CRYPTOGRAPHIE ET INTRICATION AVEC DES VARIABLES QUANTIQUES CONTINUES

Frédéric Grosshans [1], Jérome Wenger [1], Rosa Tualle-Brouri [1], Alexei Ourjoumtsev [1], Jérôme Lodewyck [1], Gilles Van Assche[2], Raul Garcia-Patron[2], Jaromir Fiuracek[2], Nicolas Cerf [2], and Philippe Grangier [1]

1 Laboratoire Charles Fabry de l'Institut d'Optique, 91403 Orsay, France

2 Ecole Polytechnique, Université Libre de Bruxelles, 1050 Brussels, Belgium

Institut d'Optique

Content of this talk

QIPC

* Quantum continuous variables
  from homodyne detection
  to Quantum Key Distribution

* Quantum cryptography with coherent states (Nature 2003).
  from Shannon's theorem
  to unconditionnal security proofs

* Manipulation of non-gaussian states of the light (PRL 2004).
  from experimental observation of non-gaussian states
  to entanglement distillation and
  « loophole-free » tests of Bell's inequalities

Optical Quantum Continuous Variables

Institut d'Optique

QIPC

* What are quantum optical continuous variables ?

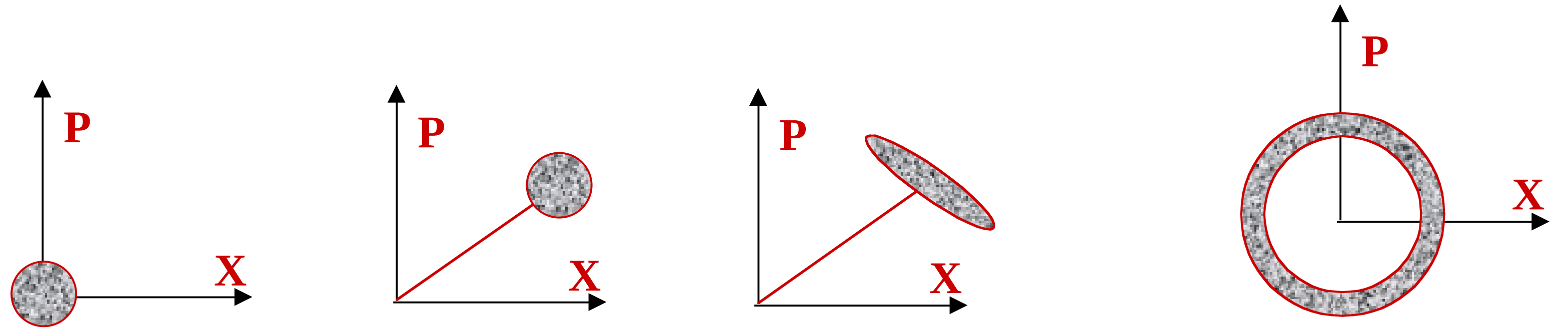
* Quantization of the Electromagnetic field

$\rightarrow$ Modes are quantum harmonic oscillators

* Discrete degrees of freedom (photon number)

* Continuous degrees of freedom (quadratures = X and P)

* Convenient representation : phase space



Vacuum state | Coherent state | Squeezed state | Number state

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

Homodyne detection

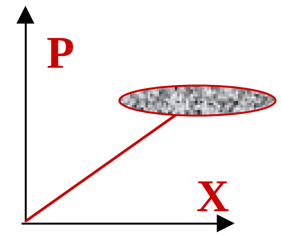
$$I_1 = |E_{LO}|^2 + |E_S|^2 + |E_{LO}| \, (E_S \, e^{-i\varphi LO} + E_S^* \, e^{i\varphi LO})$$

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

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

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

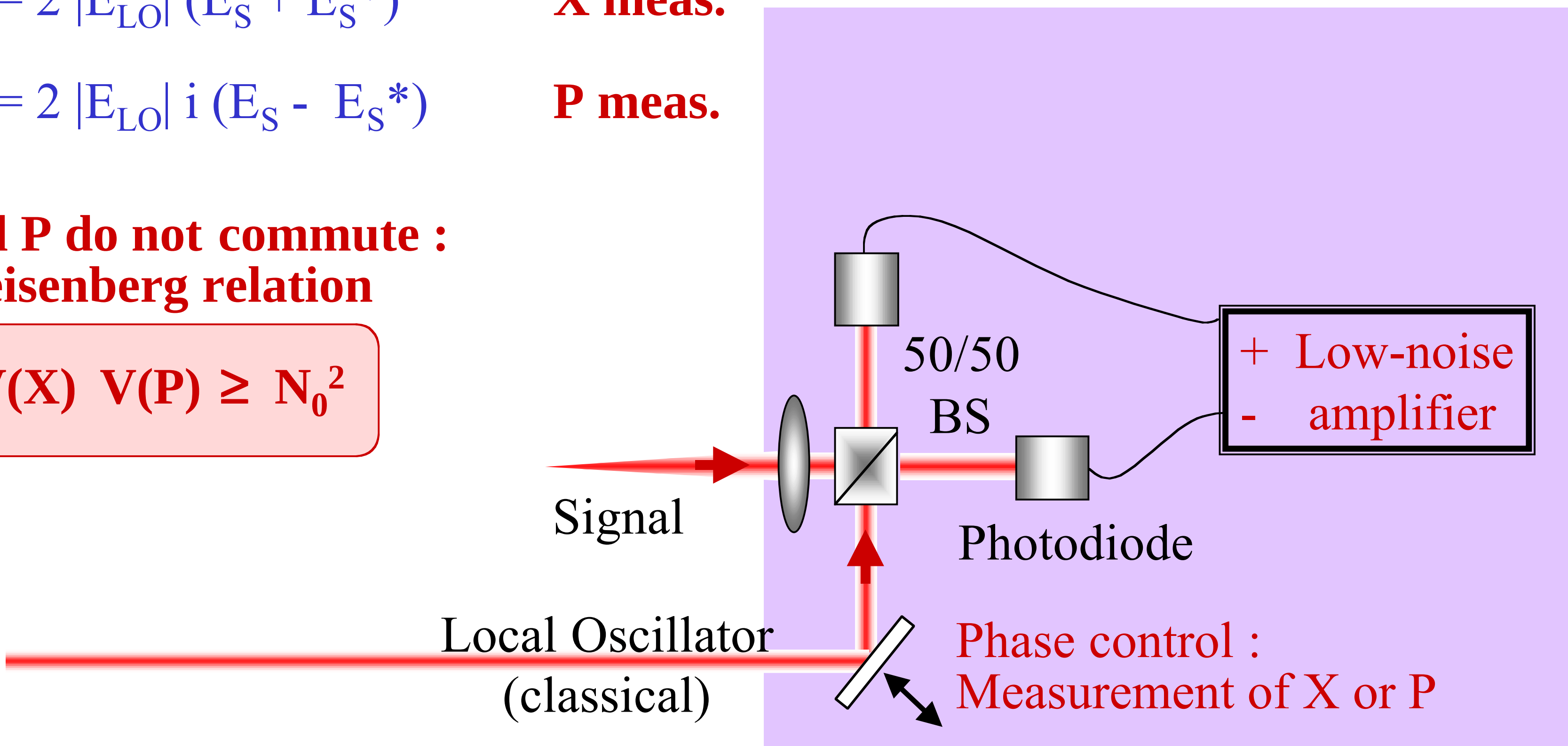
$$= 2 \, |E_{LO}| \, i \, (E_S - E_S^*) \qquad \textbf{P meas.}$$



