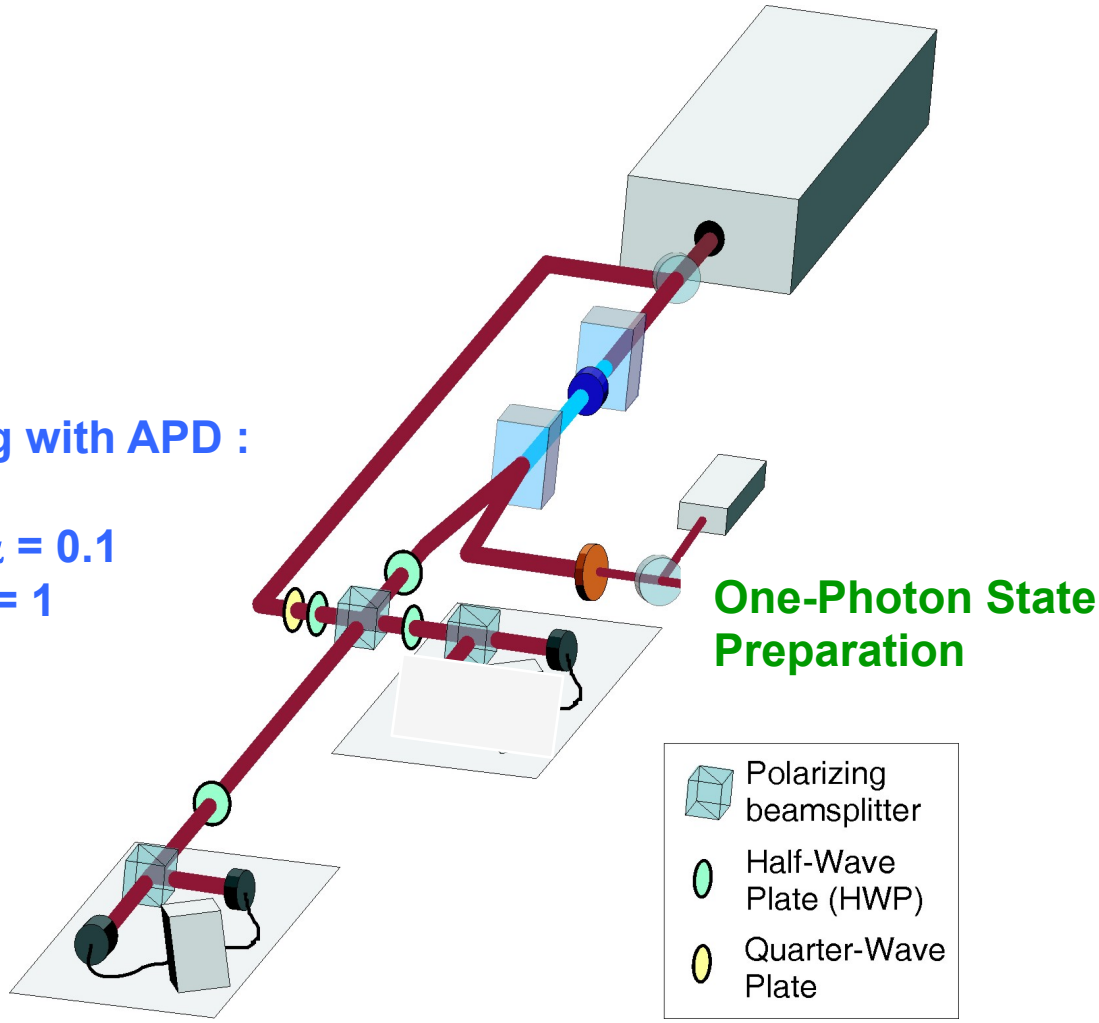
$$|\, g\, \alpha \,\rangle$$

$$g = \frac{\sqrt{1 - r^2}}{r}$$

As such works for small α only !

Basic experimental set-up

Mixing and Conditioning with APD :
Success Probability :
about 1% for $\alpha = 0.1$
up to 6% for $\alpha = 1$



One-Photon State Preparation

Tomographic analysis of the produced state

Violation of QM… ? no !

Example : Gaussian modulation with a small amplitude

$I_{AB} = ½ \log(1 + SNR)$

$I_{AB,\ ampli} = ½ \log(1 + g^2\ SNR) > IAB$!?!

$I_{AB,\ ampli,average} = P_{success}\ I_{AB,\ ampli} = (1-r^2)\ I_{AB} < I_{AB}$

OK !

Interesting question : how to use this amplifier ?