Quantum Communications with Continuous Variables

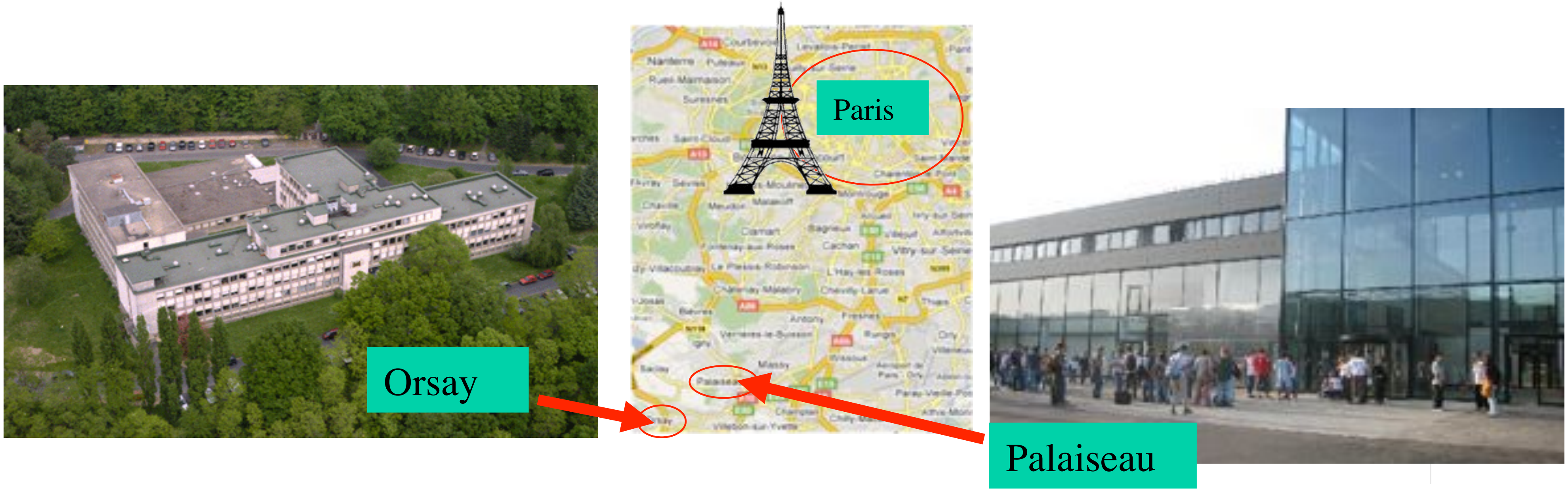
Franck Ferreyrol[1], Rémi Blandino[1], Marco Barbieri[1], Alexei Ourjoumtsev[1], Jérome Wenger, Frédéric Grosshans, Julien Laurat, Aurélien Dantan, Simon Fossier[2], Jérôme Lodewyck, Eleni Diamanti, Thierry Debuisschert[2], Rosa Tualle-Brouri[1], and Philippe Grangier[1]

1 Laboratoire Charles Fabry de l'Institut d'Optique, 91127 Palaiseau, France
2 : Thales Research and Technology, 91127 Palaiseau, France

IST / FET / ERANET European Projects :
« COVAQIAL », « COMPAS », « HIPERCOM »

Institut d'Optique
Théorique et Appliquée,
Orsay

Institut d'Optique
Graduate School,
Palaiseau



May 20th 2007 | May 30th 2007 | Sept. 30th 2007

INSTITUT d'OPTIQUE GRADUATE SCHOOL

Content of this talk

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

QIPC

1. Survival Kit on Optical Quantum Continuous Variables

*** Pulsed homodyne detection and quantum tomography**

Positive and negative Wigner functions

*** Schrödinger's kittens and cats…**

A. Ourjoumtsev et al, Science 312, 83 (2006), Nature 448, 784 (2007)

*** Quantum Key Distribution with continuous variables**

Gaussian and non-Gaussian (unconditional) security proofs

A. Leverrier et al, PRL 102, 180504 (2009)

2. New Results and Perspectives for Quantum Communications with QCV

*** Delocalized (entangled) Schrödinger's kittens**

A. Ourjoumtsev et al, PRL 98, 030502 (2007), Nat. Phys. 5, 189 (2009)

*** Non-deterministic Noiseless Amplifier (tomorrow !)**

F. Ferreyrol, M. Barbieri et al, PRL 104, 123603 (2010)

INSTITUT d'OPTIQUE GRADUATE SCHOOL

Optical Quantum Continuous Variables

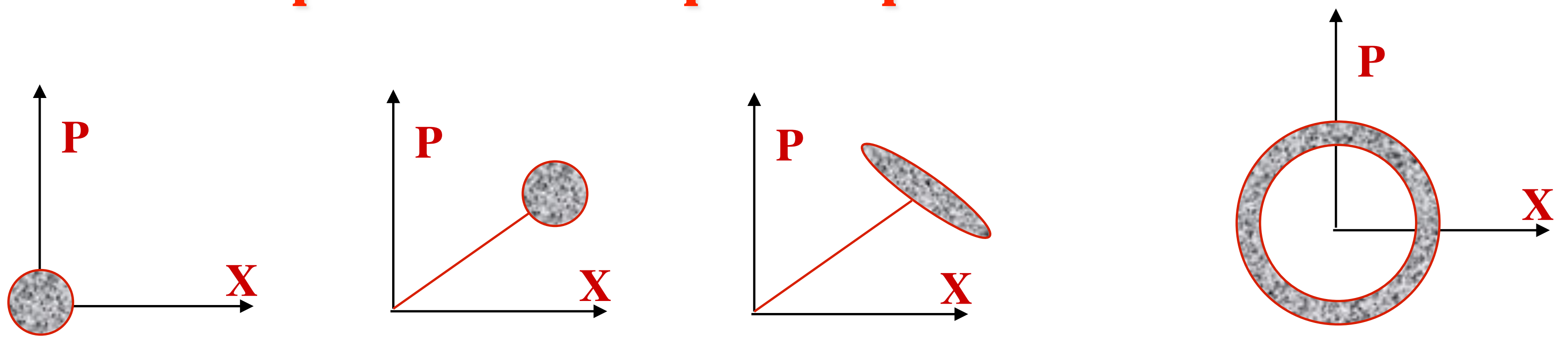
CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

QIPC

*** What are quantum optical continuous variables ?**

- * Quantization of the Electromagnetic field
  - * Modes are quantum harmonic oscillators
  - * Discrete degrees of freedom (photon number)
  - * Continuous degrees of freedom (quadratures = X and P)
- *** All is about quantized harmonic oscillators !**

*** Convenient representation : phase space**



Vacuum state | Coherent state | Squeezed state | Number state

Wigner function : Gaussian | **Non-Gaussian !**

Homodyne detection

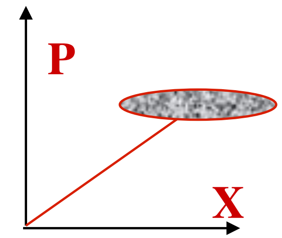
$$I_1 = |E_{LO}|^2 + |E_S|^2 + |E_{LO}| (E_S\, e^{-i\varphi LO} + E_S^*\, e^{i\varphi LO})$$

$$I_2 = |E_{LO}|^2 + |E_S|^2 - |E_{LO}| (E_S\, e^{-i\varphi LO} + E_S^*\, e^{i\varphi LO})$$

$$I_1 - I_2 = 2\,|E_{LO}| (E_S\, e^{-i\varphi LO} + E_S^*\, e^{i\varphi LO})$$

$$= 2\,|E_{LO}| (E_S + E_S^*) \qquad \textbf{X meas.}$$

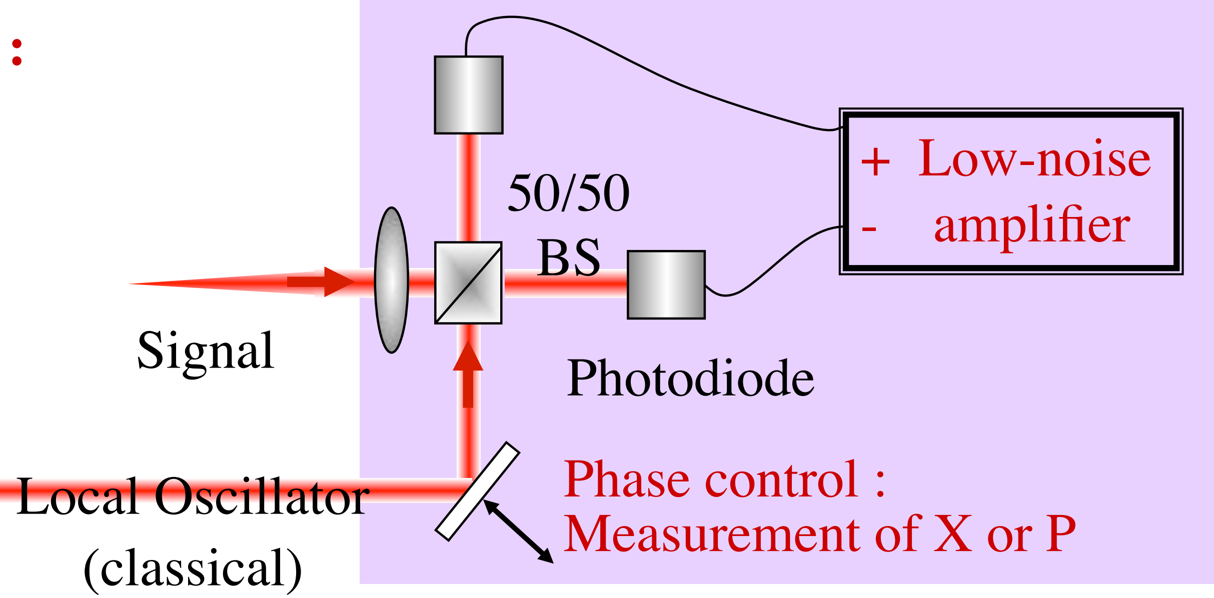
$$= 2\,|E_{LO}|\, i\, (E_S - E_S^*) \qquad \textbf{P meas.}$$



Squeezed state

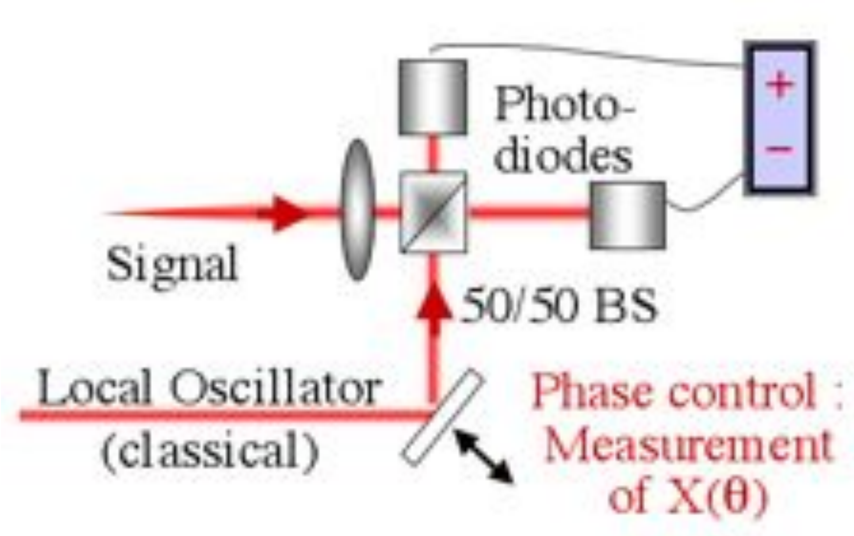
X and P do not commute : Heisenberg relation

$$V(X)\ V(P) \geq N_0^2$$



Homodyne detection,
Wigner Function and Quantum Tomography

QIPC

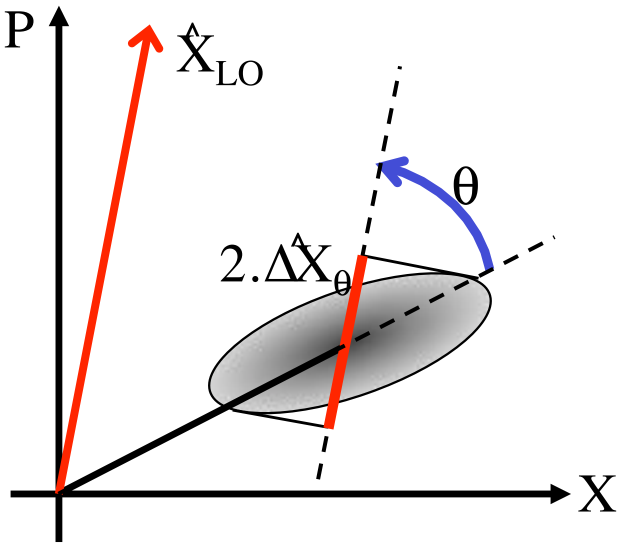


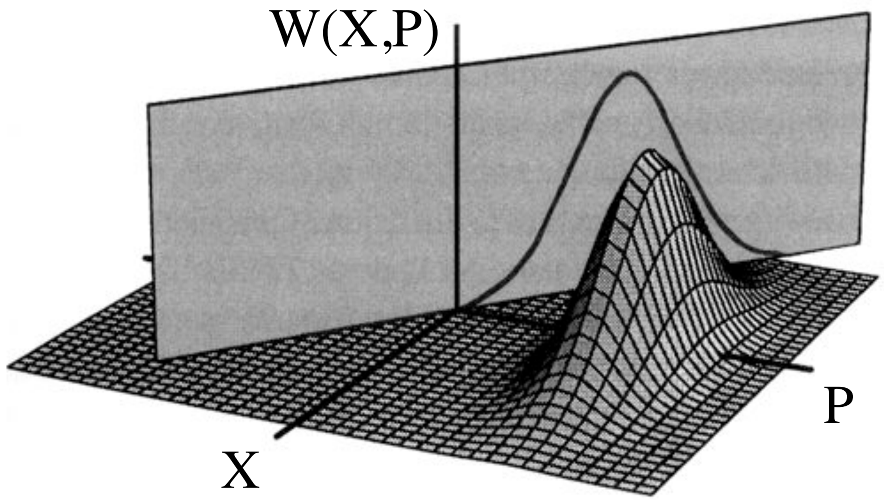
- **Quasiprobability density :**

  Wigner function W(X,P)
- **Marginals of W(X, P)**

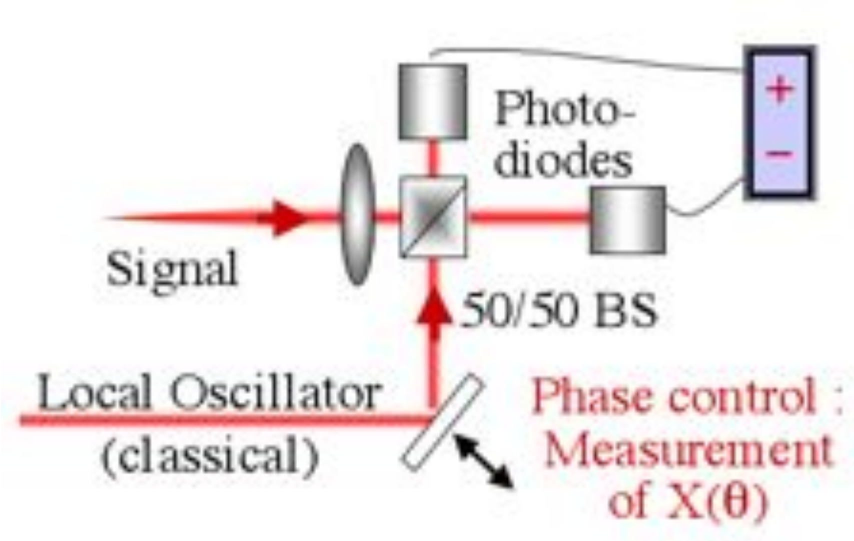
  => Probability distributions $\mathcal{P}(X_\theta)$
- **Probability distributions $\mathcal{P}(X_\theta)$**

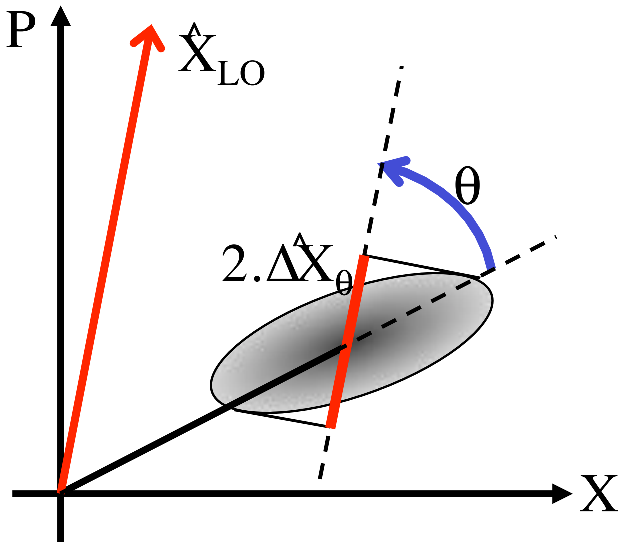
  => W(X, P) (quantum tomography)

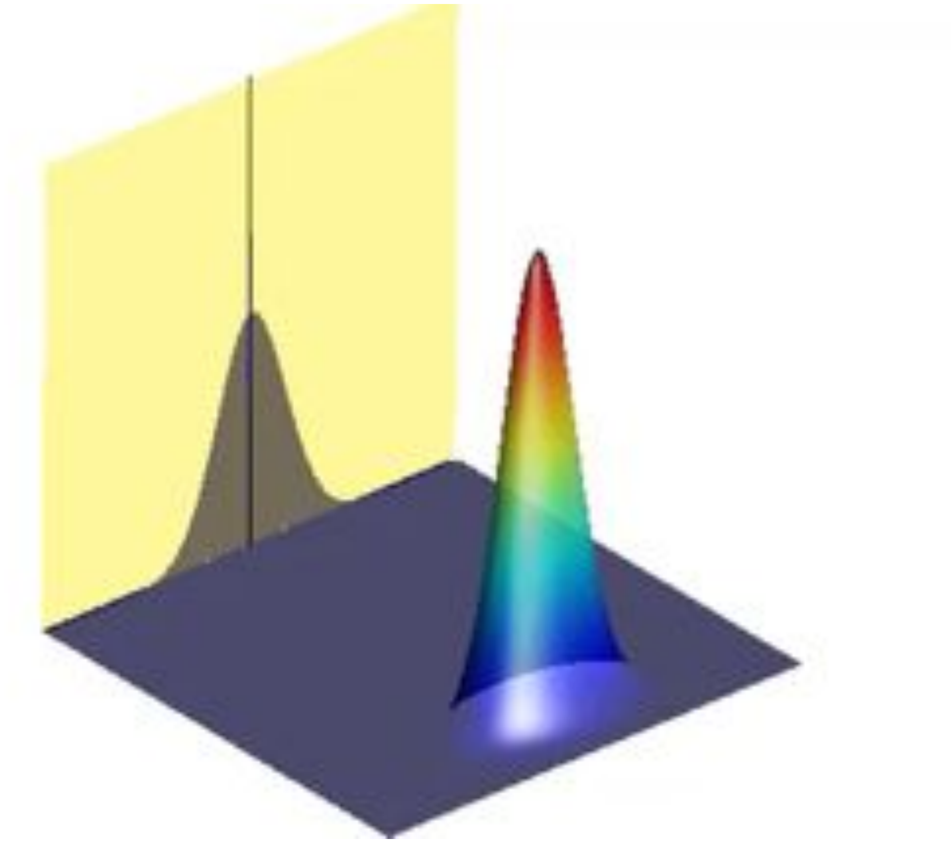




Homodyne detection,
Wigner Function and Quantum Tomography

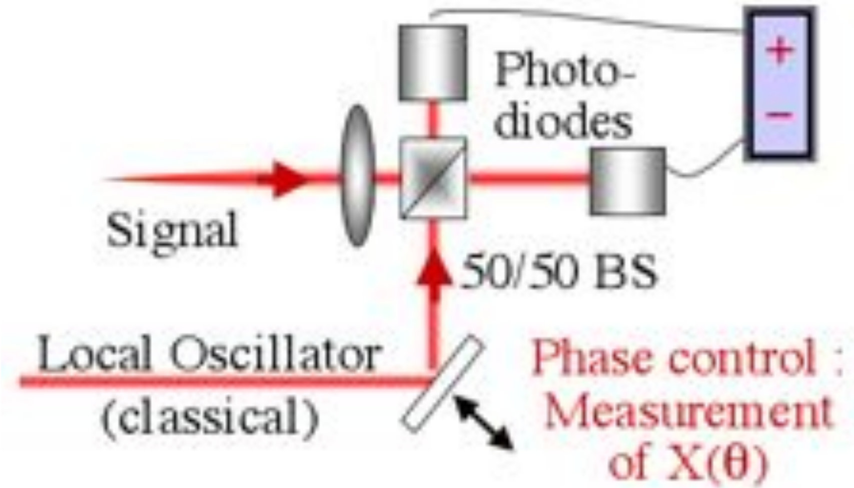


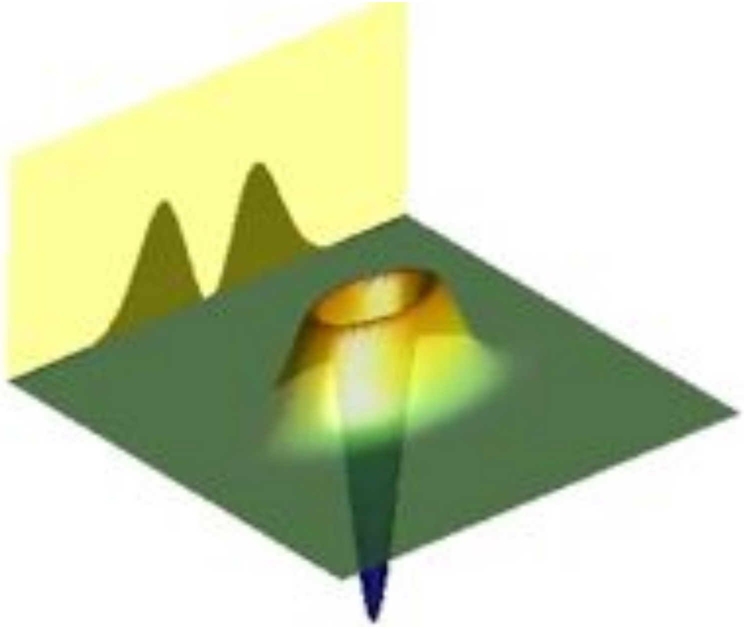


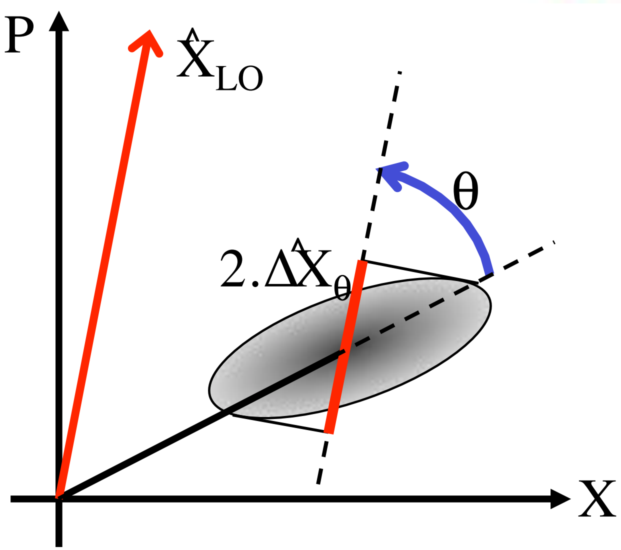


Squeezed State :
Gaussian Wigner Functions

Homodyne detection,
Wigner Function and Quantum Tomography







State with negative Wigner function !