Squeezed state

X and P do not commute :
Heisenberg relation

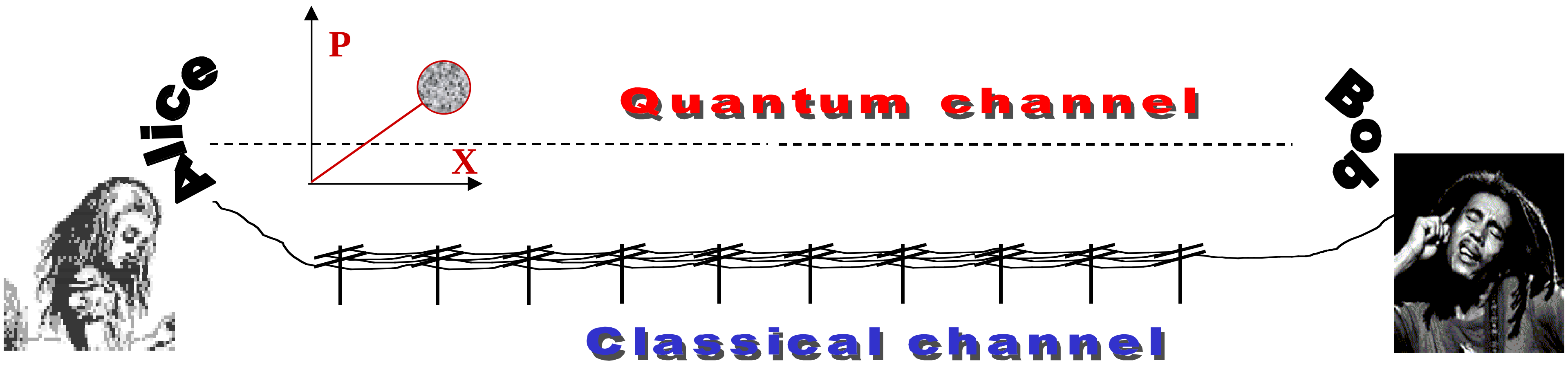
$$V(X) \; V(P) \geq N_0^2$$



Institut d'Optique

Coherent States Quantum Key Distribution

QIPC



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

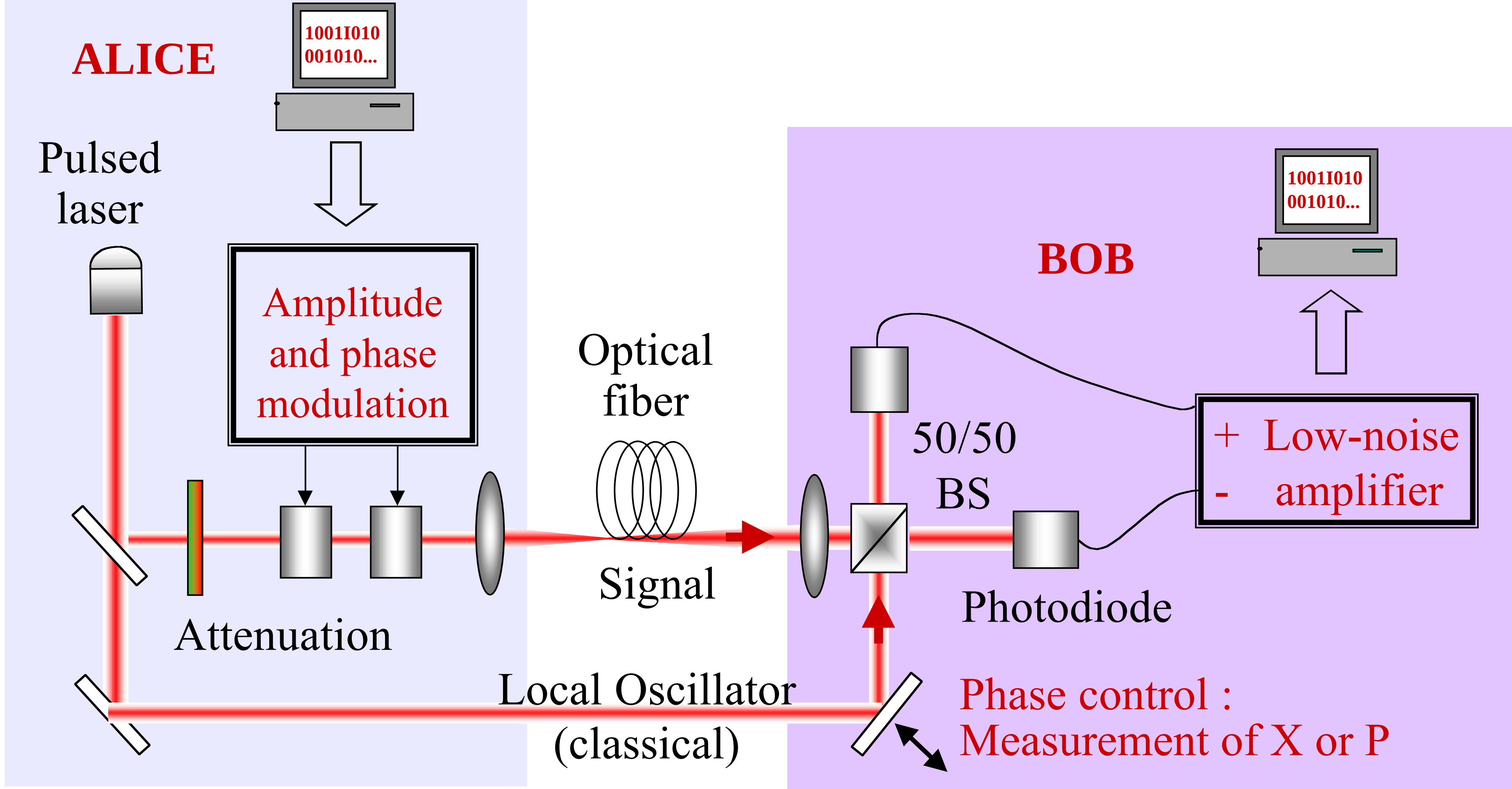
-> **not restricted to single photon polarization !**

-> New QKD protocol where :

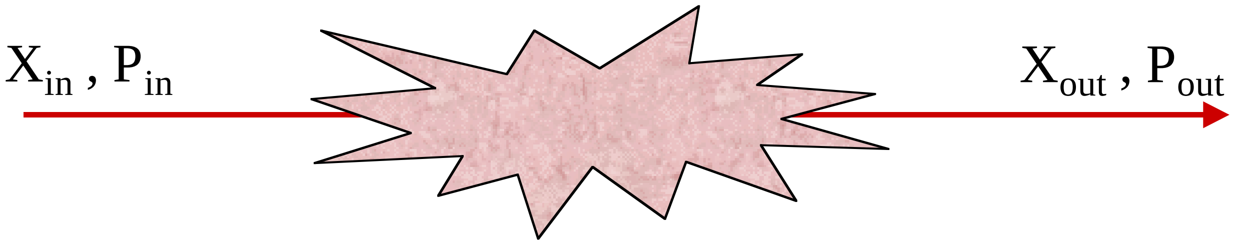
* The non-commuting observables are the quadrature operators X and P
* The transmitted light contains weak coherent pulses (about 100 photons) with a gaussian modulation of amplitude and phase
* The detection is made using shot-noise limited homodyne detection

Homodyne detection

	Homodyne	Counting (APD)
Efficiency	> 90%	10-50 %
Dark rate	negligible	problem
Data rate	10 MHz++	100 kHz



Linear Transmission Channel



General Linear Transformation (Heisenberg-Langevin type equations) :

$$\mathbf{X_{out} = g_x X_{in} + F_x} \qquad \qquad \mathbf{P_{out} = g_p P_{in} + F_p}$$

Assumption : added noise F_x , F_P are uncorrelated with X_{in} , P_{in}

Convenient characterization of the channel :

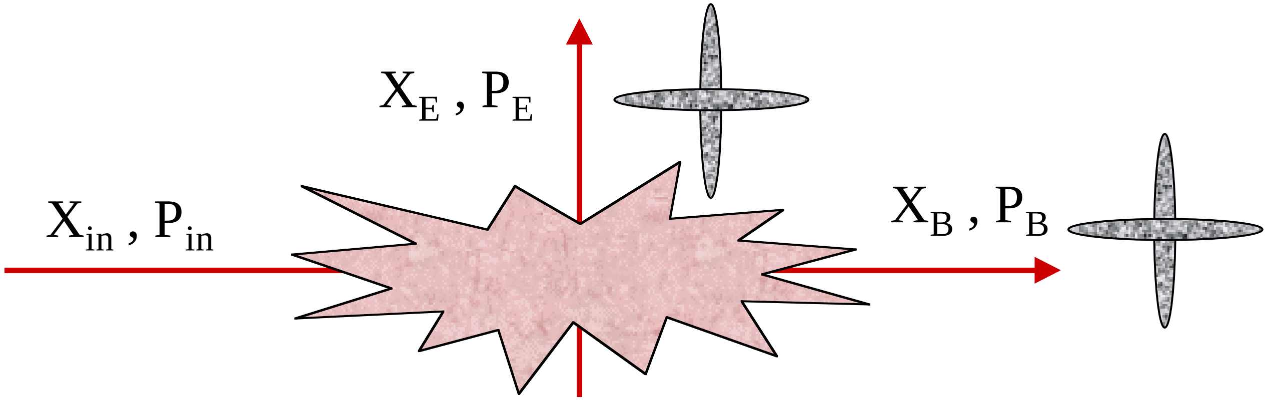
[see e.g. P. Grangier et al., Nature **396**, 537 (1998)]

*** Gain parameters g_x , g_p**

*** Equivalent Input Noises** (cf electronic amplifiers) :

$$N_{eq,X} = < F_X{}^2 > / \, | \, g_x \, |^2 \qquad \qquad N_{eq,P} = < F_P{}^2 > / \, | \, g_p \, |^2$$

Linear Transmission Channel



Two outputs denoted as « Signal » and « Meter »
« Bob » and « Eve »

Heisenberg relations on the equivalent input noises !

$$N_{eqB,X} N_{eqE,P} \geq N_0^2 \qquad N_{eqB,P} N_{eqE,X} \geq N_0^2$$

N_0 : vacuum noise

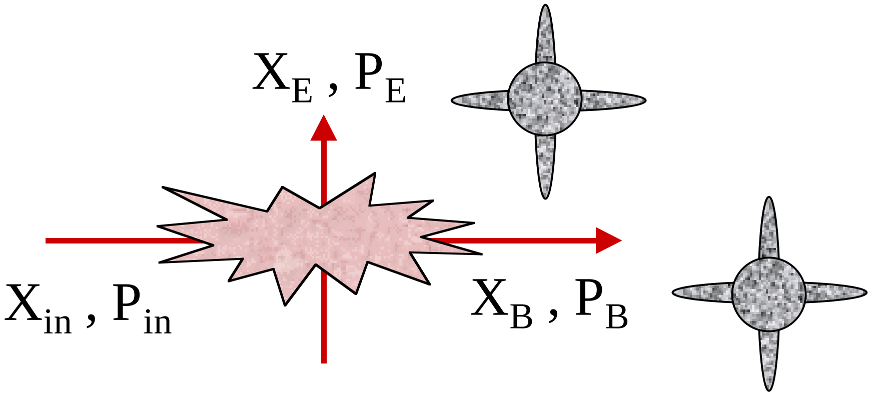
If Eve tries to measure one quadrature,
then Bob will see strong « back-action noise » on the other quadrature.