(for a pure state W is non-positive iff it is non-gaussian : Hudson-Piquet theorem)

Many interesting properties for quantum information processing

Wigner function of a single photon state ? (Fock state n = 1)

$$W(p,q) = \frac{1}{2\pi\, 2N_0} \int dx\, e^{\frac{ixp}{2N_0}} \langle\, q - \tfrac{x}{2} \,|\, \hat{\rho} \,|\, q + \tfrac{x}{2} \,\rangle$$

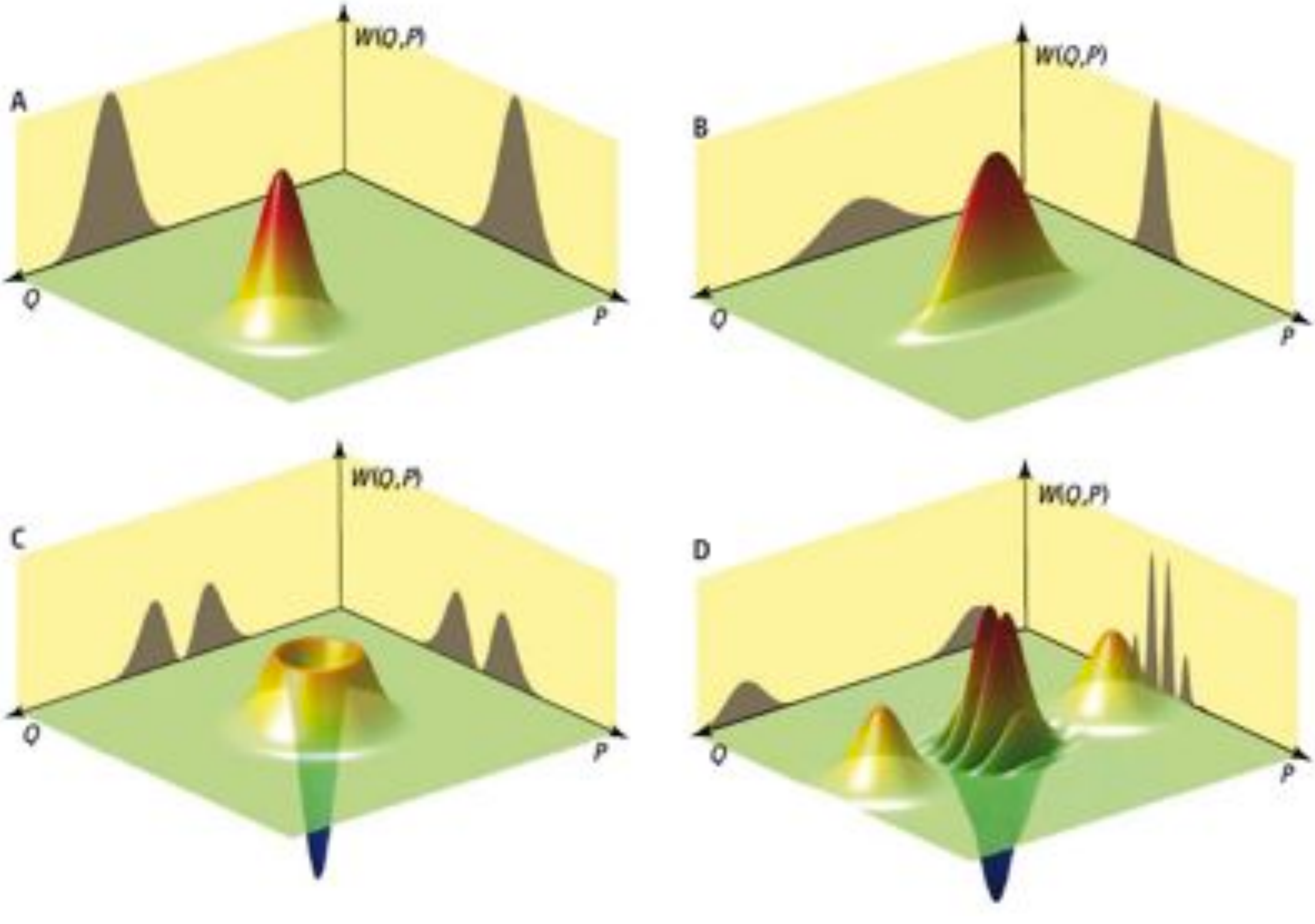
where $\hat{\rho} = |1\rangle\langle 1|$ and N_0 is the variance of the vacuum noise :

$$[\hat{Q}, \hat{P}] \equiv 2iN_0 \qquad \Delta P\, \Delta Q \geq N_0 \qquad N_0 = \Delta P^2 = \Delta Q^2.$$

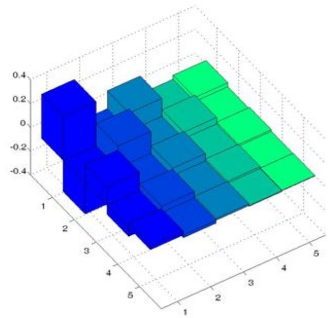
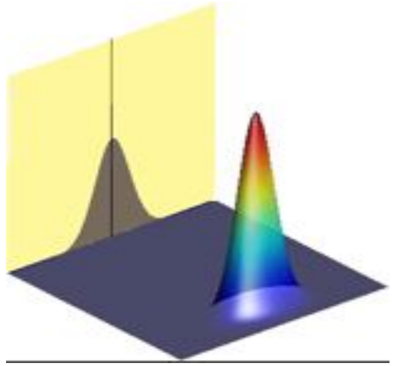
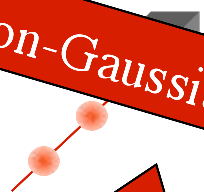
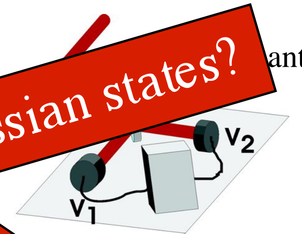
One may have $N_0 = \hbar/2$, $N_0 = 1/2$ (theorists), $N_0 = 1$ (experimentalists)

Using the wave function of the n = 1 state : $\langle\, q \,|\, 1 \,\rangle = \frac{q}{(2\pi)^{\frac{1}{4}} N_0^{\frac{3}{4}}} e^{-\frac{q^2}{4N_0}}$

one gets finally : $W_{|1\rangle}(q,p) = -\frac{1}{2\pi N_0} e^{-\frac{r^2}{2N_0}} \left(1 - \frac{r^2}{N_0}\right) \qquad r^2 = q^2 + p^2$


A
W(Q,P)
Q
P
B
W(Q,P)
Q
P
C
W(Q,P)
Q
P
D
W(Q,P)
Q
P

« Discrete » vs « continuous » Light

Light is :	Discrete Photons	Continuous Wave
We want to know :	their Number & Coherence	its Amplitude & Phase (polar) its Quadratures X & P (cartesian)
We describe it with :	Density matrix $\varrho_{n,m}$ 	Wigner function W(X,P) 
We measure it by :	Counting: APD, VLPC, TES… 	Demodulating : Homodyne Detection 
« Simple » States	ates	tates

Non-Gaussian operations on Gaussian states?

Homodyne measure… n non- Gaussian states?

Make It Quantum and Continuous

Philippe Grangier PERSPECTIVES SCIENCE VOL 332 15 APRIL 2011

Unconditional Quantum Teleportation

A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble,* E. S. Polzik

23 OCTOBER 1998 VOL 282 SCIENCE

Quantum key distribution using gaussian-modulated coherent states

NATURE | VOL 421 | 16 JANUARY 2003 |

Frédéric Grosshans*, Gilles Van Assche†, Jérôme Wenger*, Rosa Brouri*, Nicolas J. Cerf† & Philippe Grangier*

NATURE | VOL 432 | 25 NOVEMBER 2004 | www.nature.com/nature

Experimental demonstration of quantum memory for light

Brian Julsgaard[1], Jacob Sherson[1,2], J. Ignacio Cirac[3], Jaromír Fiurášek[4] & Eugene S. Polzik[1]

Vol 443 | 5 October 2006 | doi:10.1038/nature05136

Quantum teleportation between light and matter

Jacob F. Sherson[1,3], Hanna Krauter[1], Rasmus K. Olsson[1], Brian Julsgaard[1], Klemens Hammerer[2], Ignacio Cirac[2] & Eugene S. Polzik[1]

PHYSICAL REVIEW A **68**, 042319 (2003)

Quantum computation with optical coherent states

T. C. Ralph,* A. Gilchrist, and G. J. Milburn
W. J. Munro S. Glancy

Generating Optical Schrödinger Kittens for Quantum Information Processing

Alexei Ourjoumtsev, Rosa Tualle-Brouri, Julien Laurat, Philippe Grangier*

SCIENCE VOL 312 7 APRIL 2006

Vol 448 | 16 August 2007 | doi:10.1038/nature06054

Generation of optical 'Schrödinger cats' from photon number states

Alexei Ourjoumtsev[1], Hyunseok Jeong[2], Rosa Tualle-Brouri[1] & Philippe Grangier[1]

Teleportation of Nonclassical Wave Packets of Light

Noriyuki Lee,[1] Hugo Benichi,[1] Yuishi Takeno,[1] Shuntaro Takeda,[1] James Webb,[2] Elanor Huntington,[2] Akira Furusawa[1]*

15 APRIL 2011 VOL 332 SCIENCE

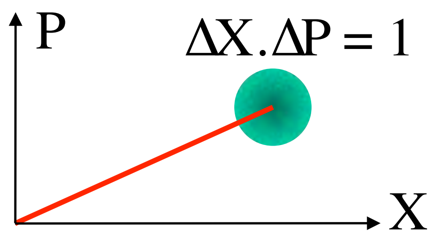
Small sample, many more papers !

Kittens, cats and beyond...

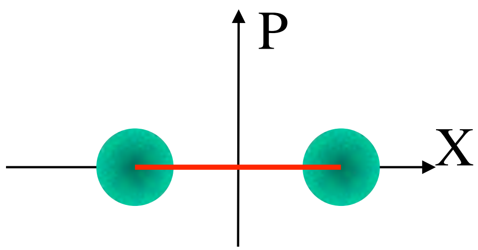
- The magic of photon subtraction...

« Schrödinger's Cat » state

- Classical object in a quantum superposition of distinguishable states
- "Quasi - classical" state in quantum optics : coherent state | α 〉

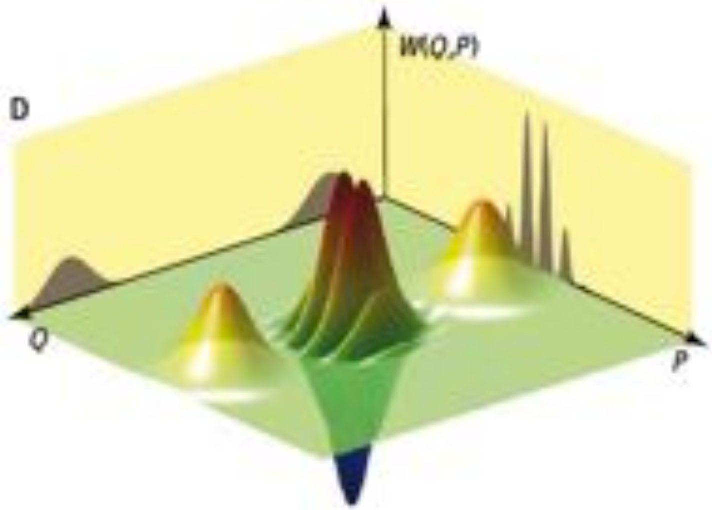


Coherent state



Schrödinger cat state

$$|\psi_{cat}\rangle = c(|\alpha\rangle - |-\alpha\rangle)$$



Wigner function of a Schrödinger cat state

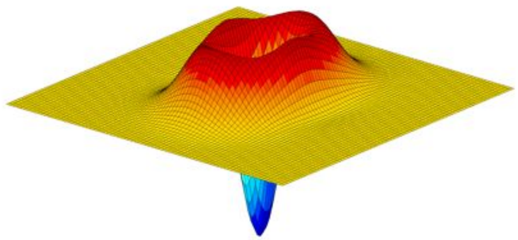
- Resource for quantum information processing
- Model system to study decoherence

« Schrödinger's Kitten »

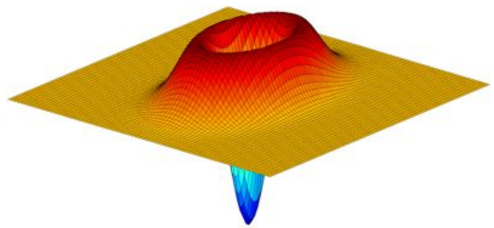
A. Ourjoumtsev et al, Science 312, 83 (2006)

QIPC

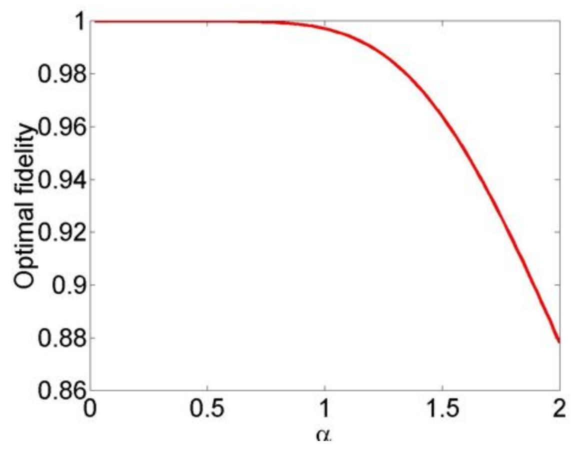
- Odd : $|\Psi\rangle = c\,(|\alpha\rangle - |-\alpha\rangle) = \sum a_n |2n+1\rangle$
- Look at small $|\alpha| \sim 1$
- **Very similar to a squeezed single-photon state**
- **Very similar to a photon-subtracted squeezed vacuum state**



Wigner function of a small Schrödinger cat



Wigner function of a Photon-subtracted squeezed state



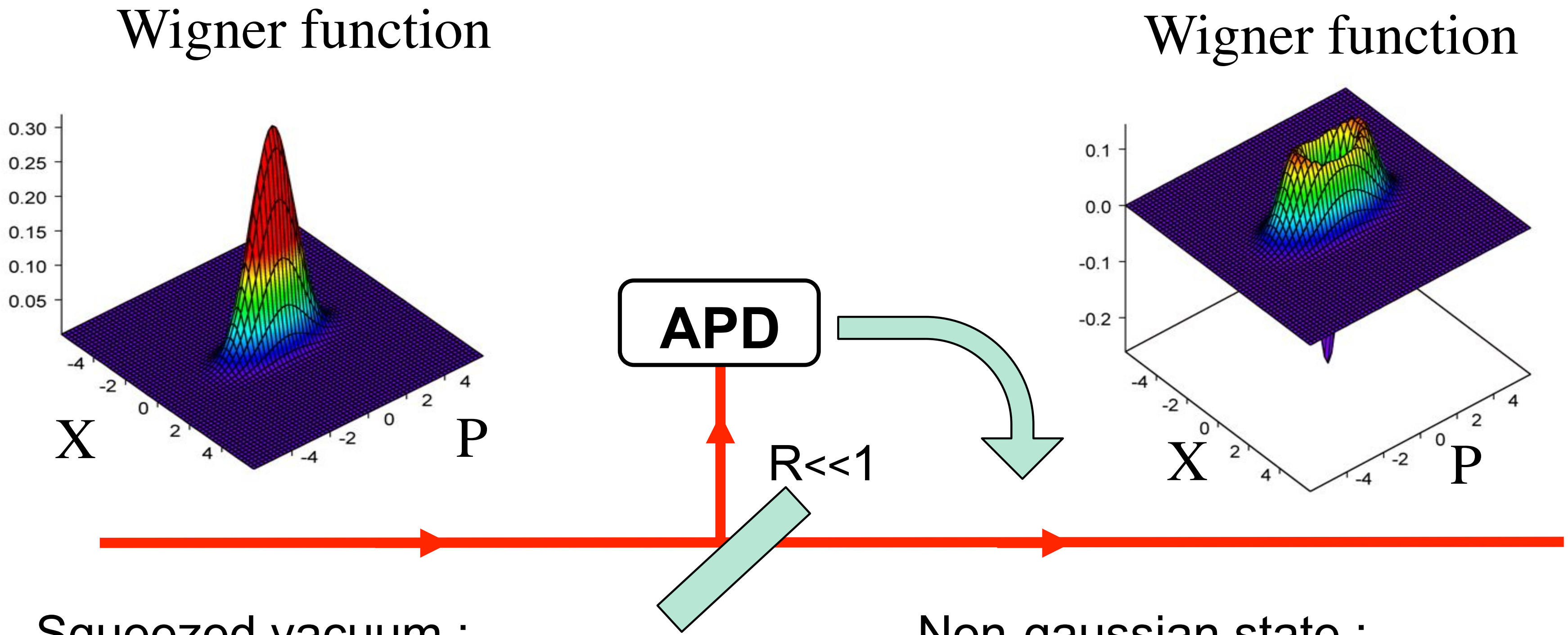
Fidelity between the kitten and the most similar photon-subtracted state

« Degaussification » of a squeezed state

J. Wenger & al., PRL 92, 153601 (2004)

QIPC

A squeezed state can be « degaussified » by photon subtraction (one single photon in the APD beam)



Squeezed vacuum :

$\alpha\,|0\rangle + \beta\,|2\rangle + \gamma\,|4\rangle + \ldots$

Non-gaussian state :

$\sqrt{2}\,\beta\;|1\rangle + \;2\,\gamma\,|3\rangle + \ldots$

Also expts at NBI (Polzik), NICT (Sasaki, Furusawa), NIST (Gerrits), LENS (Bellini), Calgary (Lvovsky)…

Experimental Set-up

QIPC

Special feature: pulsed time-domain analysis

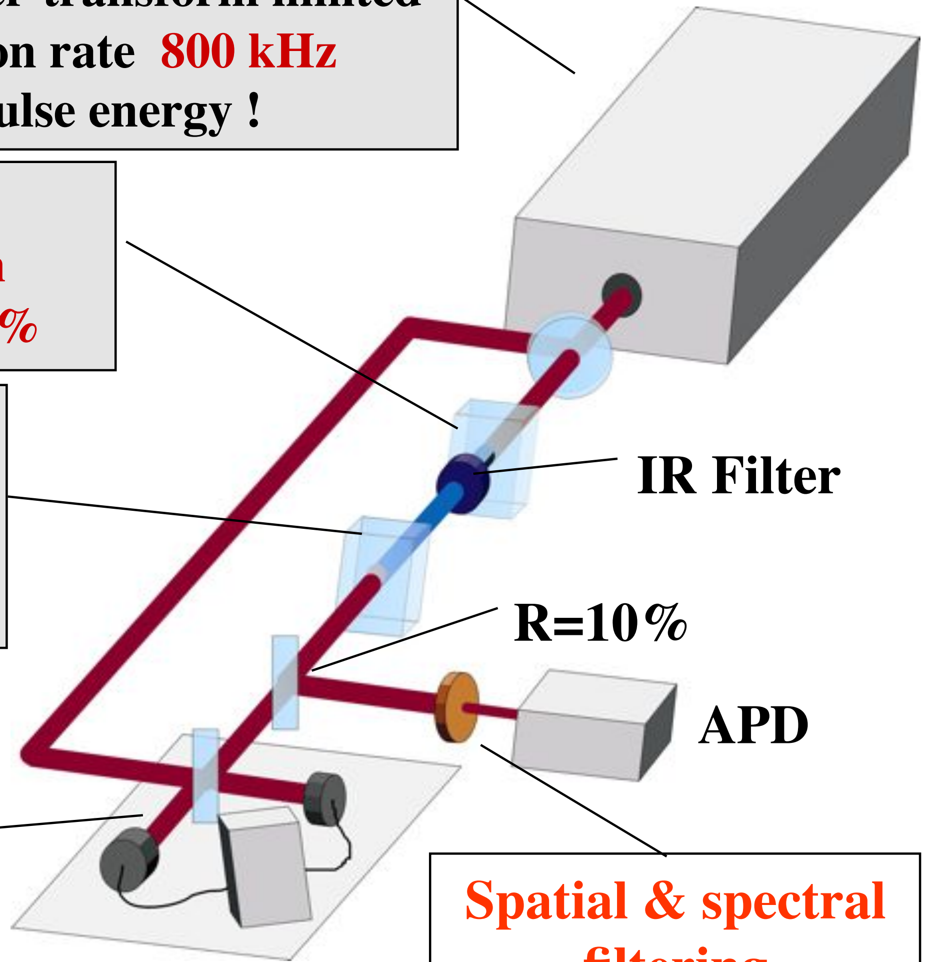
Femtosecond Ti-Sapph laser:
- 180 fs pulses, ≈ Fourier-transform limited
- energy 40 nJ, repetition rate 800 kHz
- cavity dumper : high pulse energy !