…but one can get $N_{eqB,X} N_{eqE,X} < N_0^2$

Arbitrarily good measurement of one quadrature is possible for Eve and Bob !

Initially introduced as a « criterion » for a « QND measurement » of X

From QND to QKD



$$N_{eqB,\,X}\, N_{eqE,\,P} \geq N_0^2$$
$$N_{eqB,\,P}\, N_{eqE,\,X} \geq N_0^2$$

(N_0 : vacuum noise)

Fundamental idea for quantum key distribution:
Alice and Bob encode information on X and P (and don't tell it in advance !)

Then $N_{eqB,\,X} = N_{eqB,\,P} = N_{eqB}$ and the best choice for Eve is $N_{eqE,\,X} = N_{eqE,\,P} = N_{eqE}$

Since everything is symmetric for X and P then :

$N_{eqB}\, N_{eqE} \geq N_0^2$ (no-cloning theorem !)

(optimal cloning for QCV : $N_{eqB} = N_{eqE} = N_0$)

QKD protocol using coherent states with gaussian amplitude and phase modulation

Institut d'Optique

QIPC

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

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

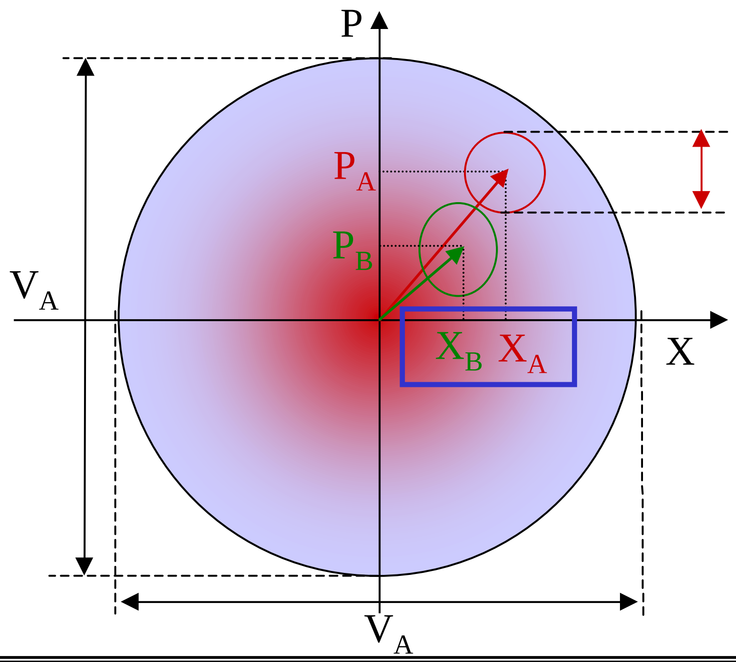
Reminder : I(X; Y) =
H(X) - H(X | Y) =
H(Y) - H(Y| X) =
H(X) + H(Y) - H(X; Y)

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

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

(c) Bob measures either X_B or P_B

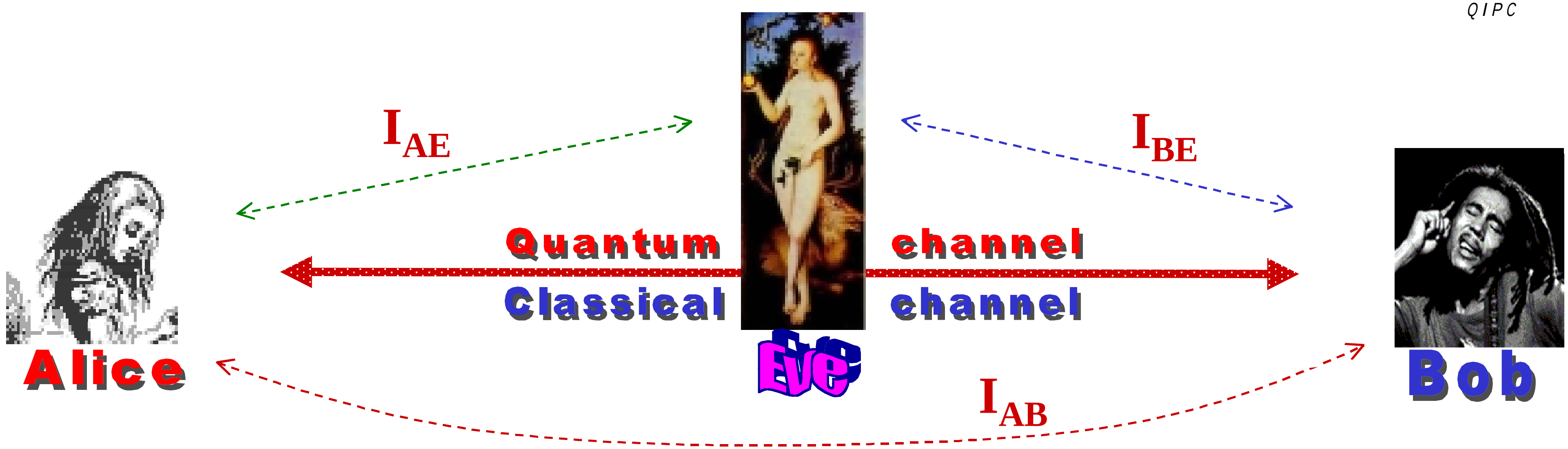
(d) Bob and Alice agree on the basis choice (X or P), and keep the relevant values.