Frequence doubling :
- $KNbO_3$ crystal, thickness 100 μm
- Single pass efficiency : $\eta_{SHG} = 30\%$

Parametric amplifier
- $KNbO_3$ crystal, thickness 100 μm
- Degenerate (DOPA) : squeezing
- 3 dB typical squeezing (single pass)

Pulsed Homodyne Detection

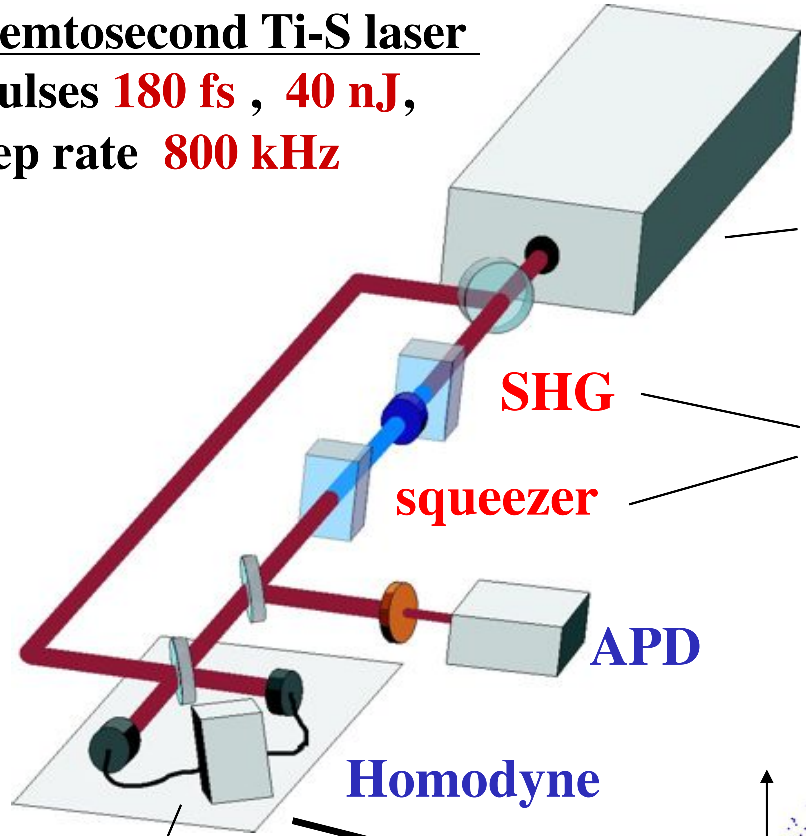
Time resolved (single pulse) analysis
- Measures $X(\theta_n)$ for each pulse
- Global quantum efficiency : $\eta = 80\%$
- Rejection > 82dB, SNR > 20dB

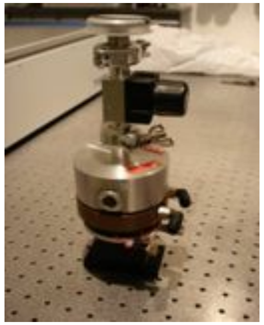


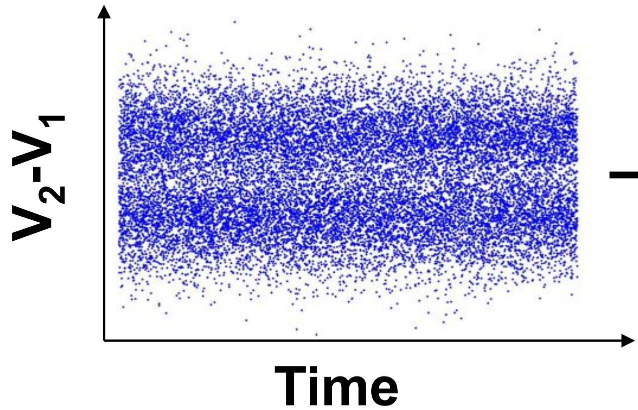
Spatial & spectral filtering

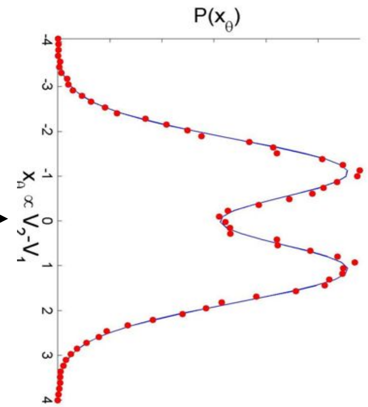
Experimental Set-up

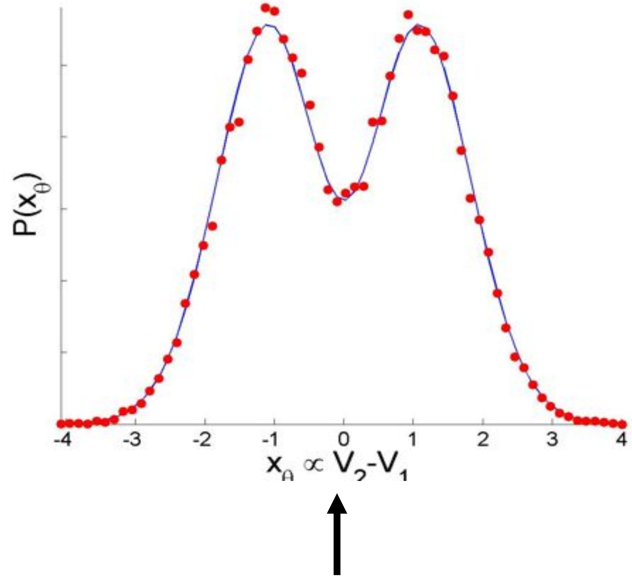
Femtosecond Ti-S laser
pulses 180 fs , 40 nJ,
rep rate 800 kHz







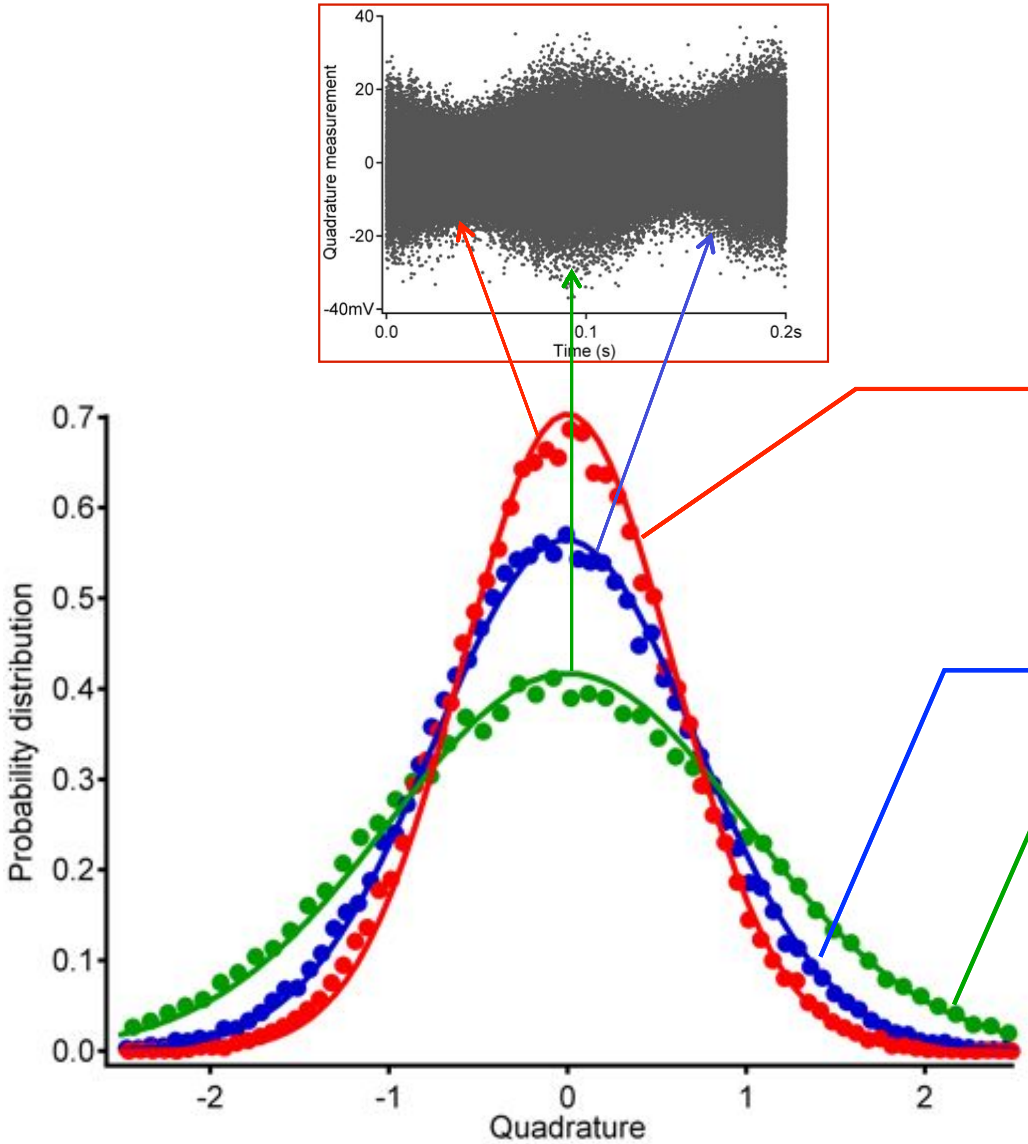




Pulsed Squeezed State Characterization

QIPC

Time-domain analysis
Scan of the LO phase
No conditioning
(all pulses are detected)



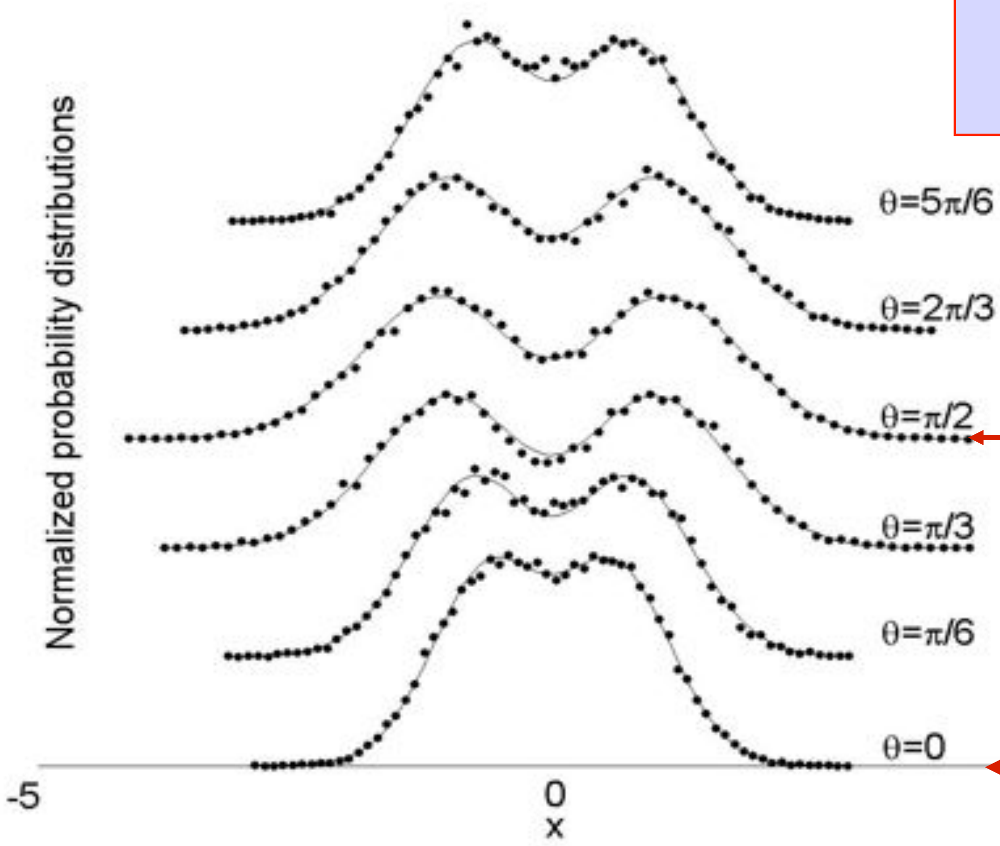
Squeezed quadrature
-1.9dB below SNL (no correction)
[-2.7dB corrected for losses]

Shot Noise Level (SNL)

Anti-squeezed quadrature
+ 3.3dB above SNL (no correction)
[+ 4.0dB corrected for losses]

Measured Probability Distributions after photon subtraction

Measured probability distributions of the quadratures components as function of the LO phase

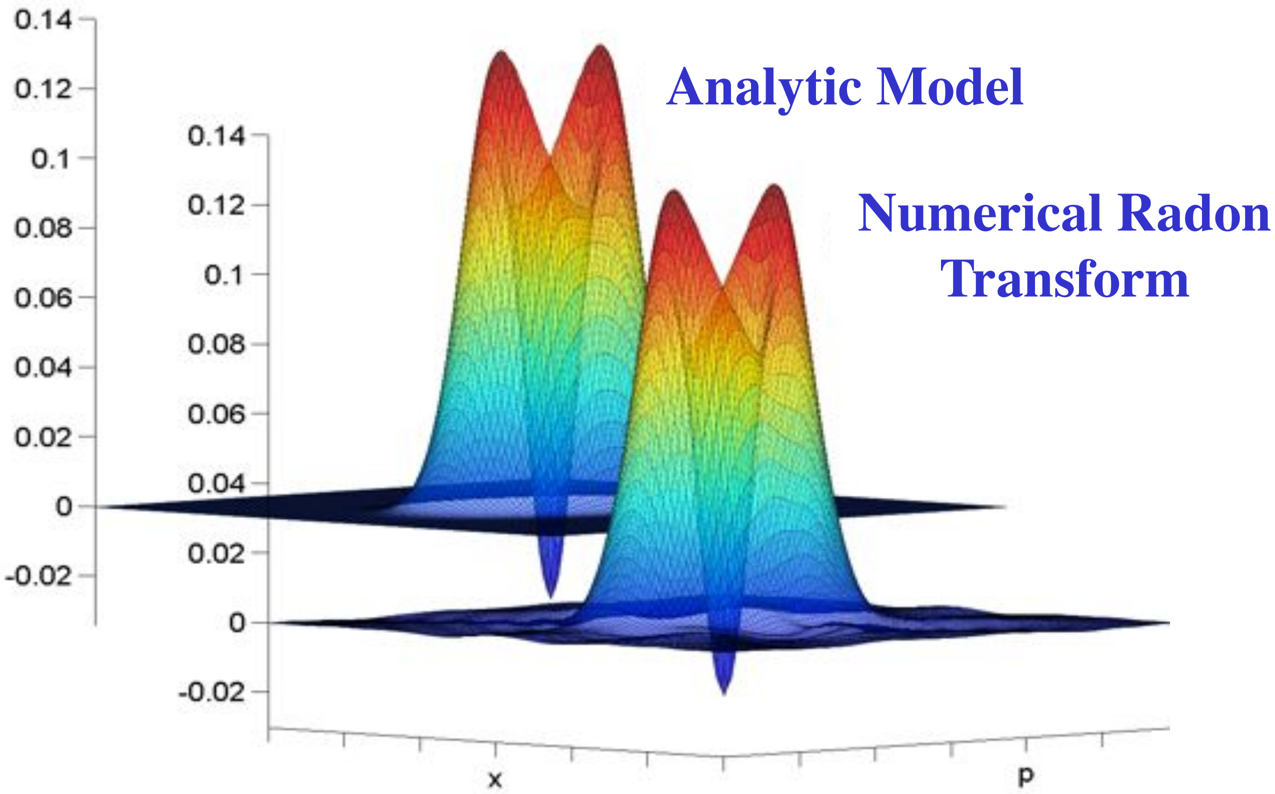


Anti-squeezed quadrature

Squeezed quadrature

Dip in the squeezed quadrature : hint for a negative Wigner function !

Wigner function of the « raw » measured state (no correction)



Radon transform clearly negative ! (no hypothesis, no correction)
… but no physical analysis => analytic model

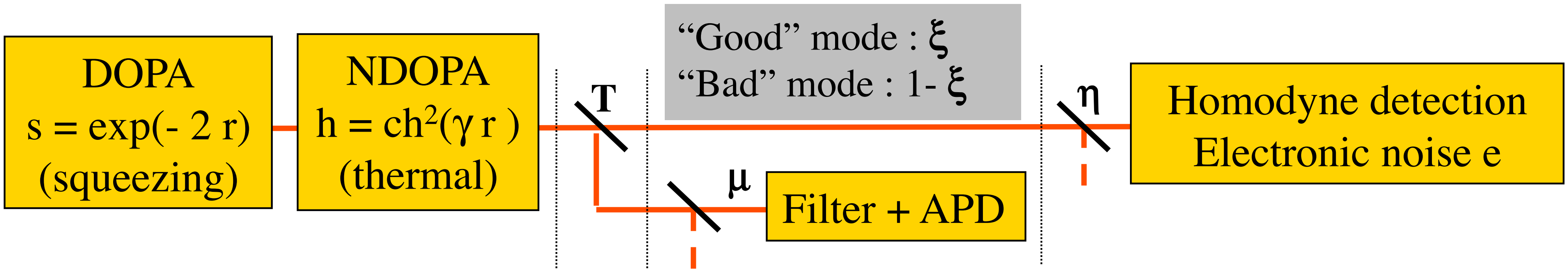
A simple physical model

Alexei Ourjoumtsev, 2005

Institut d'Optique

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

QIPC



Assuming that $\mu \ll 1$ the Wigner function has the simple generic form :

$$W(x,p) = \left[2a\frac{x^2}{c} + 2b\frac{p^2}{d} + 1 - a - b\right]\frac{e^{-\frac{x^2}{c}-\frac{p^2}{d}}}{\pi\sqrt{cd}}$$

The parameters a, b, c, d, are simple functions of s, γ, T, ξ, η , e

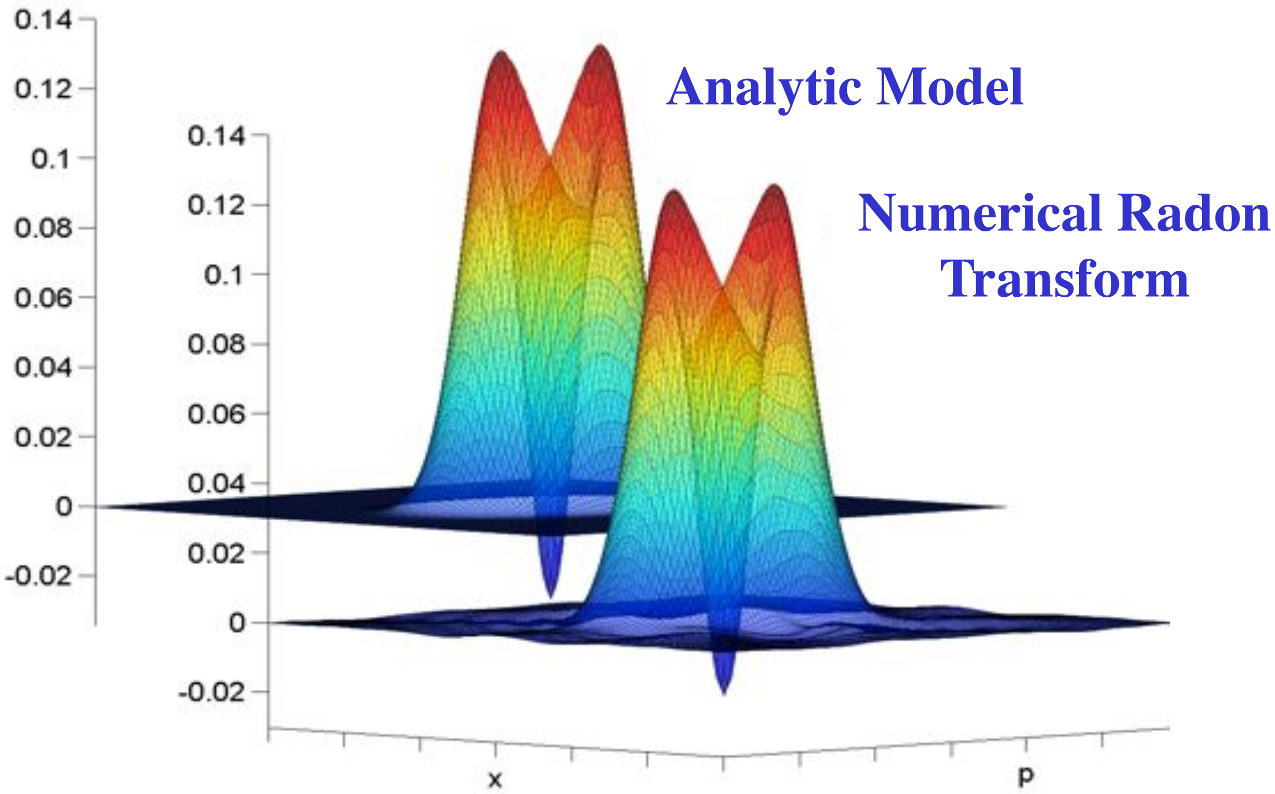
The corresponding quadrature probability distribution is :

$$P(x_\theta) = \left[2f\frac{x_\theta^2}{g} + 1 - f\right]\frac{e^{-\frac{x_\theta^2}{g}}}{\sqrt{\pi g}}$$

$$\begin{aligned} f &= cos^2(\theta)a + sin^2(\theta)b \\ g &= cos^2(\theta)c + sin^2(\theta)d \end{aligned}$$

All parameters can be obtained from the 2d and 4th order moments of P(xθ)

Wigner function of the « raw » measured state (no correction)



« Physical » analytic model fully consistent with Radon transform

-> one can reliably correct for the homodyne efficiency

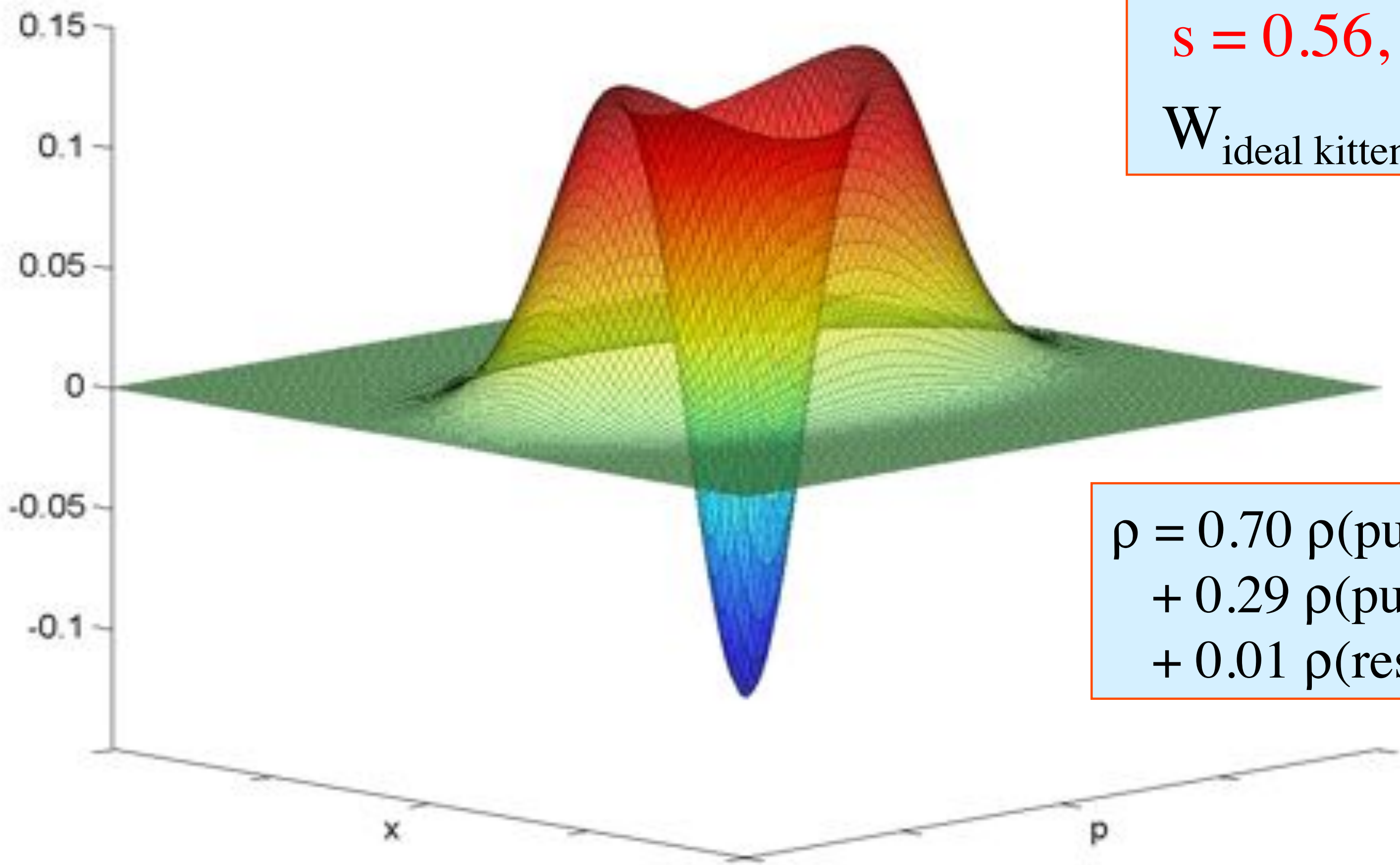
Correction for homodyne efficiency

QIPC

- We are interested in the *generated (propagating) state*
  => one should correct for the measurement efficiency
- Two possible methods to correct for homodyne losses :
  - numerical method (Maximum Likelihood)
  - using the previous analytical model :