Data Reconciliation

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

QIPC



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

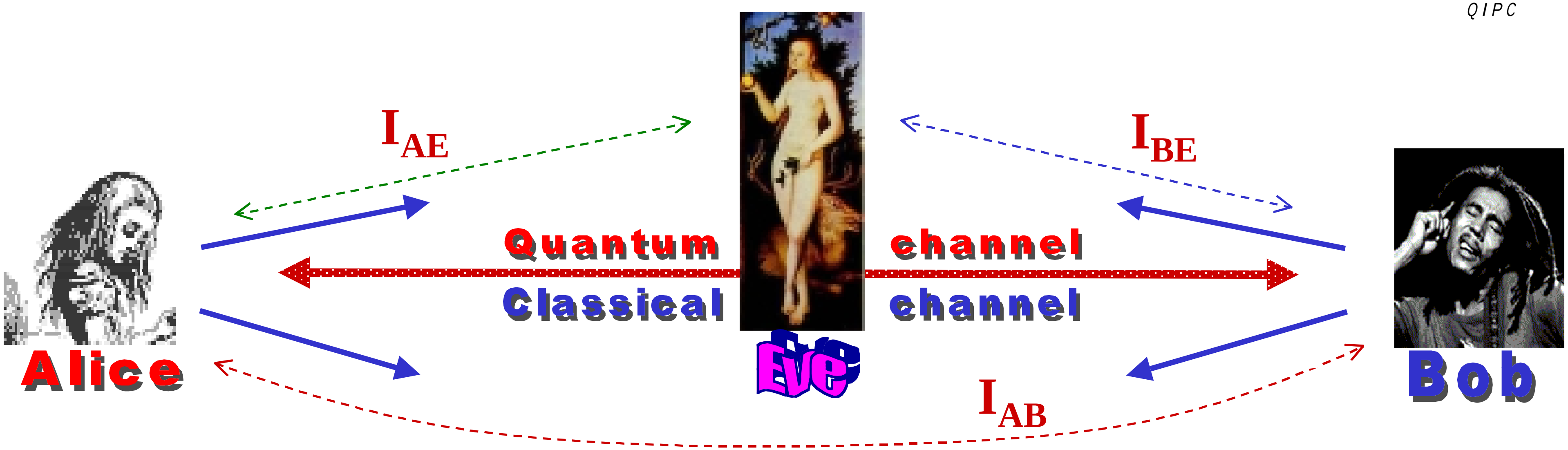
Alice and Bob can in principle distill, from their correlated key elements, a common secret key of size $S > \sup(I_{AB} - I_{AE}, I_{AB} - I_{BE})$ bits per key element.

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).

Institut d'Optique

Data Reconciliation

QIPC



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 orrects 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} ?

Direct reconciliation

Bounding I_{AE} (F. Grosshans and P. Grangier, *PRL* **88**, 057902 (2002)).

$$I_{AB} = 1/2 \ \log_2 [1 + V_A / (N_0 + N_{eqB})]$$

$$I_{AE} = 1/2 \ \log_2 [1 + V_A / (N_0 + N_{eqE})]$$

where
- V_A : variance of Alice's modulation
- N_0 : shot noise (coherent state)
- N_{eqB} : « equivalent input noise » on Bob 's side
- N_{eqE} : « equivalent input noise » on Eve 's side

see e.g. : P. Grangier et al., Nature **396**, 537 (1998).

From Heisenberg $N_{eqB} N_{eqE} \geq N_0^2$ (no cloning !) and thus :

$$I_{AE} \leq 1/2 \ \log_2 [1 + V_A / (N_0 + N_0^2 / N_{eqB})]$$

$$I_{AB} > (I_{AE})_{best} \quad \text{iff} \quad N_{eqB} < N_0$$

Reverse Reconciliation

Bounding I_{BE} (F. Grosshans et al., *Nature* **421**, 238 (2003))

How well can Alice and Eve infer Bob's measurement results ?

Define the « conditional variance » $V(X_B \mid X_E) = V(X_B) - |\langle X_B X_E \rangle|^2 / V(X_E)$

Conditional variances are also bounded by Heisenberg relations :

$$V(X_B|X_A)_{min}\, V(P_B|P_E) \geq N_0^2 \qquad V(P_B|P_A)_{min}\, V(X_B|X_E) \geq N_0^2$$

Using again Shannon's theorem… (and some algebra…)

$$I_{BA} > (I_{BE})_{best} \quad \text{iff} \quad T^2 (N_0 + N_{eqB}) (N_0 / V + N_{eqB}) < N_0^2$$

The security condition involves both T (channel transmission) **and N_{eqB}**

(for direct reconciliation : $N_{eqB} < N_0$)

Summary on reconciliation protocols

QIPC

The noise seen by Bob can be split in two parts (known by Alice and Bob !):

$$N_{eqB} = N_{losses} + N_{excess} = N_0 (1 - T_{line}) / T_{line} + N_{exc}$$

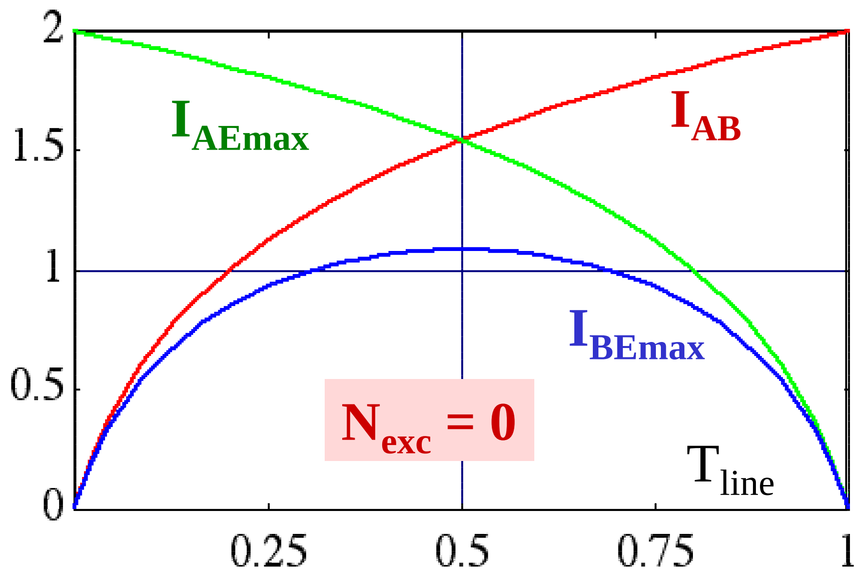
Summary on reconciliation protocols

QIPC

The noise seen by Bob can be split in two parts (known by Alice and Bob !):

$$N_{eqB} = N_{losses} + N_{excess} = N_0 (1 - T_{line}) / T_{line} + N_{exc}$$

Mutual information (bits / symbol) for V_A=15 N_0



* I_{AE} : relevant for direct reconciliation, requires $T_{line} > 0.5$ and $N_{exc} < N_0$
* I_{BE} : relevant for reverse reconciliation, requires $N_{exc} < 0.5\ N_0$

can be secure for any line transmission !