1. From the moments of $P(x_\theta)$ determine $(s, \gamma, T, \xi, \eta, e)$
2. Check with measured experimental values : OK
3. **Calculate W $(s, \gamma, T, \xi, \eta, e)$, compare with Radon : OK**
4. Ideal detection : $\eta = 1$ and $e = 0$
5. **Calculate W $(s, T, \gamma, \xi, 1, 0)$, compare with MaxLike : OK !**

Wigner function of the Kitten (corrected for homodyne efficiency)



$W_0 = -0.13 \pm 0.01$

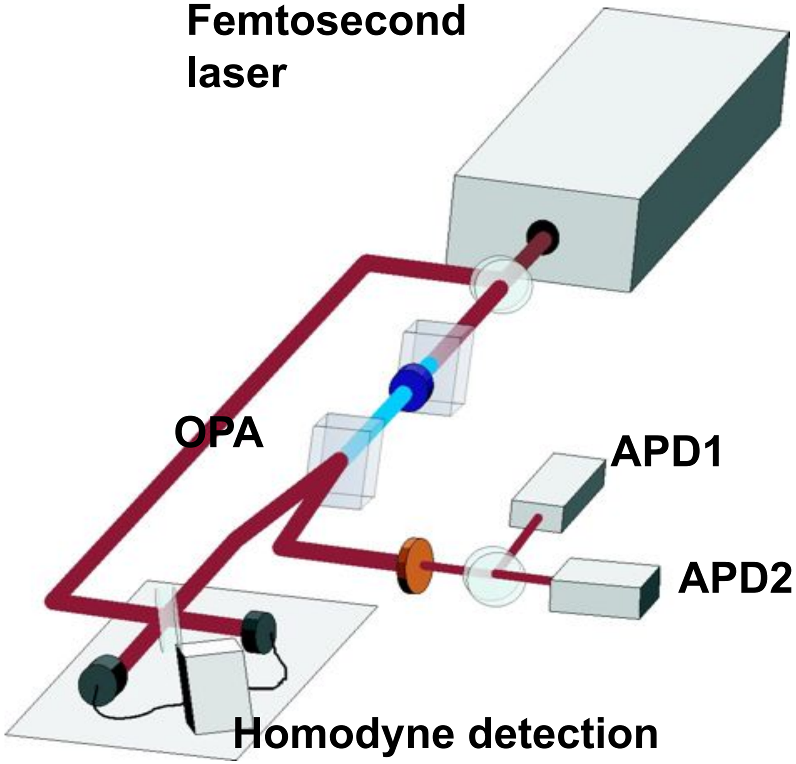
$s = 0.56, |\alpha| \approx 0.9$

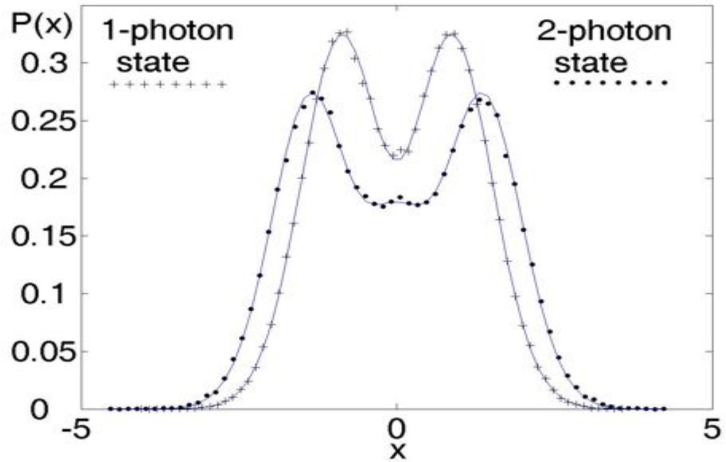
$W_{\text{ideal kitten}} = -0.32$

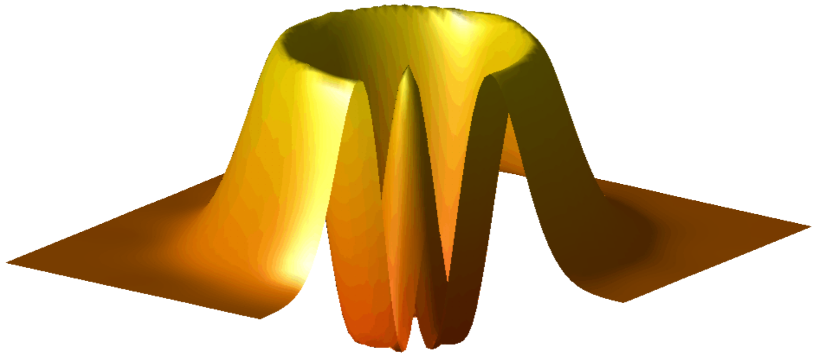
$\rho = 0.70\ \rho(\text{pure kitten})$
$+ 0.29\ \rho(\text{pure squeezed})$
$+ 0.01\ \rho(\text{residuals})$

A. Ourjoumtsev et al, Science 312: 83, 2006

Resource : Two-Photon Fock States







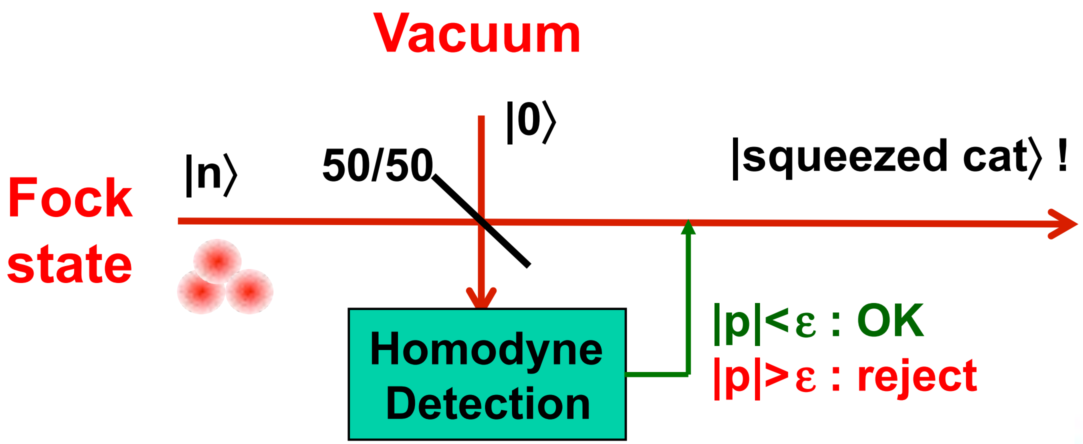
Experimental Wigner function
(corrected for homodyne losses)
Phys. Rev. Lett **96,** 213601 (2006)

What next ?

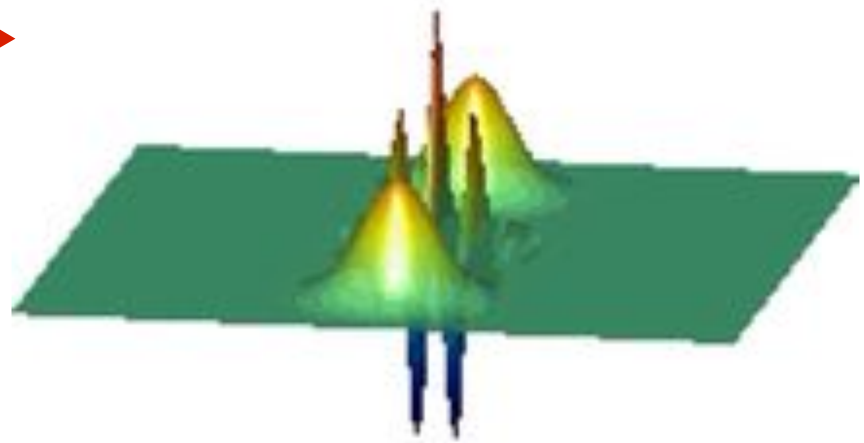
Generating BIG Schrödinger cats

How to create a Schrödinger's cat ?

Suggestion by Hyunseok Jeong, proofs by Alexei Ourjoumtsev :



Squeezed Cat state



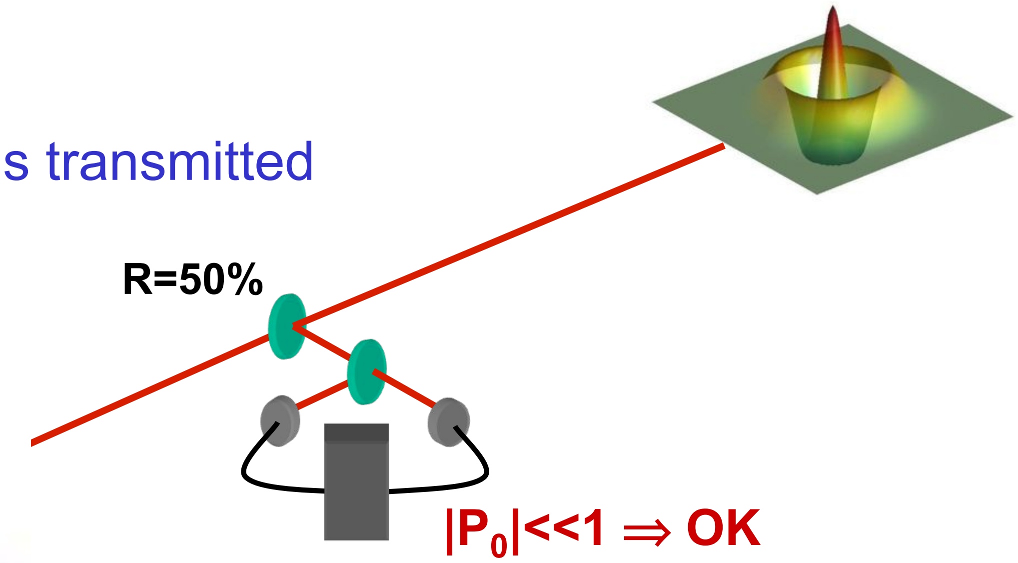
For n ≥ 3 the fidelity of the conditional state with a Squeezed Cat state is F ≥ 99%

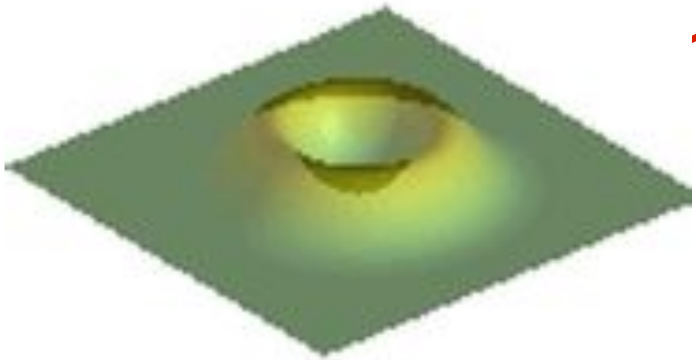
$$S(r)(|\alpha\rangle + e^{i\theta}|-\alpha\rangle)$$

Size :	$\alpha^2 = n$
Same Parity as n :	$\theta = n*\pi$
Squeezed by :	**3 dB**

The rebirth of the cat

- Make a n-photon Fock state
- 50/50 BS : ≈ n/2 photons transmitted





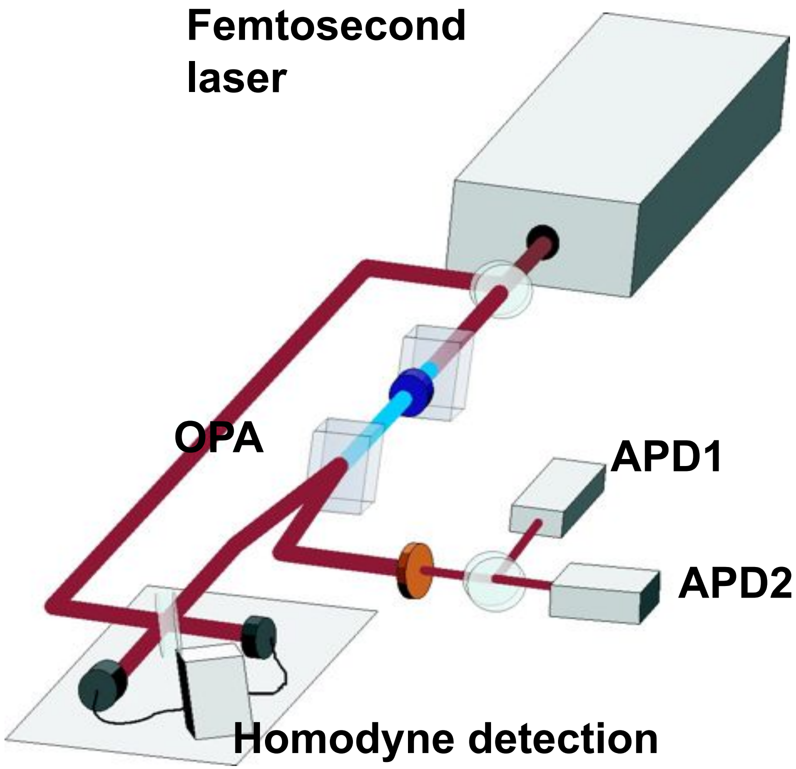
Homodyne measurement
- Phase dependence
- Parity measurement : $\langle P_0=0|2k+1\rangle = 0$

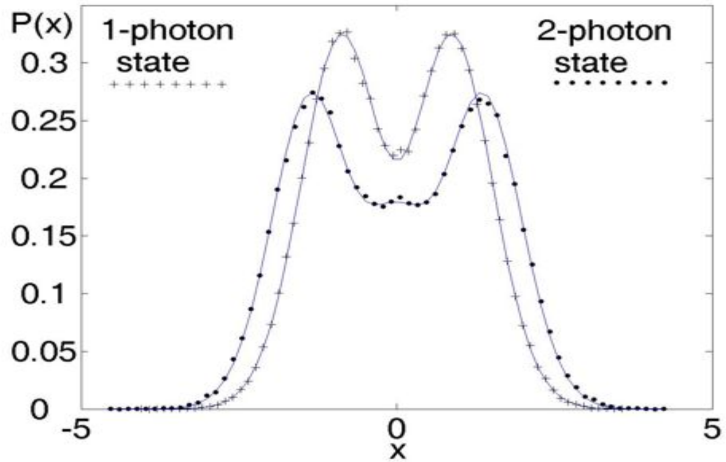
Reflected : even number of photons

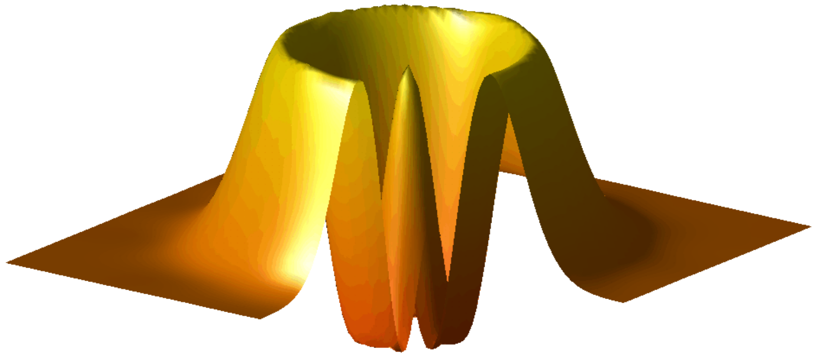
Transmitted : same parity as n

Squeezed cat state (from n=2) = $\sqrt{2/3}\ |2\rangle - \sqrt{1/3}\ |0\rangle$

Resource : Two-Photon Fock States

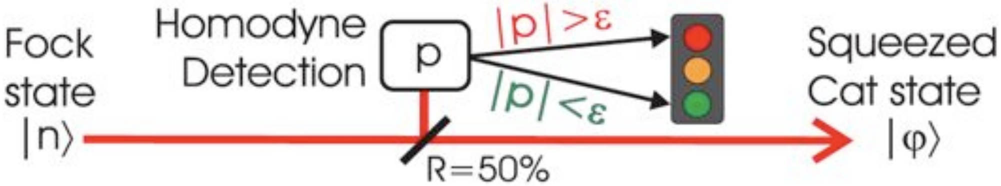


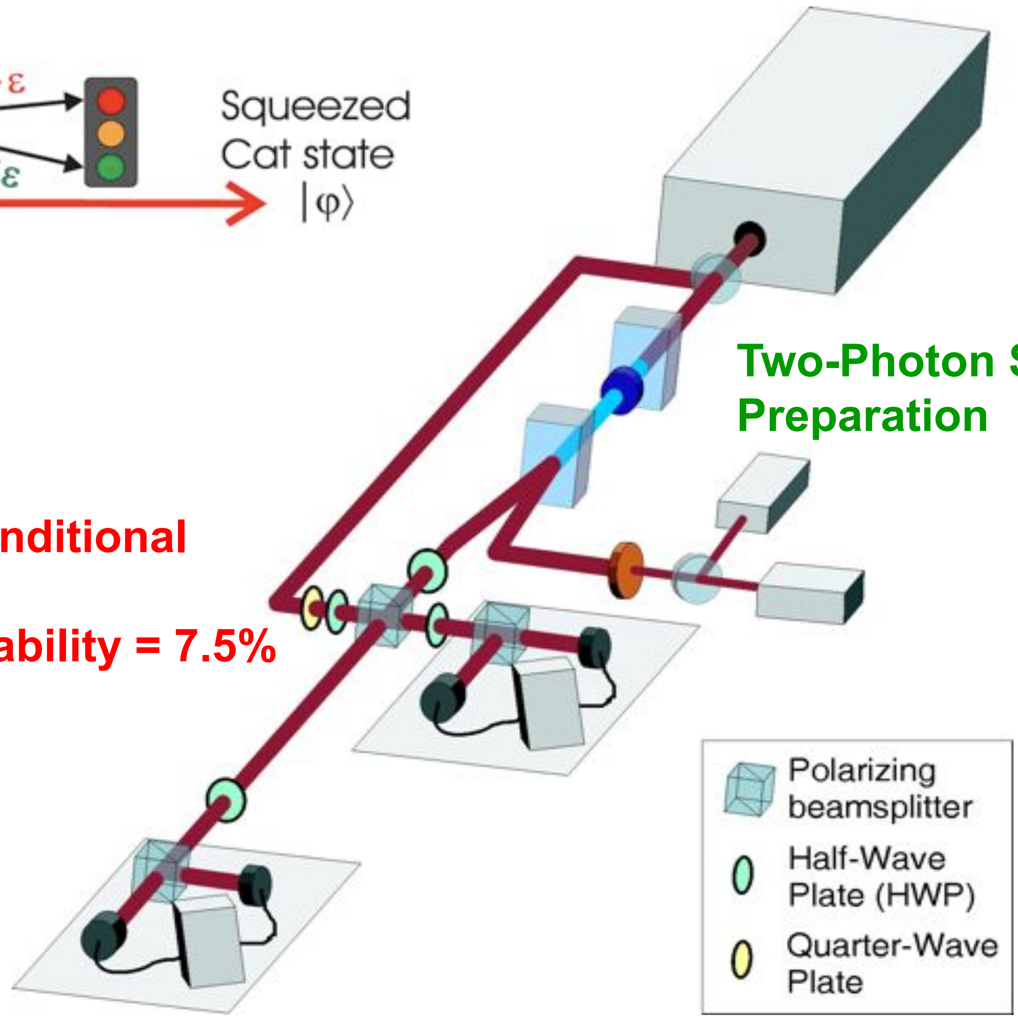




Experimental Wigner function
(corrected for homodyne losses)
Phys. Rev. Lett **96,** 213601 (2006)

Squeezed Cat State Generation





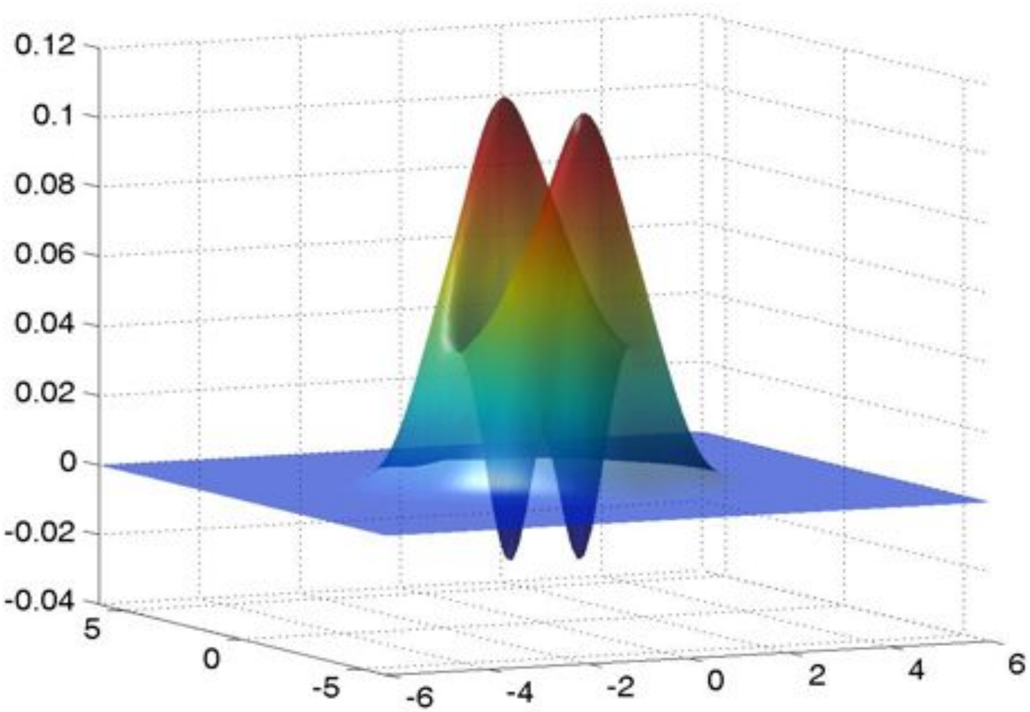
Two-Photon State Preparation

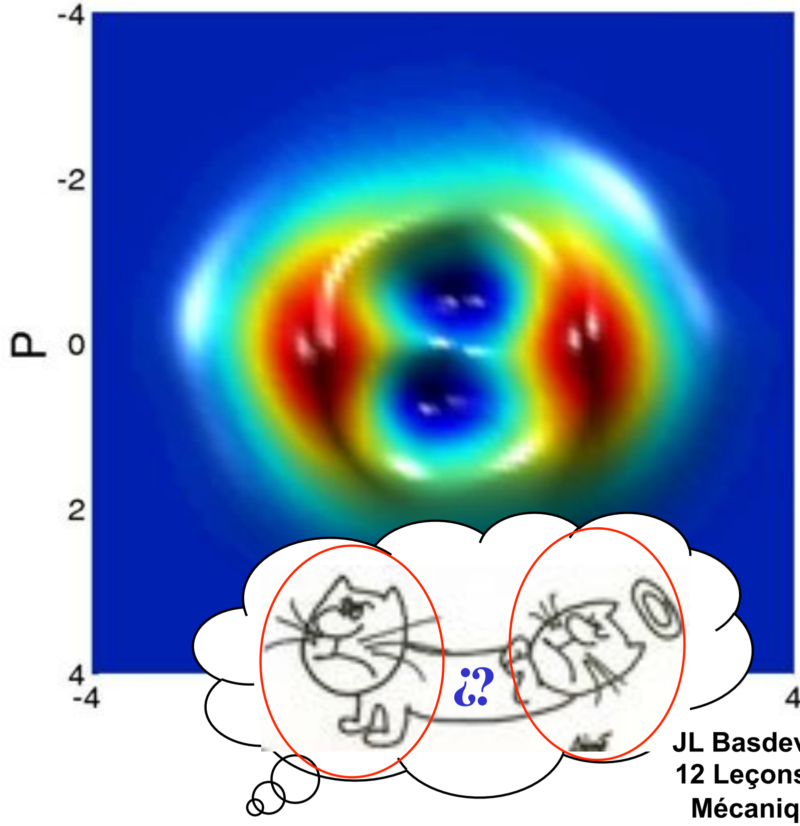
Homodyne Conditional Preparation :
Success Probability = 7.5%

Tomographic analysis of the produced state

Experimental Wigner function

A. Ourjoumtsev et al, Nature 448, 784, 16 august 2007





JL Basdevant
12 Leçons de
Mécanique
Quantique

Wigner function of the prepared state
Reconstructed with a Maximal-Likelihood algorithm
Corrected for the losses of the final homodyne detection.

Bigger cats : NIST (Gerrits, 3-photon subtraction), ENS (Haroche, microwave cavity QED), UCSB…

Towards quantum communications and quantum networks ?

- Towards quantum communications ?
- First, look at continuous variable entanglement !

Continuous-variables entangled beams: "EPR state" or "two-mode squeezed light"

$(X_A + X_B)$ and $(P_A - P_B)$ are squeezed (commuting operators !)

then $(P_A + P_B)$ and $(X_A - X_B)$ are anti squeezed

If Alice measures X_A , she will know X_B

If Alice measures P_A , she will know P_B

and for a large enough squeezing we have :

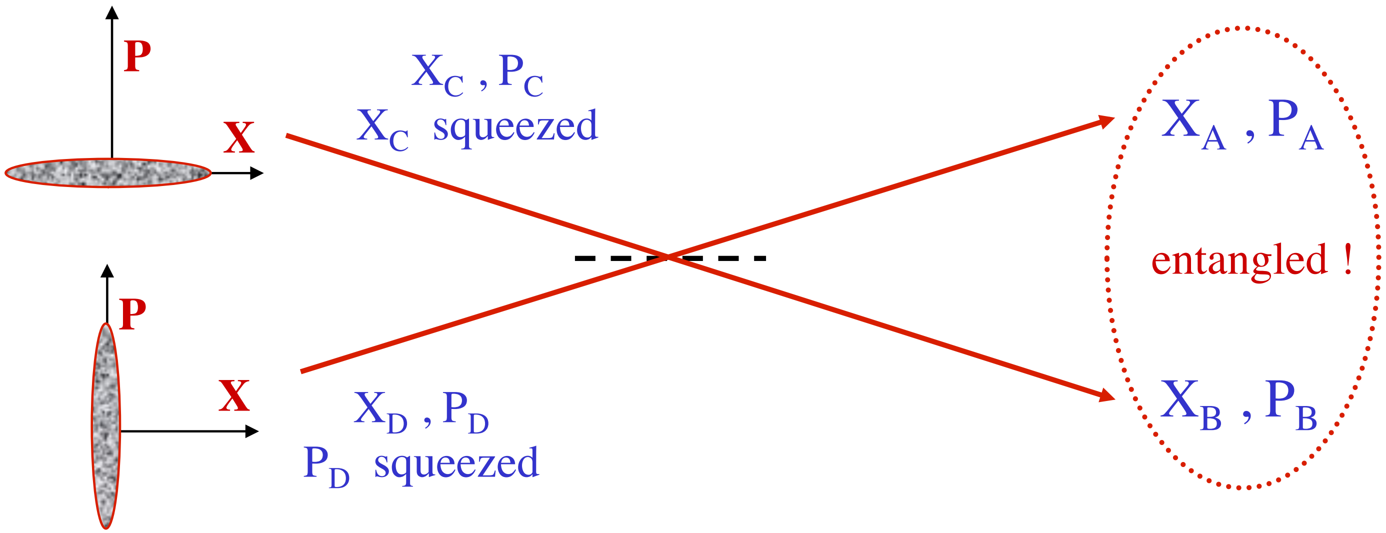
$$V(X_B|X_A)\ V(P_B|P_A) < N_0^2 \quad !!!$$

« apparent » violation of Heisenberg relations $V(X_B)\ V(P_B) \geq N_0^2$

If the squeezing goes to infinity : original EPR state (1935) !

How to produce CV entangled beams ?

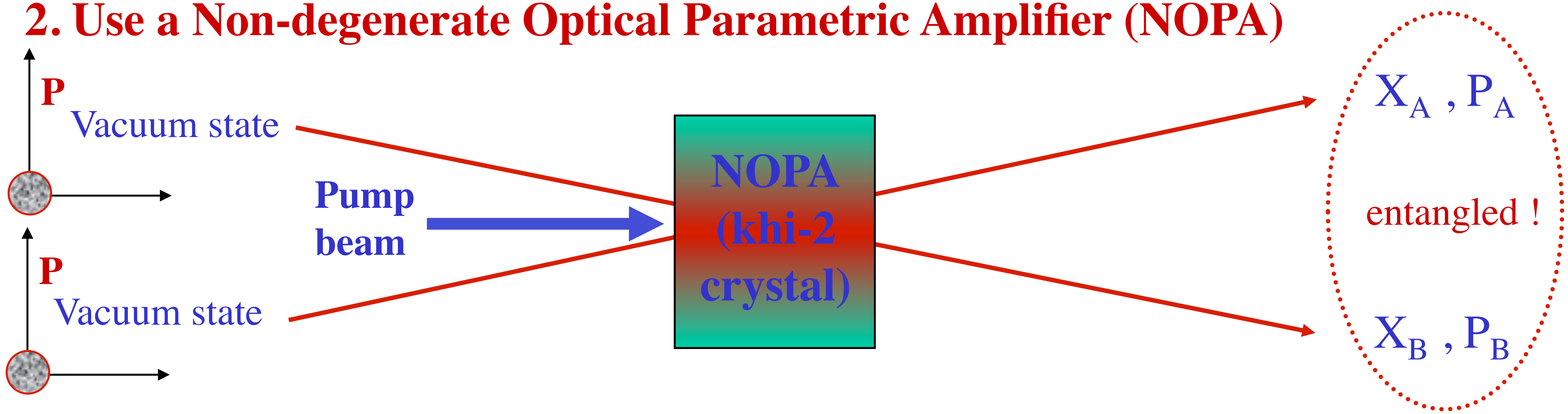
1. Combine two orthogonally squeezed beams



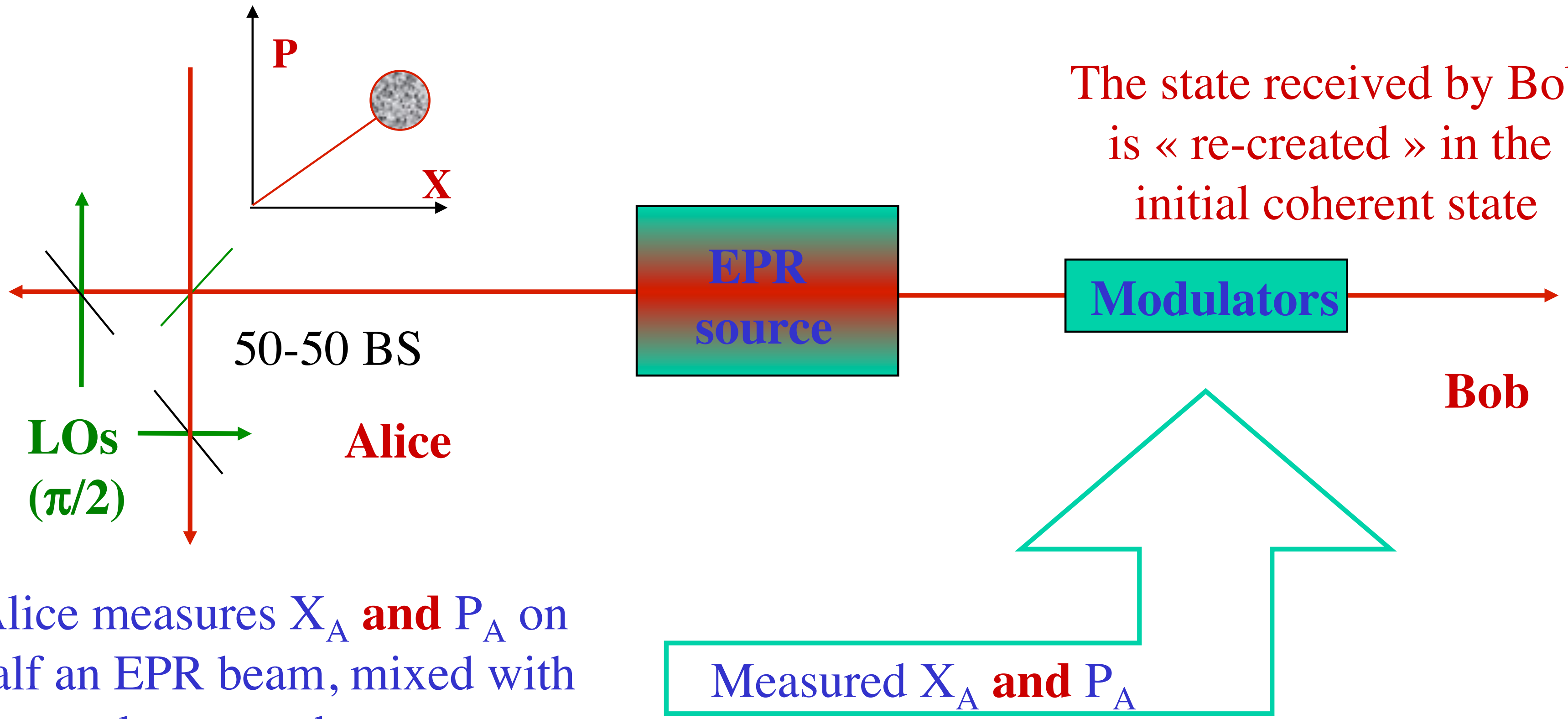
$$X_C = (X_A + X_B)/\sqrt{2}$$
$$P_C = (P_A + P_B)/\sqrt{2}$$
$$X_D = (X_A - X_B)/\sqrt{2}$$
$$P_D = (P_A - P_B)/\sqrt{2}$$

OK !

2. Use a Non-degenerate Optical Parametric Amplifier (NOPA)



Quantum teleportation of coherent states



The state received by Bob is « re-created » in the initial coherent state

Alice measures X_A **and** P_A on half an EPR beam, mixed with an unknown coherent state

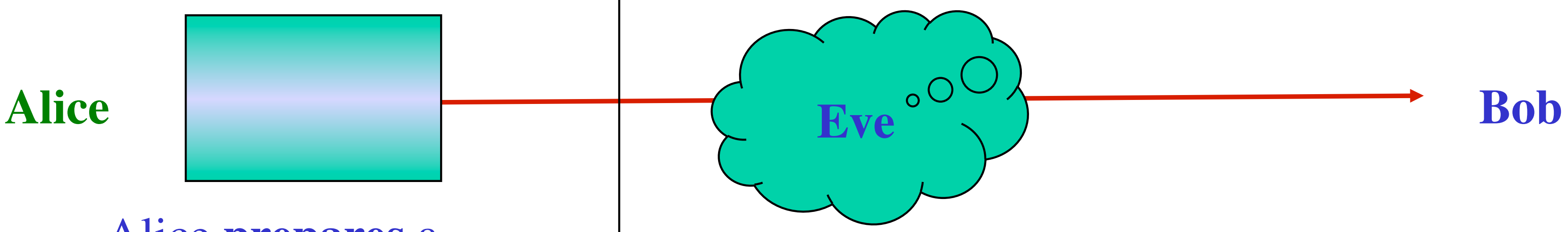
Experiments :

A. Furusawa et al, Science **282**, 706 (1998)

W. Bowen et al, Phys. Rev. A **67**, 032302 (2003)

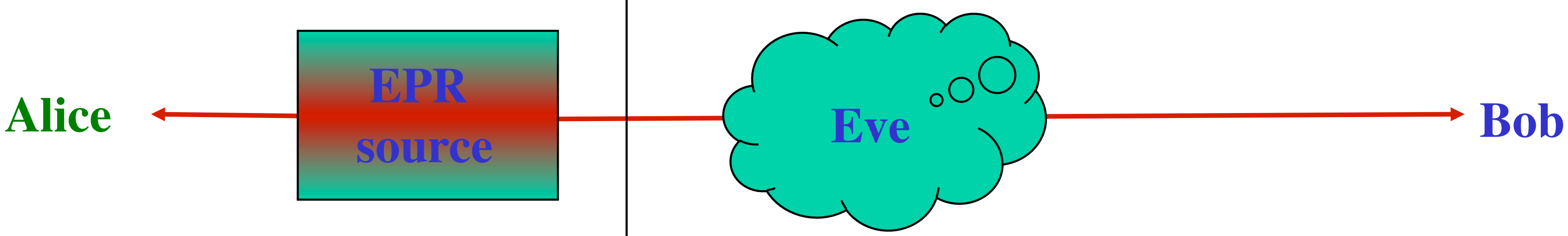
T.C. Zhang et al, Phys. Rev. A **67**, 033802 (2003)

A very useful equivalence : "virtual entanglement"



Alice **prepares** a random quantum state and sends it to Bob

Eve and Bob receive the states prepared by Alice



Alice **measures** half an EPR state, the other half goes to Bob

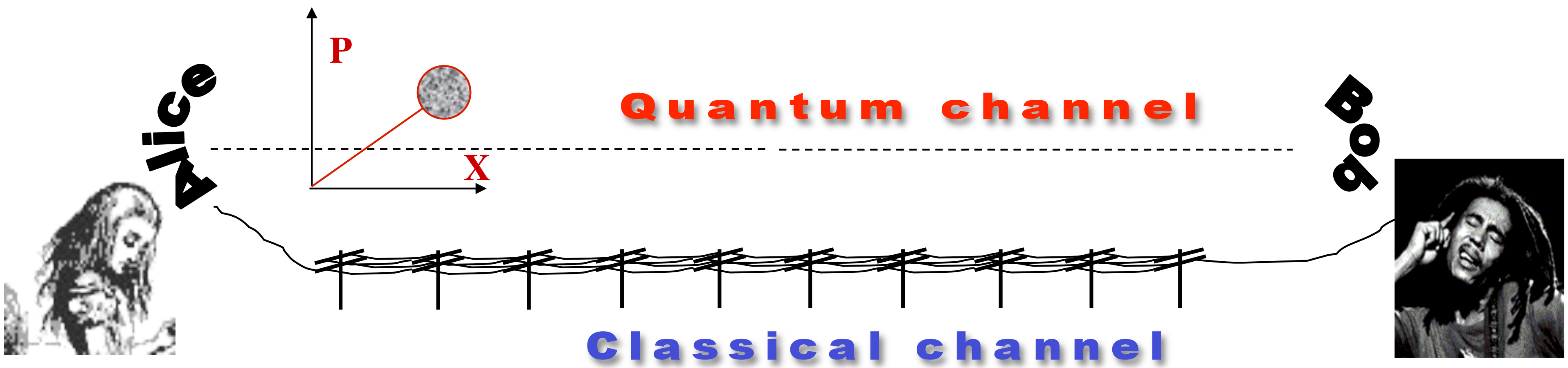
The density matrix received Eve and Bob is the same in both cases : Eve cannot know more !

"Prepare and measure" protocol is equivalent to an entangled state protocol !

This equivalence is extensively used in security proofs

CVQKD :
from the idea to
unconditionnal security proofs

Coherent States Quantum Key Distribution



* Essential feature : quantum channel with non-commuting quantum observables

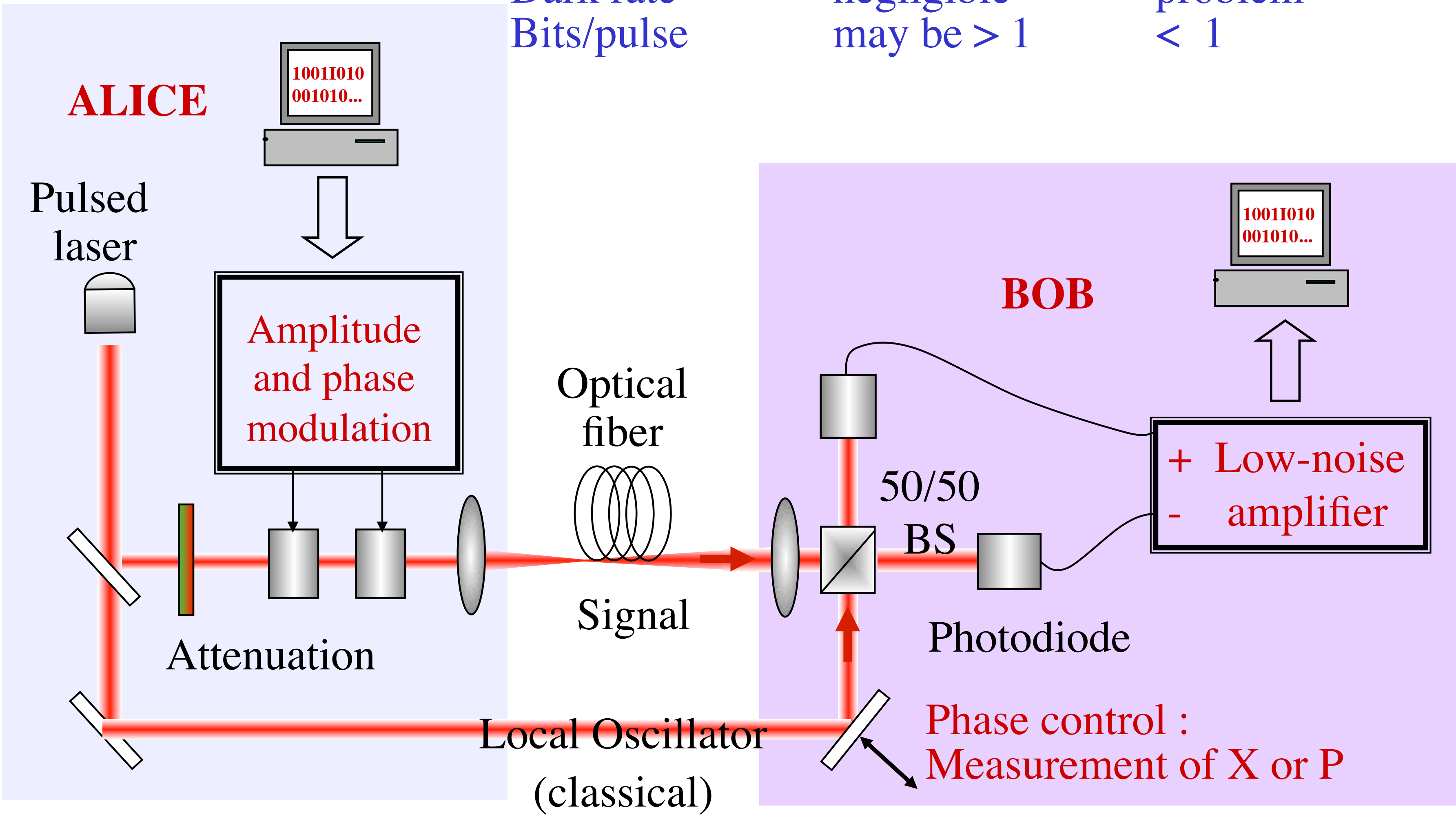
-> not restricted to single photon polarization or phase !

-> Design of Continuous-Variable QKD protocols where :

* The non-commuting observables are the quadrature operators X and P
* The transmitted light contains weak coherent pulses (about 10 photons) with a gaussian modulation of amplitude and phase
* The detection is made using shot-noise limited homodyne detection

Coherent States Quantum Key Distribution

	Homodyne	Counting (APD)
Efficiency	> 90%	10-50 %
Dark rate	negligible	problem
Bits/pulse	may be > 1	< 1



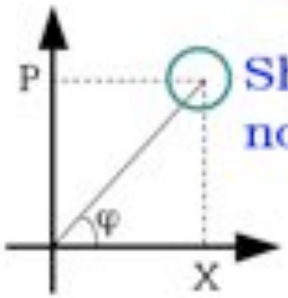
Coherent state continuous variables QKD protocol

- Key information encoded in both quadratures of a coherent state

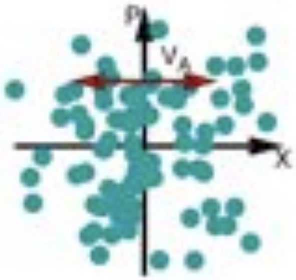
Eve

Alice  Quantum channel (T, ε) + Classical Channel (auth.)  Bob

Gaussian modulation



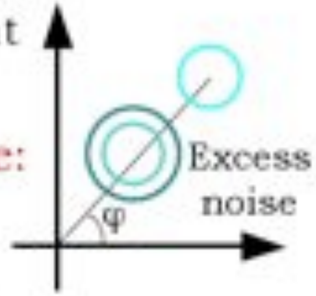
Shot noise



Random measurement of the quadrature of each coherent state (with efficiency η)

Total channel-added noise:

$$\chi = \underbrace{1/T - 1}_{\text{equivalent to photon loss}} + \underbrace{\varepsilon}_{\text{equivalent to errors}}$$



- Bob reveals measurement choice
- Alice and Bob share a set of Gaussian correlated data
- Further communication to calculate channel parameters and derive secret key based on Bob's data → **reverse reconciliation**

F. Grosshans et al, Phys. Rev. Lett. 88, 057902 (2002) & Nature 421, 238 (2003)

QKD protocol using coherent states with gaussian amplitude and phase modulation

Efficient transmission of information using continuous variables ?