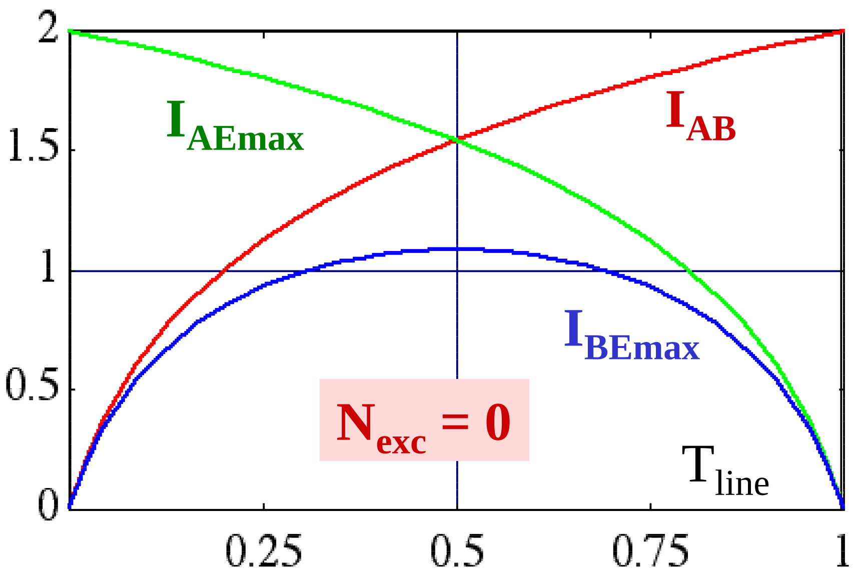
Summary on reconciliation protocols

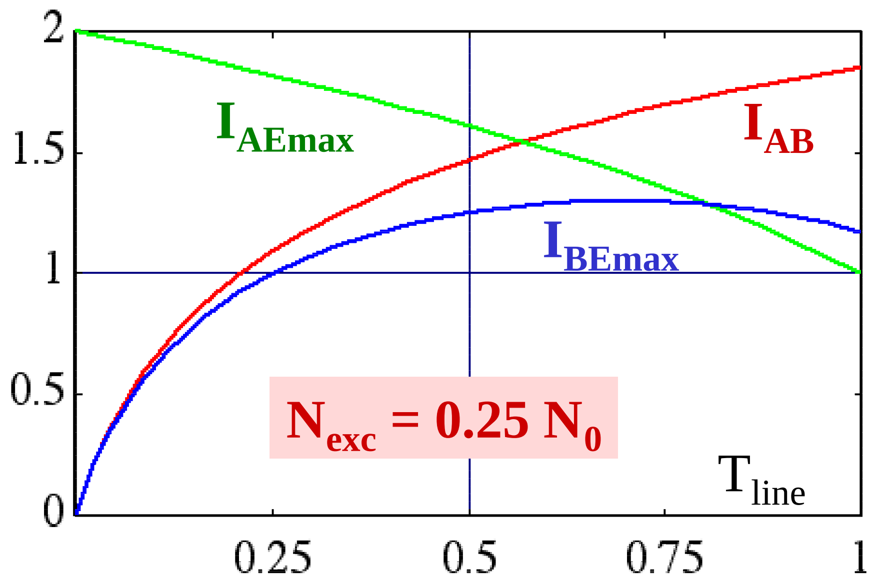
QIPC

The noise seen by Bob can be split in two parts (known by Alice and Bob !):

$$N_{eqB} = N_{losses} + N_{excess} = N_0 (1 - T_{line}) / T_{line} + N_{exc}$$

Mutual information (bits / symbol) for $V_A = 15\ N_0$



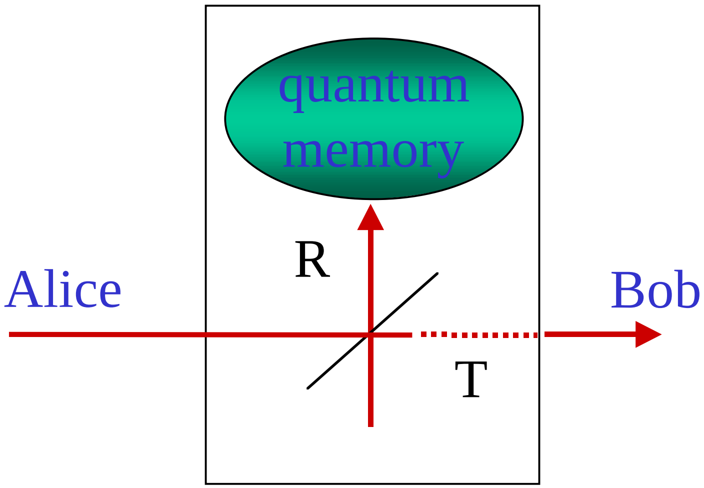


* I_{AE} : relevant for direct reconciliation, requires $T_{line} > 0.5$ and $N_{exc} < N_0$
* I_{BE} : relevant for reverse reconciliation, requires $N_{exc} < 0.5\ N_0$

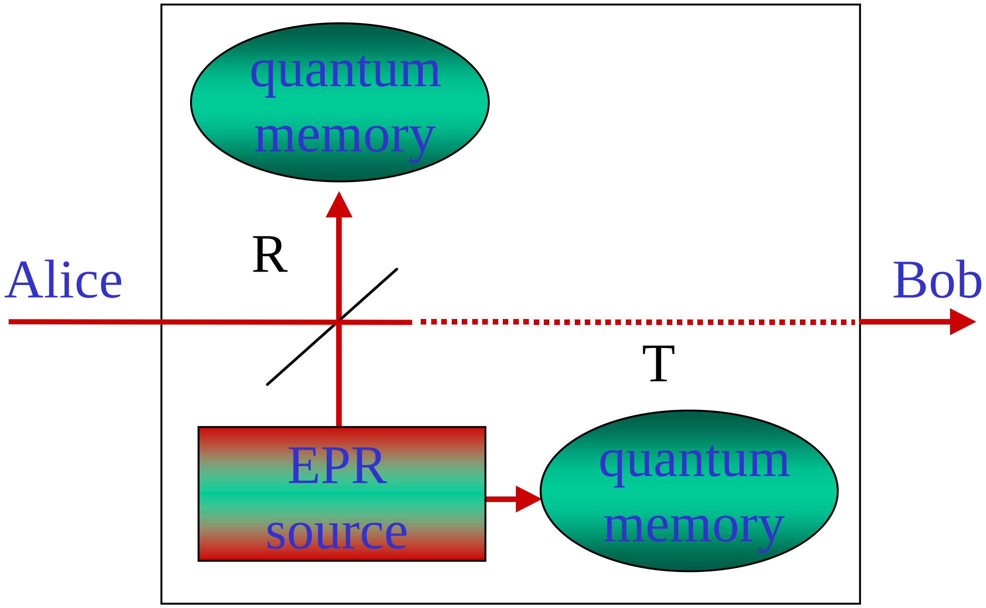
can be secure for any line transmission !