-> Shannon's formula (1948) : the mutual information I_{AB} (unit : bit / symbol) for a gaussian channel with additive noise is given by

$$I_{AB} = 1/2 \ \log_2 [\ 1 + V(signal) / V(noise)\ ]$$

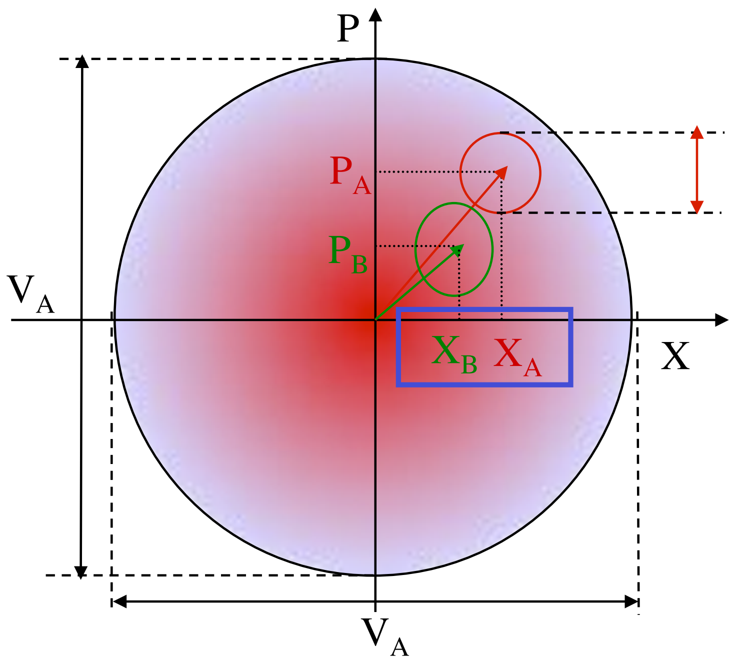
Reminder : I(X; Y) = H(X) - H(X | Y) = H(Y) - H(Y| X) = H(X) + H(Y) - H(X; Y)

(a) Alice chooses X_A and P_A within two random gaussian distributions.

(b) Alice sends to Bob the coherent state | $X_A + i P_A$ >

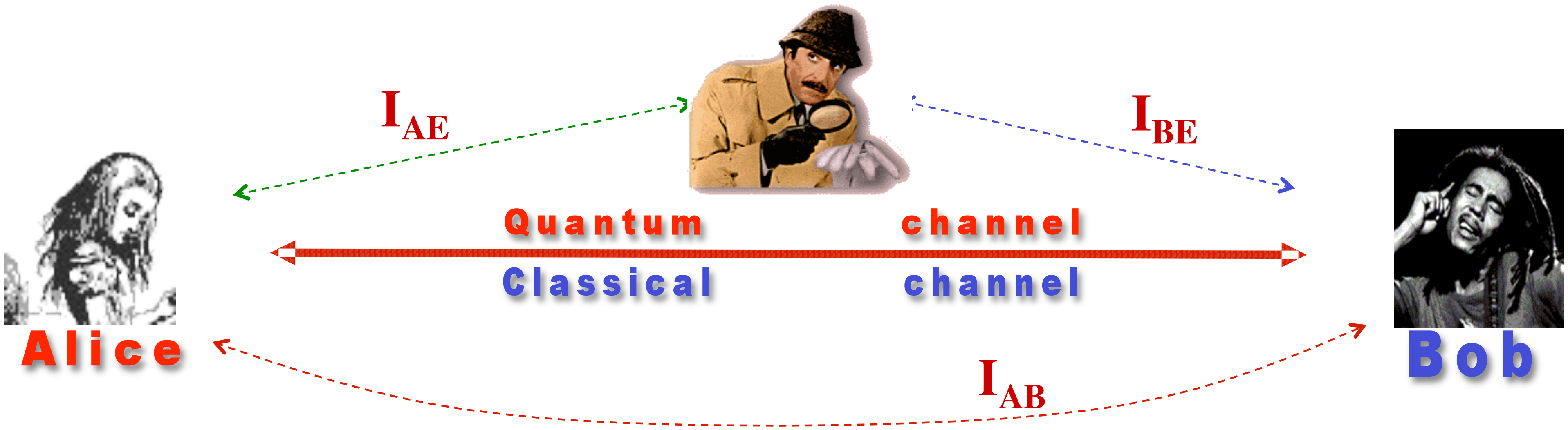
(c) Bob measures either X_B or P_B

(d) Bob and Alice agree on the basis choice (X or P), and keep the relevant values.



Data Reconciliation

how to correct errors, revealing as less as possible to Eve ?

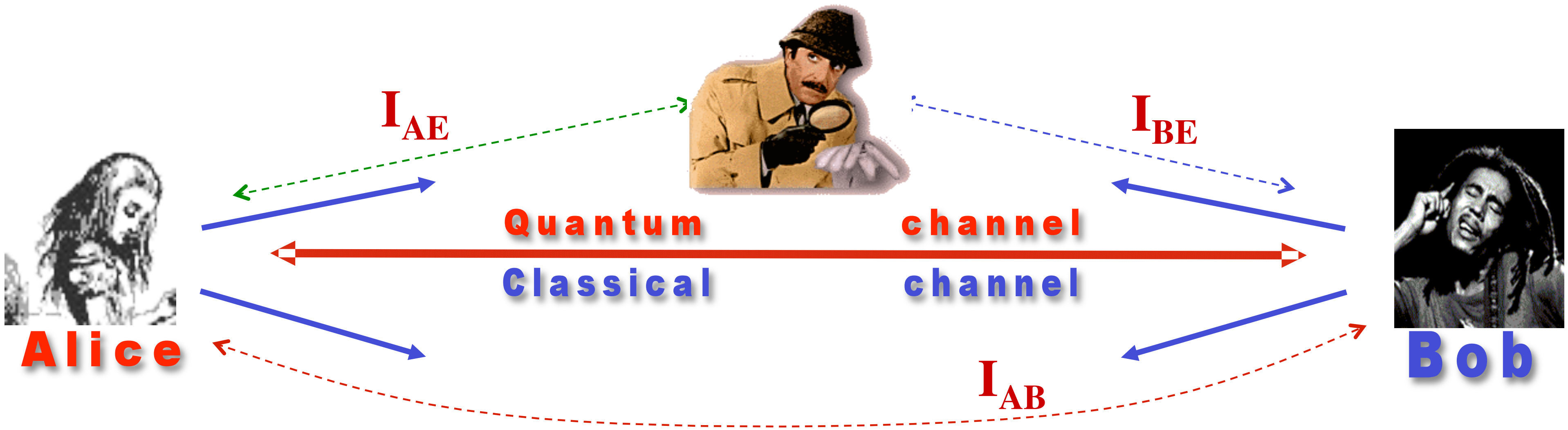


Main idea (Csiszar and Körner 1978, Maurer 1993) :

Alice and Bob can in principle distill, from their correlated key elements, a common secret key of size $S > \sup(I_{AB} - I_{AE}, I_{AB} - I_{BE})$ bits per key element.

Crucial remark : it is enough that I_{AB} is larger than the **smallest** of I_{AE} and I_{BE} (i.e. one has to take the best possible case).

Data Reconciliation

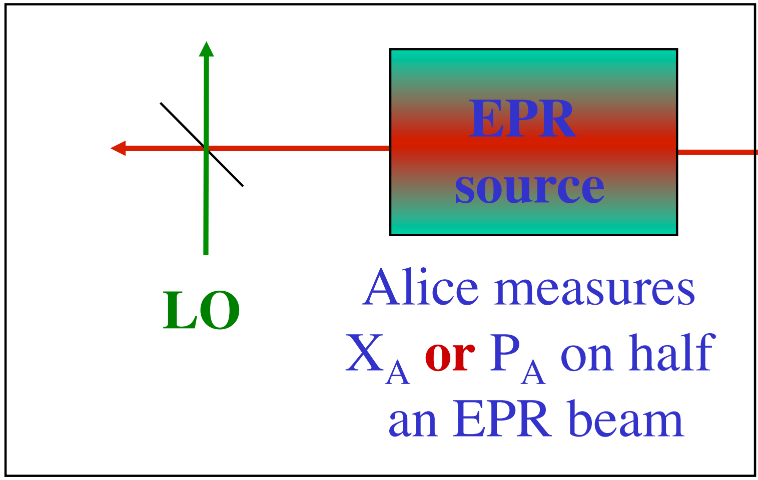


If I_{AE} is the smallest, the reconciliation must keep $S = I_{AB} - I_{AE}$ constant :
Alice gives correction data to Bob (and also to Eve),
and Bob corrects his data :
« direct reconciliation protocol »

If I_{BE} is the smallest, the reconciliation must keep $S = I_{AB} - I_{BE}$ constant :
Bob gives correction data to Alice (and also to Eve),
and Alice corrects his data :
« reverse reconciliation protocol »

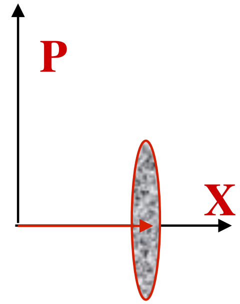
Crucial question for Alice and Bob :
how to bound I_{AE} and I_{BE}, knowing I_{AB} ?

EPR versus coherent protocol

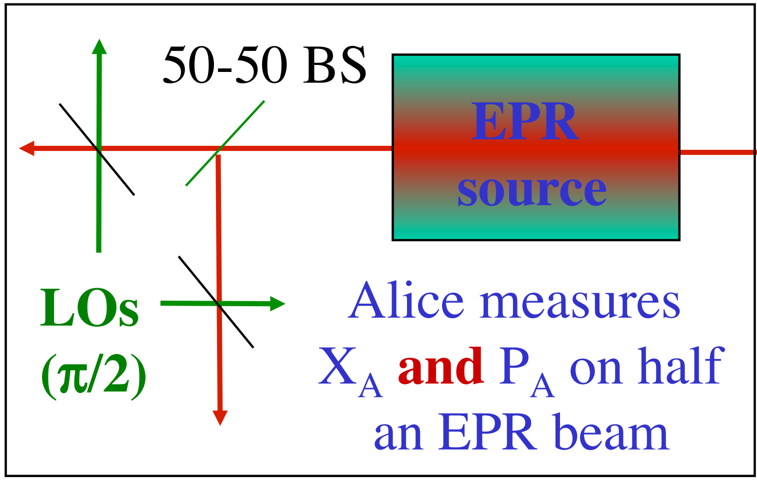


$(X_A + X_B)$ and $(P_A - P_B)$
are squeezed

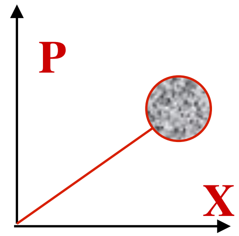
Bob



The state received by Bob is prepared in a squeezed state, conditional to Alice 's result



Bob



The state received by Bob is prepared in a coherent state, conditional to Alice 's result

EPR protocol equivalent to coherent state protocol !

Cf BB84 vs entangled pair (Ekert) protocol

Entropic Heisenberg Inequalities

F. Grosshans and N.J. Cerf, PRL **92**, 047905 (2004)

* Mutual Informations can be calculated from conditional entropies

* Conditional entropies are bounded by « entropic » uncertainty relations for X and P:

$$\mathbf{H(X_B|E) + H(P_B|P_A) \geq 2\, H_0}$$

* The security of the protocol follows from a calculation similar to the one used for discrete variables (qubits)

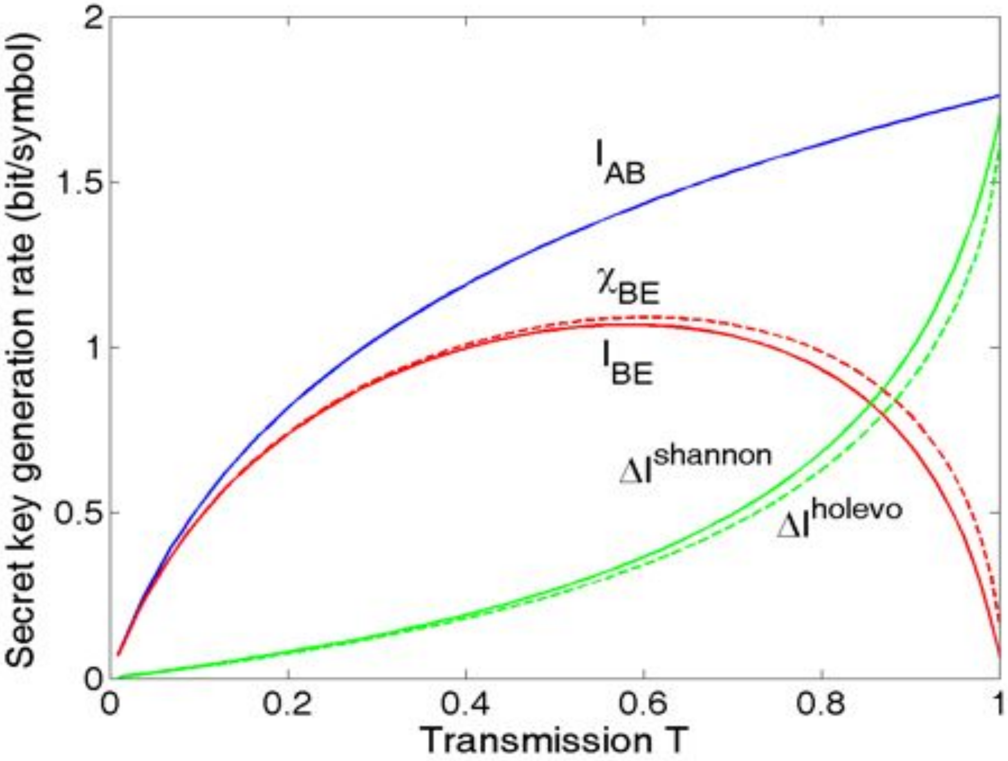
* Important parameters :

- transmission of the channel $\mathbf{T_{line}}$
- "added noise in the channel" $\mathbf{N_{eq} = N_{losses} + N_{exc}}$

where $N_{losses} = (1 - T_{line}) / T_{line}\, N_0$ (N_0 is the shot noise)

N_{exc} is the "excess noise" (e.g. laser amplifier…)

Security of coherent state CV-QKD protocol



Alice-Bob mutual information : I_{AB}

Eve-Bob mutual information :

I_{BE} (Shannon : individual attacks)

χ_{BE} (Holevo : collective attacks)

Secret Key Rate :

$\Delta I = I_{AB} - I_{BE}$ (Shannon)

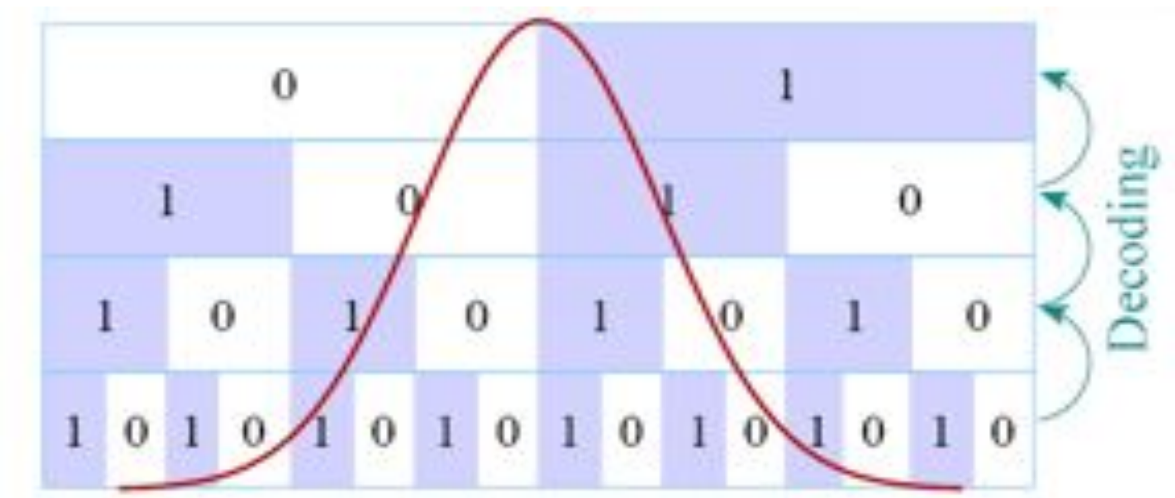
$\Delta I = I_{AB} - \chi_{BE}$ (Holevo)

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

Fig : $V_A = 21$ (shot noise units)
$\varepsilon = 0.005$ (shot noise units), $\eta = 0.5$

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

Reconciliation of correlated Gaussian variables

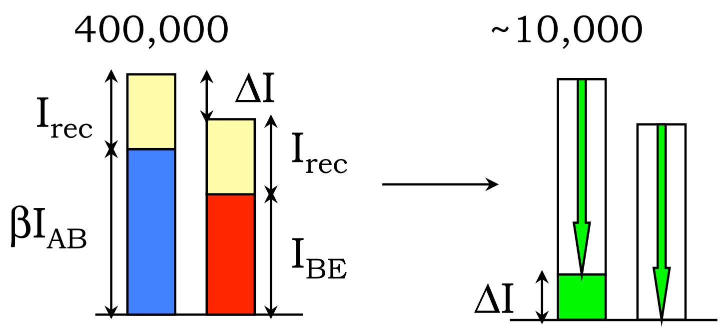


- Each level has a different error rate
- Non-independent levels

→ Error correction performed using multi-level iterative soft decoding with LDPC codes

G. Van Assche et al, IEEE Trans. on Inf. Theory 50, 394 (2004)
M. Bloch et al, arXiv:cs.IT/0509041 (2005)

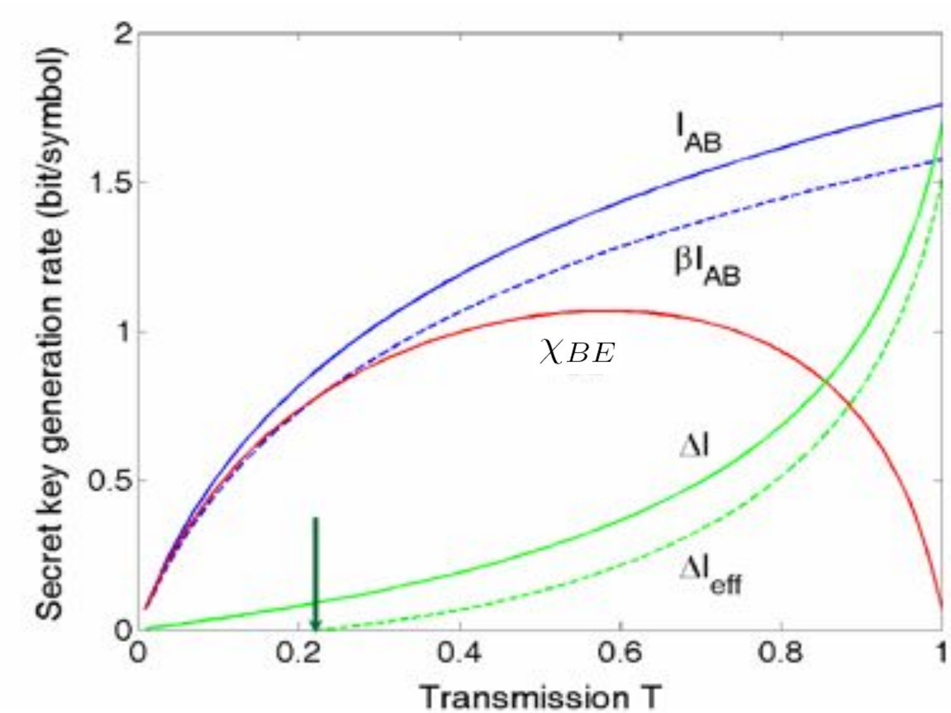
- Standard privacy amplification based on universal hash functions
- Small processing time

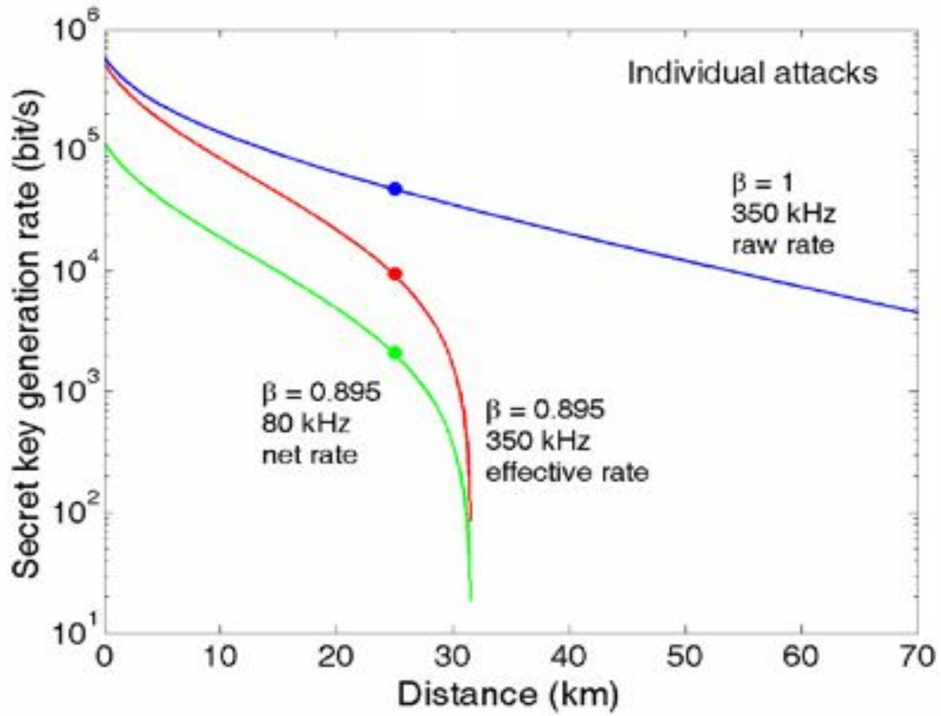


Error correcting codes efficiency

Error correction with LDPC codes, efficiency β

$$\Delta I^{eff} = \beta I_{AB} - \chi_{BE}$$





Imperfect correction efficiency induces a limit to the secure distance

Post-processing at SeQureNet

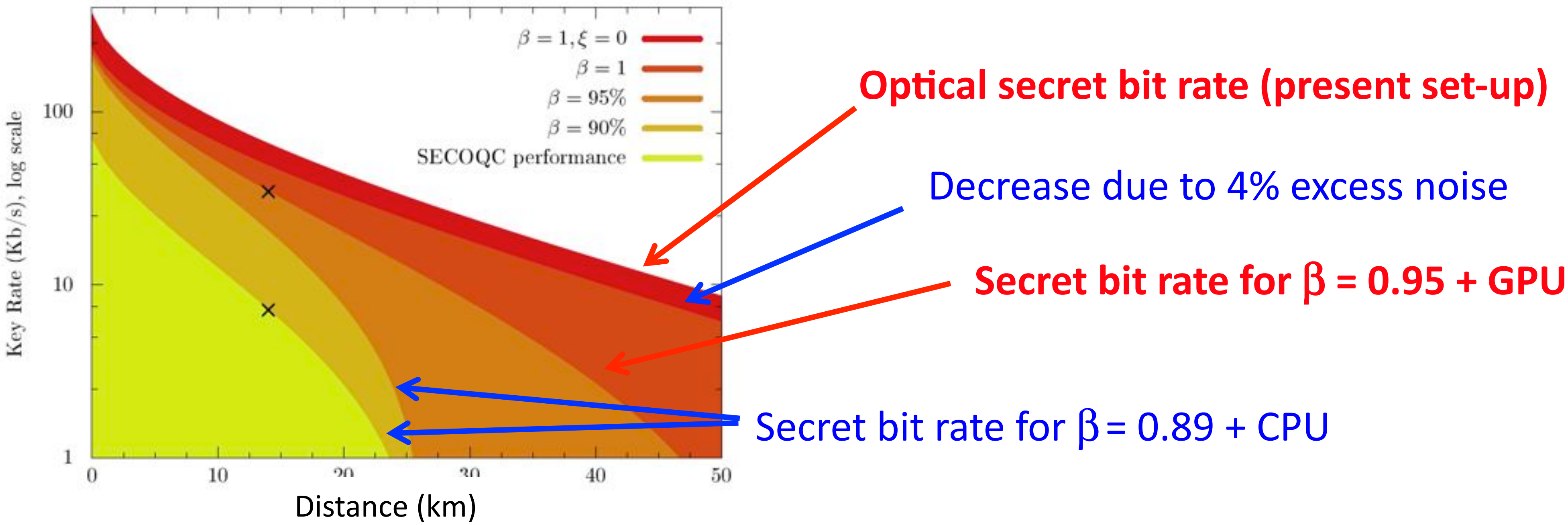
SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