Eve 's attacks

Attacks considered in our proof are **individual gaussian attacks** (not easy !)



Eve's best attack against
direct reconciliation :
cloning machine (= BS)
+ quantum memory
$\mathbf{N_{eqB} = (T/R)\, N_0}$
$\mathbf{N_{eqE} = (R/T)\, N_0}$



Eve 's best attack against
reverse reconciliation :
« entangling cloner »
+ quantum memories

Experimental set-up

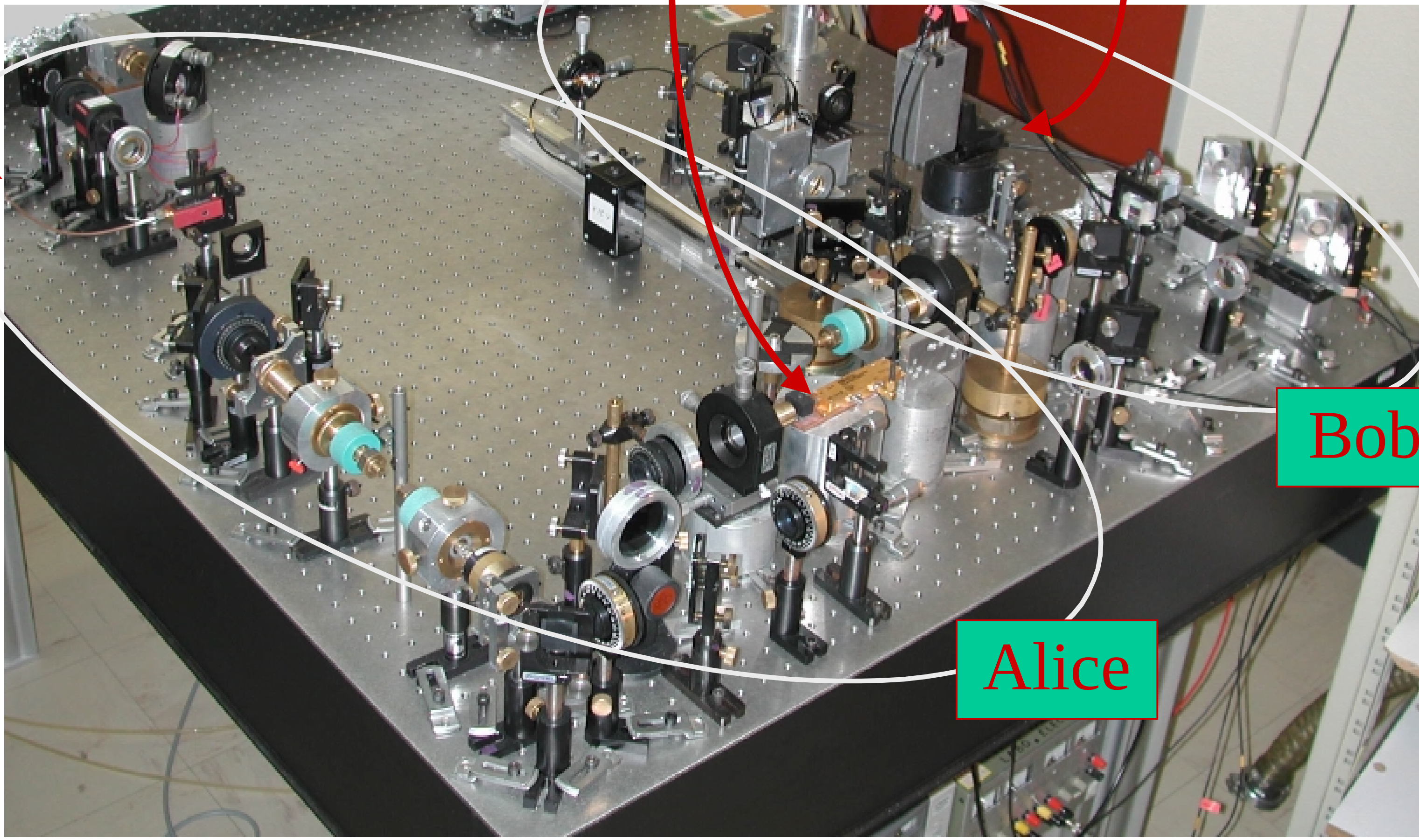
F. Grosshans et al., Nature **421**, 238 (2003)

QIPC

Laser diode (780 nm)
+ Pulsing AOM
(120 ns, rep. rate 800 kHz)

Alice EO Modulator

Pulsed homodyne detection
Signal pulses : 100 phot.
LO pulses : 3 10^8 phot.