Paul Jouguet, Sébastien Kunz-Jacques, Romain Alléaume

Optimize LDPC codes, use Graphic Processing Units (GPU) rather than CPU

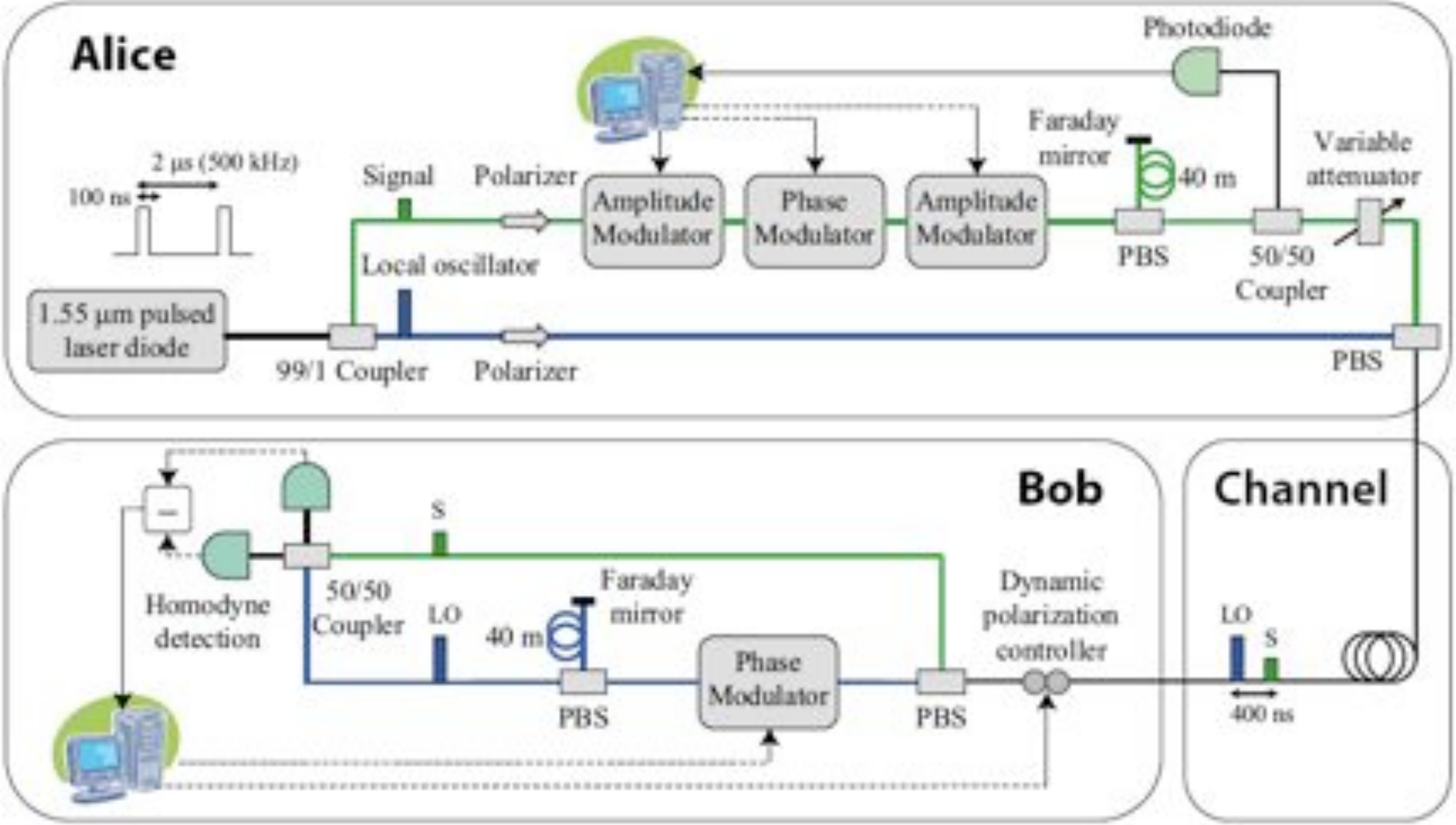
=> Calculation speed is no more limiting the secret bit rate !

=> β is improved from 89% to 95% for any SNR : longer distance (100 km) !



CVQKD :
practical implementation
and field demonstrations

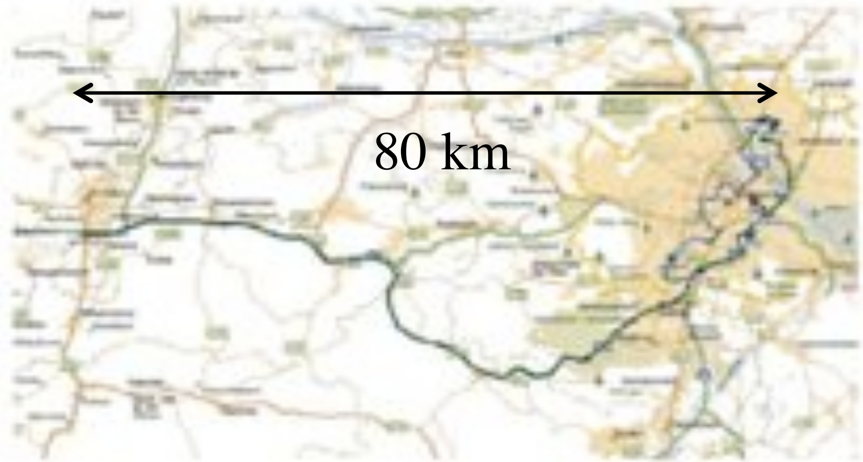
All-fibered CVQKD @ 1550 nm

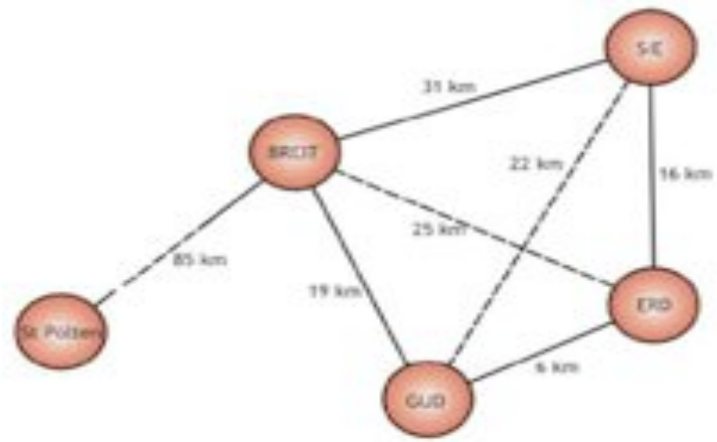


Field test of a continuous-variable quantum key distribution prototype
S Fossier, E Diamanti, T Debuisschert, A Villing, R Tualle-Brouri and P Grangier
New J. Phys. 11 No 4, 04502 (April 2009)

Quantum Back-Bone demonstrator SECOQC, Vienna, 8 october 2008

Real-size demonstration of a **secure quantum cryptography network** by the European Integrated Project SECOQC, Vienna, 8 october 2008





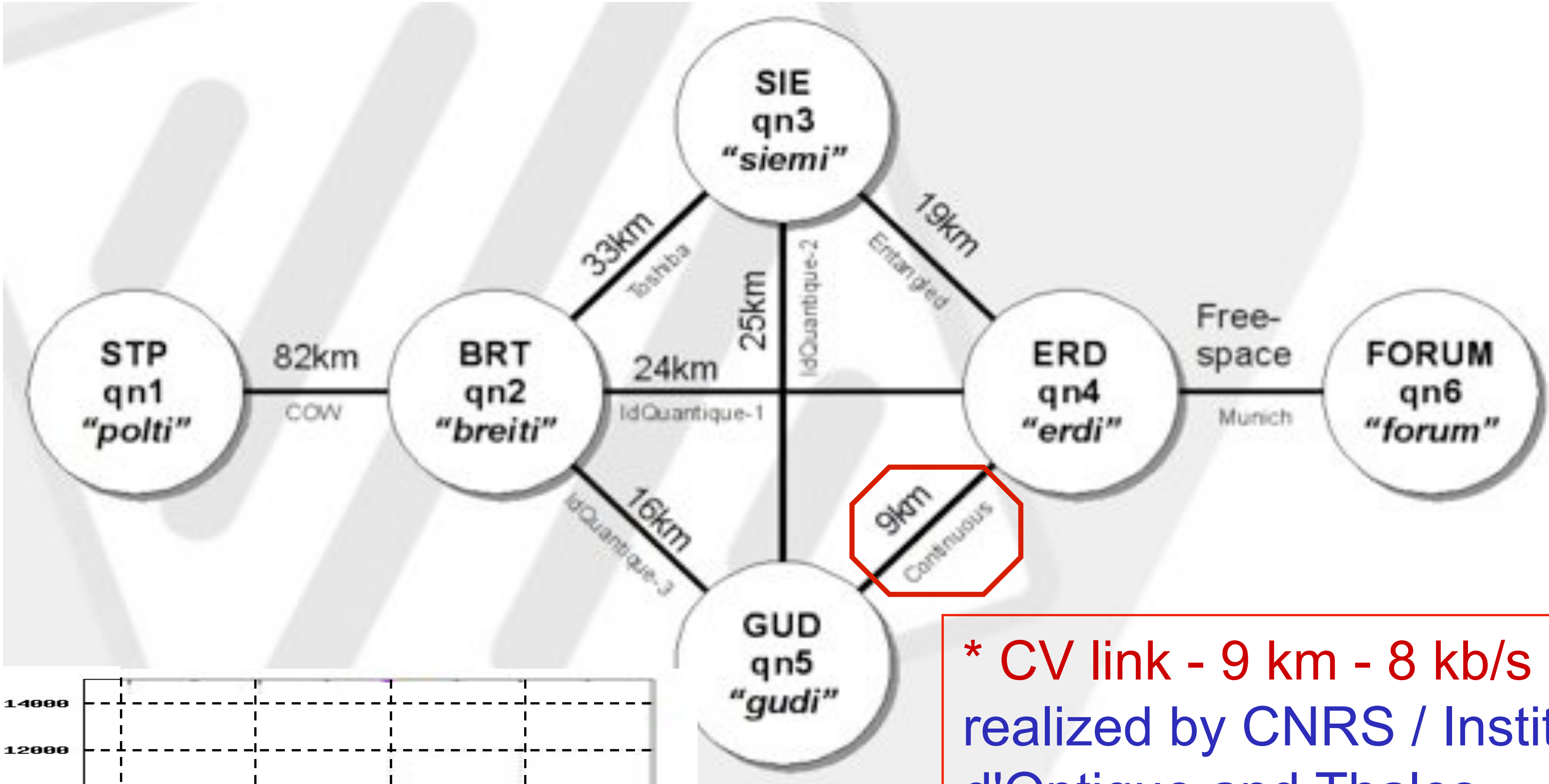
Node server

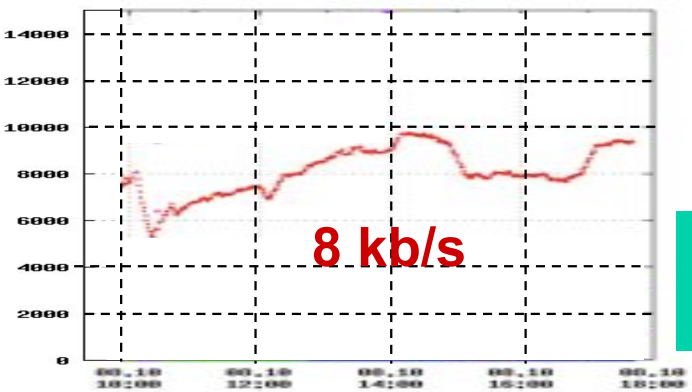
Continuous Variables

Id Quantique

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 link - 9 km - 8 kb/s realized by CNRS / Institut d'Optique and Thales

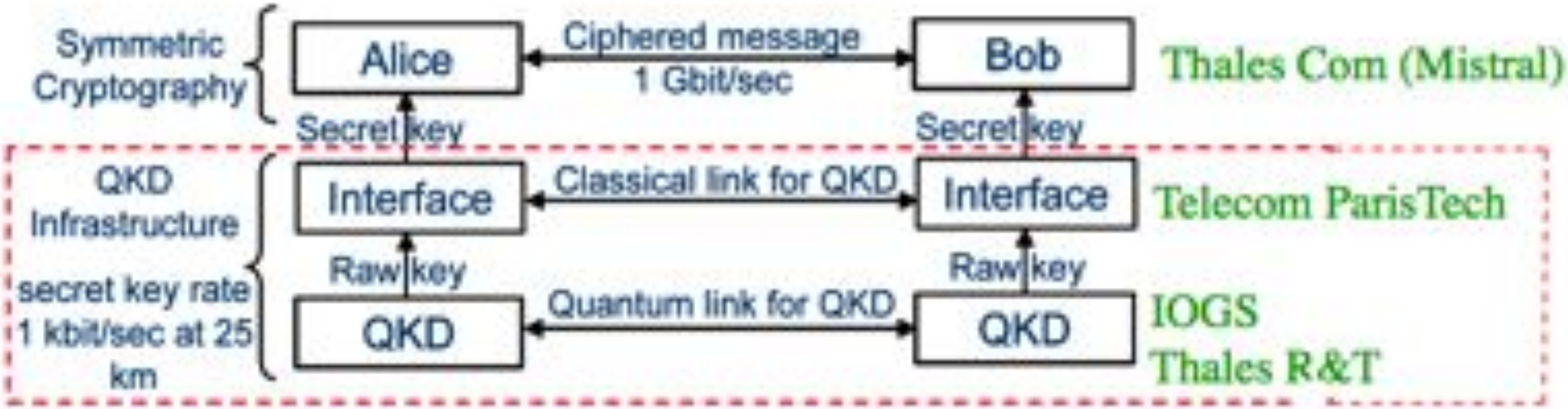
CV secret bit rate during the demo (8h)

SEQURE

10110101110110010100010 11

Secure Encryption with QUantum key REnewal

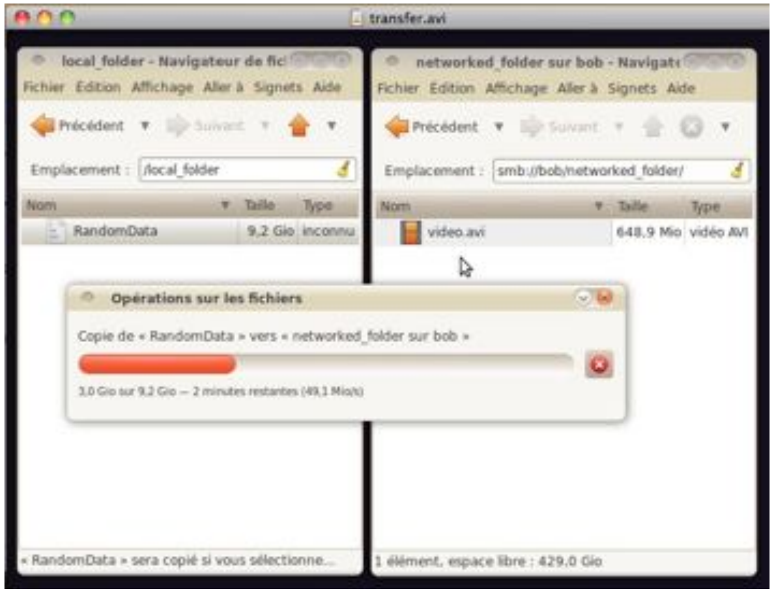
- Combining QKD (1 kbit/sec) with fast symmetric encryption (1 Gbit/sec)
- Use 128 bits AES, change key every 10 seconds



THALES · TELECOM ParisTech · INSTITUT d'OPTIQUE GRADUATE SCHOOL · SEQURENET

Symmetric Encryption with QUantum key REnewal

- Thales : Mistral Gbit
  (fast dedicated AES encryptor)



User window : « sequre drag and drop »

Complete set-up

SEQURE 1011010111011001010001011 THALES TELECOM ParisTech INSTITUT d'OPTIQUE GRADUATE SCHOOL SEQURENET A QUANTUM KEY TO NETWORK SECURITY

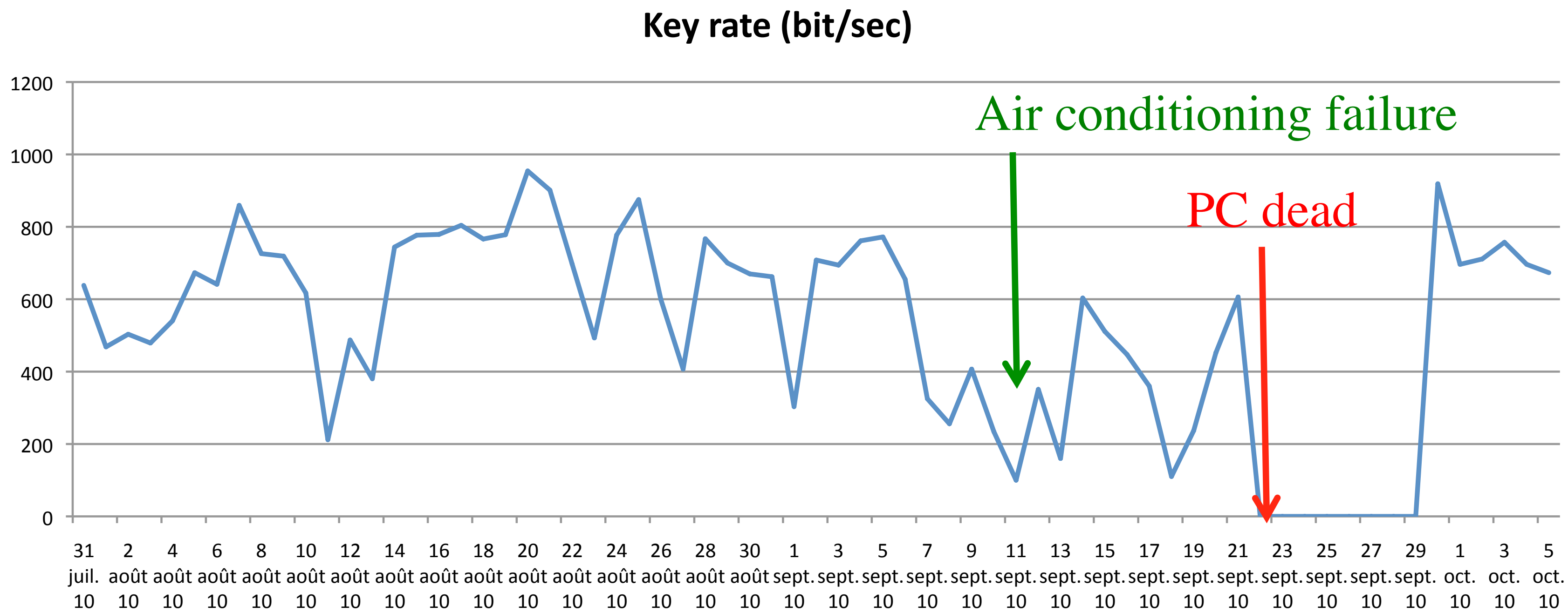
Field implementation

- Fibre link : Thales R&T (Palaiseau) <-> Thales Raytheon Systems (Massy)
- Fiber length about 12 km, 5.6 dB loss

SEQURE 1011010111011001010001011 THALES TELECOM ParisTech INSTITUT d'OPTIQUE GRADUATE SCHOOL SEQURENET A QUANTUM KEY TO NETWORK SECURITY

Results

On site, 12 km distance, 5.6 dB loss
Minimal direct action on hardware (feedback loops, remote control)



See http://www.demo-sequre.com

SEQURE 1011010111011001010001011
THALES
TELECOM ParisTech
INSTITUT d'OPTIQUE GRADUATE SCHOOL
SEQURENET A Quantum Key to Network Security

Quantum Hacking

NTNU Department of Electronics and Telecommunications

UNIK UNIVERSITY GRADUATE CENTER

- Several recent exemples of "quantum hacking" (e.g. Makarov et al.)
- Exploits weaknesses in single photon detectors
- Will NOT work against CVQKD (PIN photodiodes, linear regime)
- Hackers will have to work harder...

Many other works on CVQKD !
<= Theory and Experiments :
(incomplete list !)

arXiv.org > quant-ph > arXiv:1106.0825

Quantum Physics

Security of Post-selection based Continuous Variable Quantum Key Distribution against Arbitrary Attacks

Nathan Walk, Thomas Symul, Timothy C. Ralph, Ping Koy Lam

(Submitted on 4 Jun 2011)

arXiv.org > quant-ph > arXiv:1011.0304

Quantum Physics

Continuous variable quantum key distribution in non-Markovian channels

Ruggero Vasile, Stefano Olivares, Matteo G A Paris, Sabrina Maniscalco

(Submitted on 1 Nov 2010)

arXiv.org > quant-ph > arXiv:0904.1694

Quantum Physics

Feasibility of continuous-variable quantum key distribution with noisy coherent states

Vladyslav C. Usenko, Radim Filip

(Submitted on 10 Apr 2009 (v1), last revised 21 Jan 2010 (this version, v2))

arXiv.org > quant-ph > arXiv:0904.1327

Quantum Physics

Security bound of continuous-variable quantum key distribution with noisy coherent states and channel

Yong Shen, Jian Yang, Hong Guo

(Submitted on 8 Apr 2009 (v1), last revised 29 Jun 2009 (this version, v2))

arXiv.org > quant-ph > arXiv:0903.0750

Quantum Physics

Confidential direct communications: a quantum approach using continuous variables

Stefano Pirandola, Samuel L. Braunstein, Seth Lloyd, Stefano Mancini

(Submitted on 4 Mar 2009)

arXiv.org > quant-ph > arXiv:1006.1257

Quantum Physics

A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution

Yue-Meng Chi, Bing Qi, Wen Zhu, Li Qian, Hoi-Kwong Lo, Sun-Hyun Youn, A. I. Lvovsky, Liang Tian

(Submitted on 7 Jun 2010 (v1), last revised 16 Jul 2010 (this version, v2))

arXiv.org > quant-ph > arXiv:0910.1042

Quantum Physics

A 24 km fiber-based discretely signaled continuous variable quantum key distribution system

Quyen Dinh Xuan, Zheshen Zhang, Paul L. Voss

(Submitted on 6 Oct 2009)

arXiv.org > quant-ph > arXiv:0811.4756

Quantum Physics

Feasibility of free space quantum key distribution with coherent polarization states

D. Elser, T. Bartley, B. Heim, Ch. Wittmann, D. Sych, G. Leuchs

(Submitted on 28 Nov 2008 (v1), last revised 13 Mar 2009 (this version, v2))

arXiv.org > quant-ph > arXiv:0705.2627

Quantum Physics

Experimental Demonstration of Post-Selection based Continuous Variable Quantum Key Distribution in the Presence of Gaussian Noise

Thomas Symul, Daniel J. Alton, Syed M. Assad, Andrew M. Lance, Christian Weedbrook, Timothy C. Ralph, Ping Koy Lam

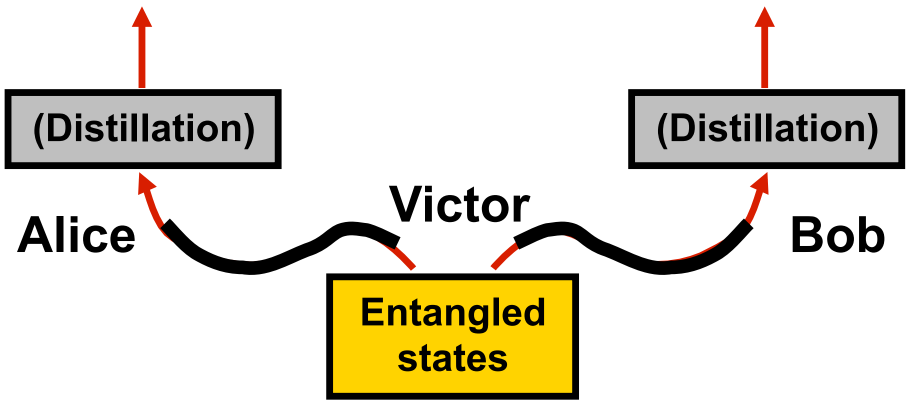
(Submitted on 18 May 2007)

Towards quantum communications and quantum networks ?

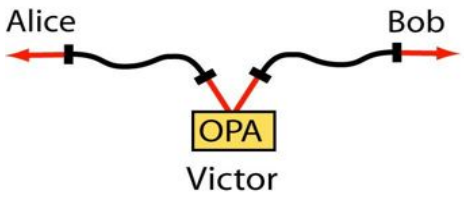
- **Longer distances require « real » entanglement !**
- **"Delocalized" Schrödinger kittens !**

How to create entanglement at a large distance ?

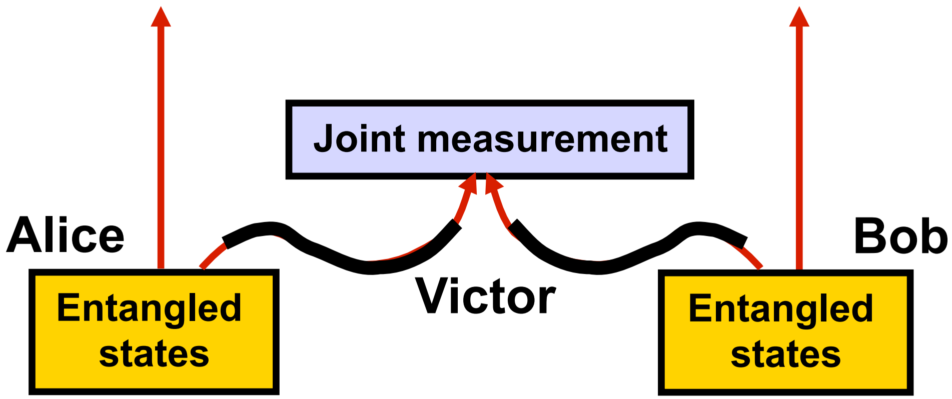
Two main approaches



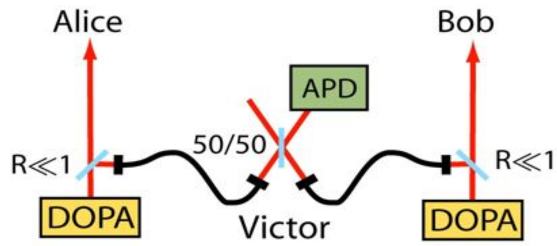
Exemple :



Mostly limites by losses



Exemple :

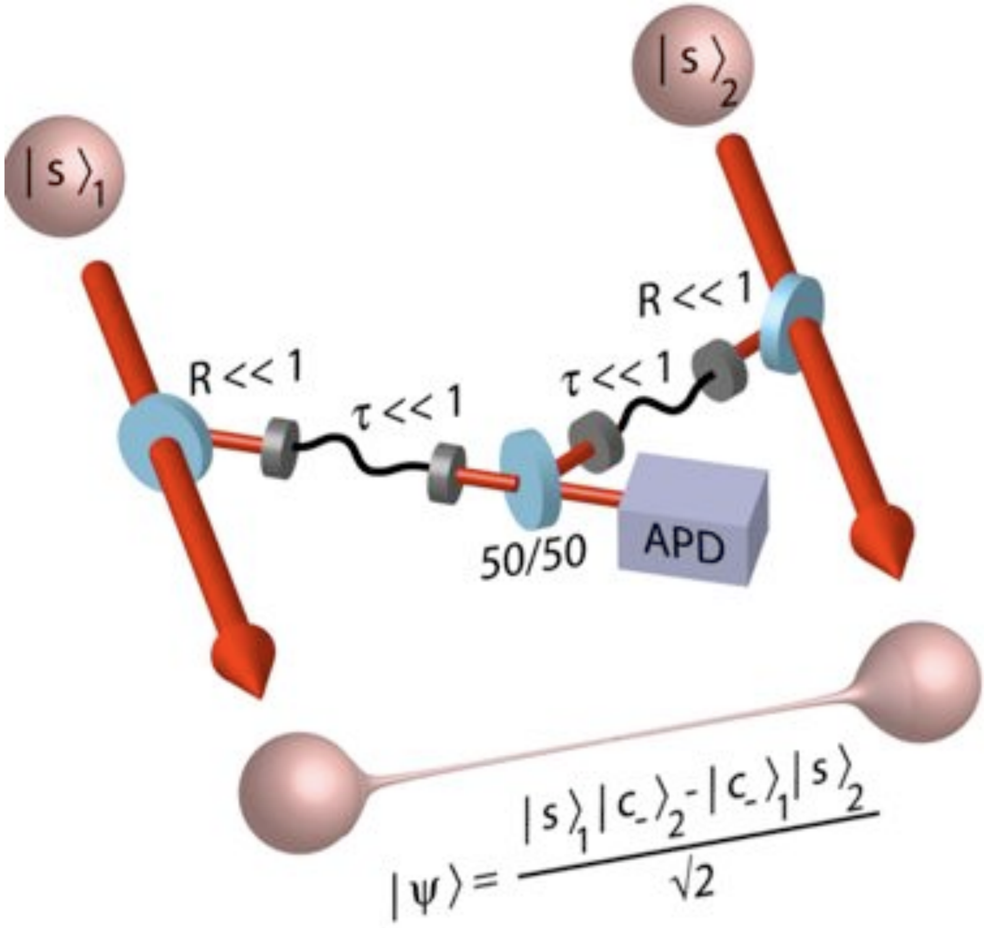


Mostly limited by noise

In the present state of technology, this is much more efficient for distances ~ 100 km

Delocalized photon subtraction

How to avoid the bad effect of losses ? Basic idea :
one should not « distribute » the entangled state, but rather create it at a distance



* Start from two remote squeezed states $|\, s\, \rangle_1$ and $|\, s\, \rangle_2$

* Subtract a photon coherently from the two beams

* Since subtracting a photon creates a cat, creation of an entangled state :

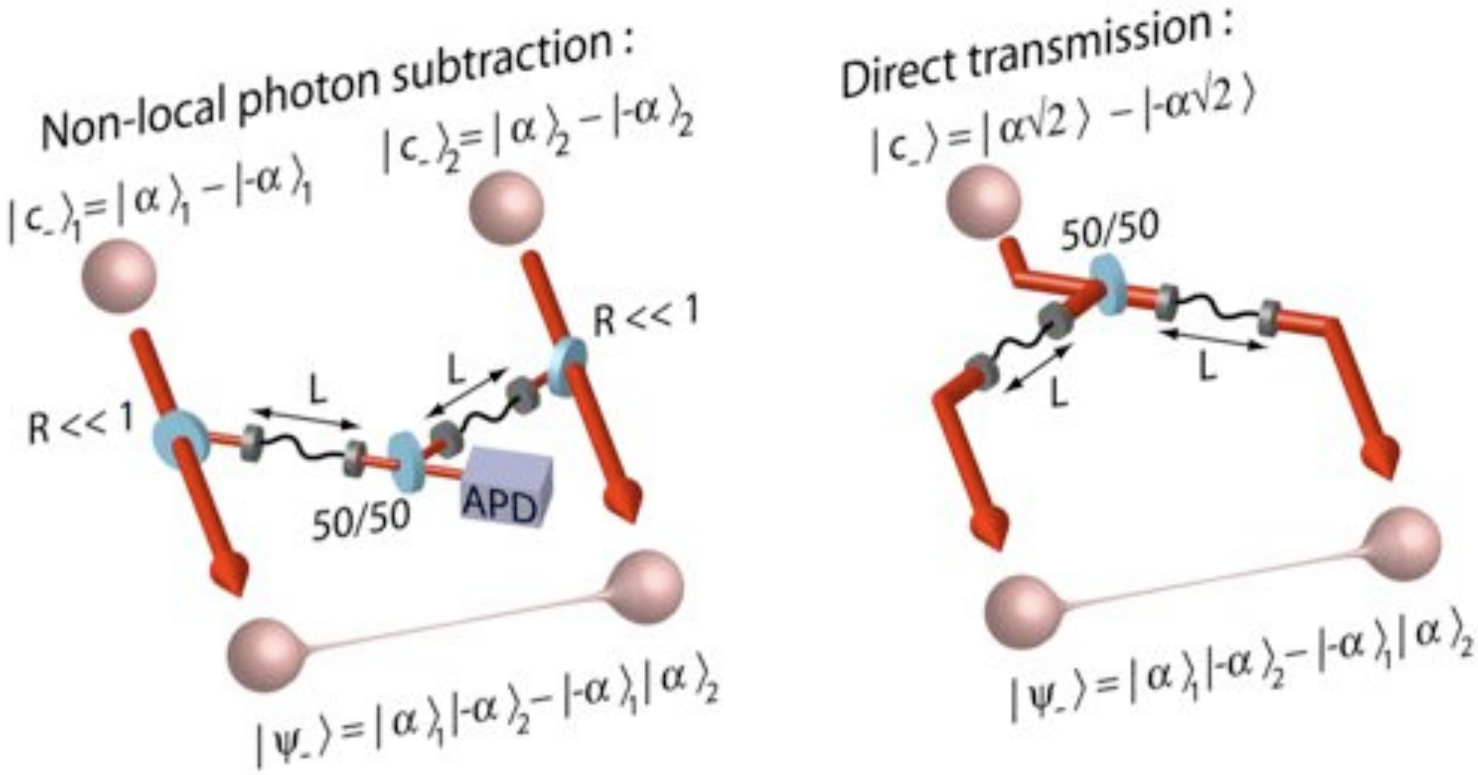
$|\, \Psi \rangle = (|\, s\, \rangle_1\, |\, \mathrm{cat}\, \rangle_2 - |\, \mathrm{cat}\, \rangle_1 |\, s\, \rangle_2)/\sqrt{2}$

"Hamlet state"
(to be or not to be... a cat)

Quantum repeaters with entangled coherent states

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**

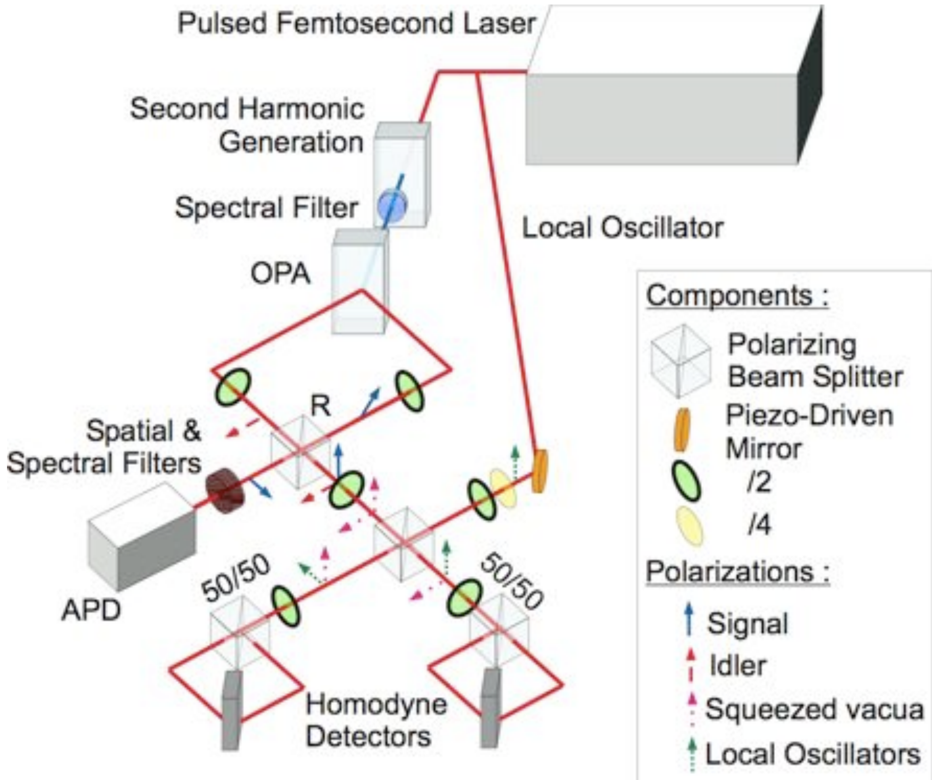
INSTITUT d'OPTIQUE GRADUATE SCHOOL

Experiment

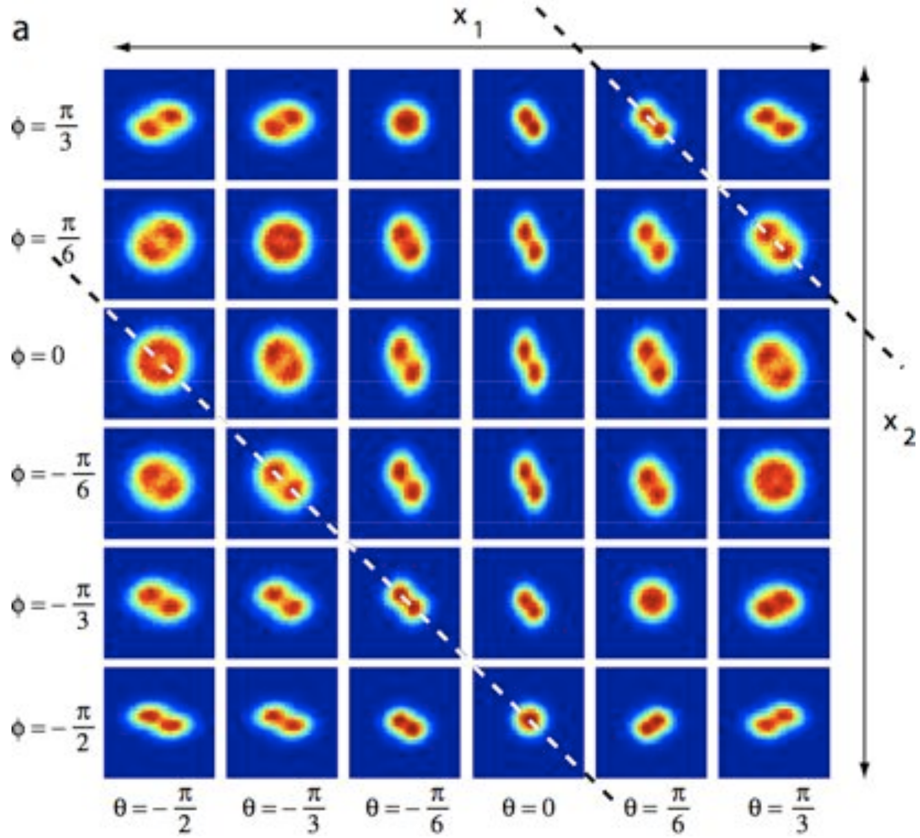
A. Ourjoumtsev et al, Nature Physics, 5, 189, 2009

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

QIPC



Experimental set-up



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

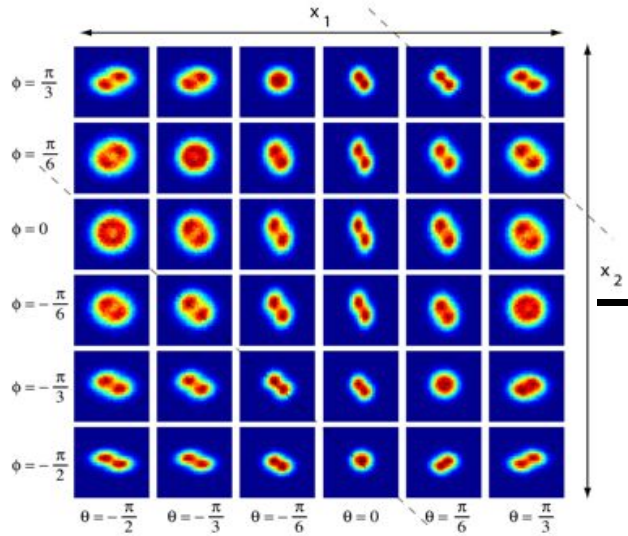
Results

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

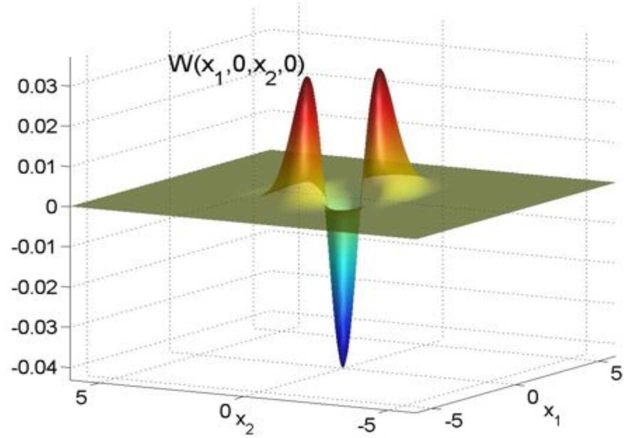
QIPC

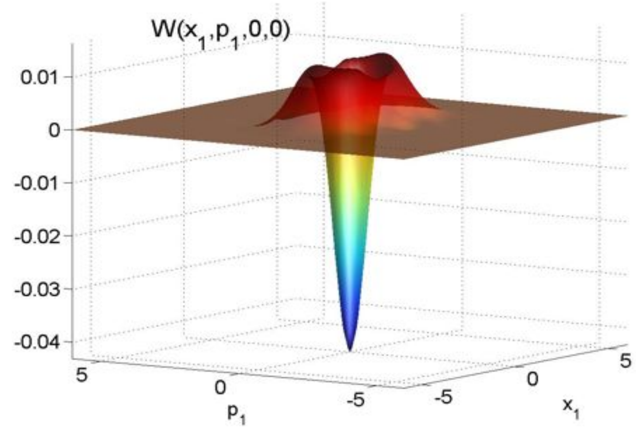
Full two-mode tomography :

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



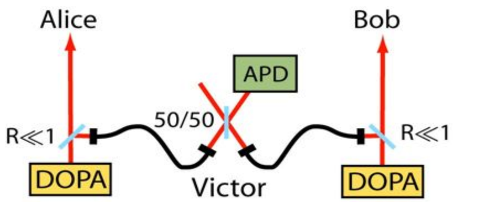
Cuts of the experimental 4D Wigner function, corrected for homodyne losses





Entanglement : N = 0,25 ± 0,04

Almost insensitive to losses in the quantum channel !



… but still far from a quantum repeater !

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

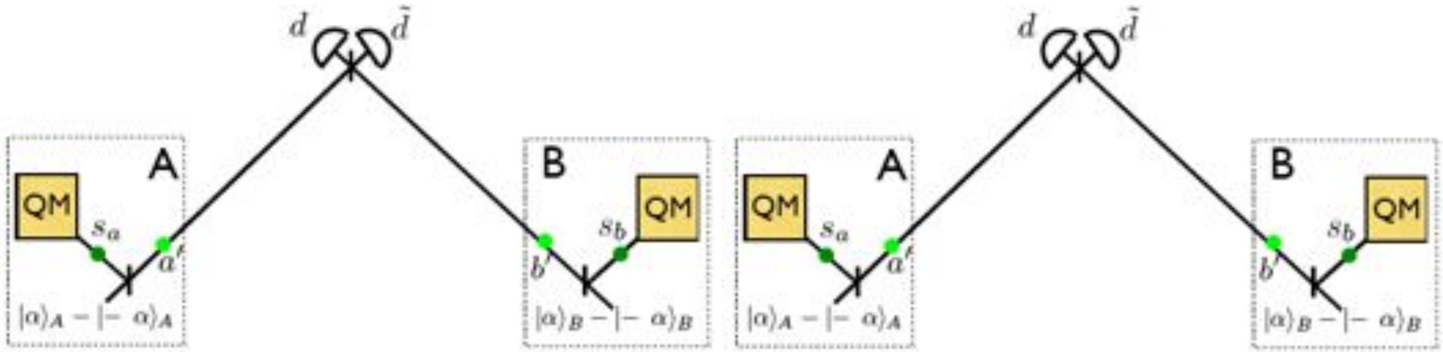
~ 100 km optical fiber

Quantum repeaters with entangled cats ?

N. Sangouard, C. Simon, N. Gisin, J. Laurat,

R. Tualle-Brouri and P. Grangier, JOSA B 27, 137 (2010)

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 →

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

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)

Conclusion

Many potential uses for Quantum Continuous Variables…

* Quantum cryptography

* Coherent states protocols using reverse reconciliation,

secure against any (gaussian or non-gaussian) collective attack

* Working fine in optical fibers @1550 nm (SECOQC project)

* Conditional preparation of « squeezed » non-gaussian pulses / cats

* Big family of phase-dependant states with negative Wigner functions !

* See also many new experimental results by the groups of

A. Lvovsky, M. Bellini, E. Polzik, T. Gerrits, A. Furusawa, M. Sasaki...

* First step towards : - entanglement distillation procedures ?

- new tests of Bell's inequalities ?

- quantum computing ? (QCV version of KLM…)