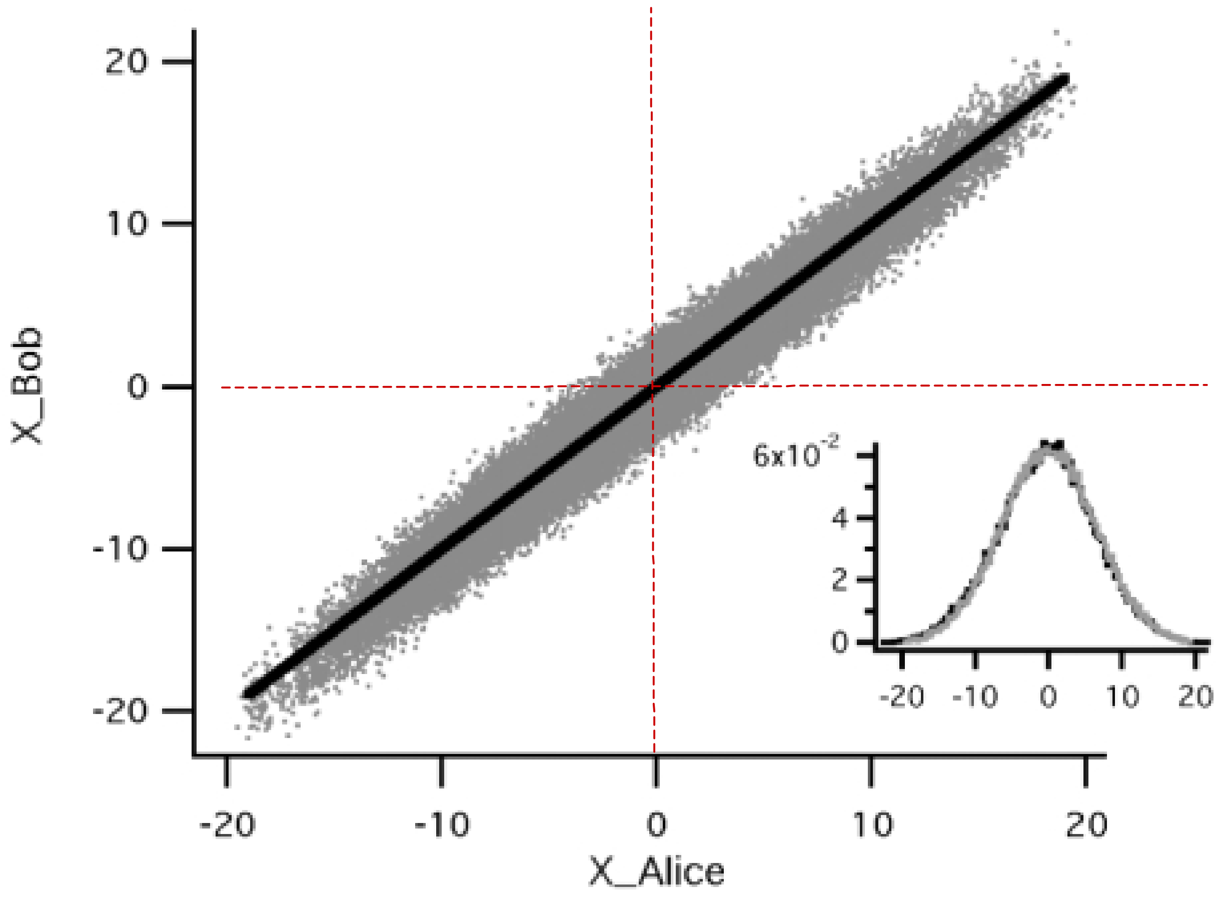


Coherent state QKD : experiment

F. Grosshans et al., Nature **421**, 238 (2003)

QIPC

Example of exchanged data
(burst of 60000 pulses @ 800 kHz, no on-line loss)



Gaussian with
$V_A \approx 40\ N_0$
$\sigma_X \approx 6.5\ \sigma_0$

Coherent state QKD : results

F. Grosshans et al., Nature **421**, 238 (2003)

QIPC

Practical SK rate : final results, taking into account « all » imperfections

Requires an optimized method for extracting secret bits from the correlated strings of continuous data shared by Alice and Bob : **"sliced reconciliation"**

[N.J. Cerf, M. Lévy and G. Van Assche, *PRA* **63**, 052311 (2001)].

V_A	T_{line}	I_{BA}	I_{BE} (% of I_{BA})	Ideal SK rate	Practical SK rate
40.7	1	2.39	0%	1920 kb/s	1700 kb/s
37.6	0.79	2.17	58%	730 kb/s	470 kb/s
31.3	0.68	1.93	67%	510 kb/s	185 kb/s
26.0	0.49	1.66	72%	370 kb/s	75 kb/s

in shot-noise units

bits/pulse

Corresponding to a pulse rate 800 kHz

Some questions…

* Security of QKD is often said to be related to entanglement…

Where is the entanglement here ?

* The security proof is valid for individual gaussian attacks

What about « unconditional » security ?
(i.e. vs collective non-gaussian attacks ?)

Continuous-variables EPR beams

$(X_A + X_B)$ 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) !

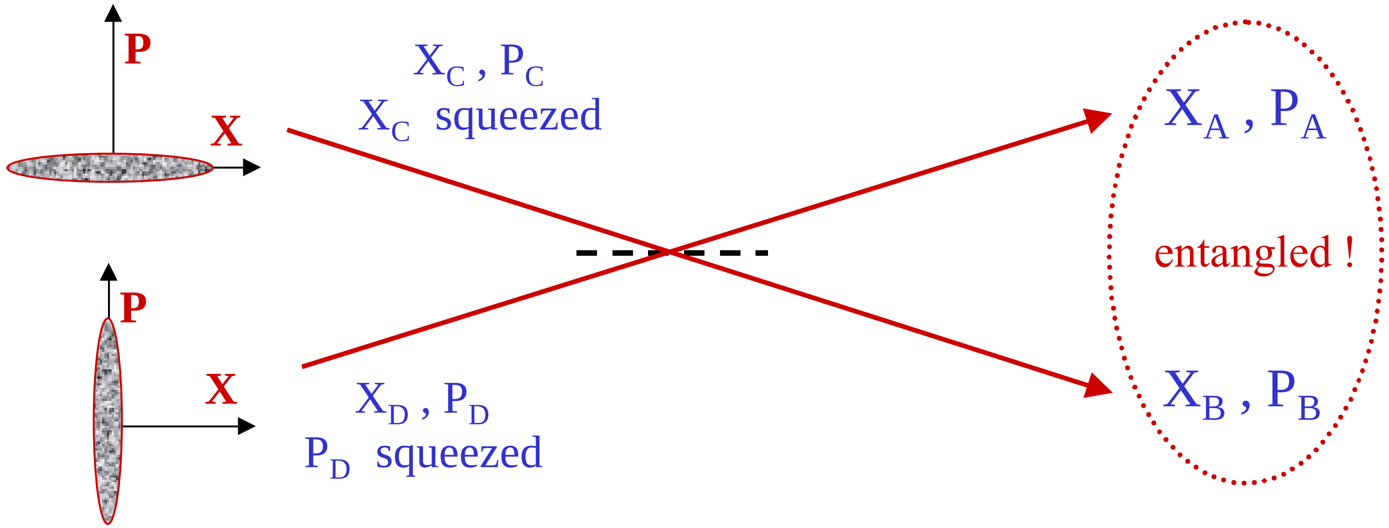
How to produce QCV entangled beams ?

(see also poster by Alexei Ourjoumtsev)

Institut d'Optique

QIPC

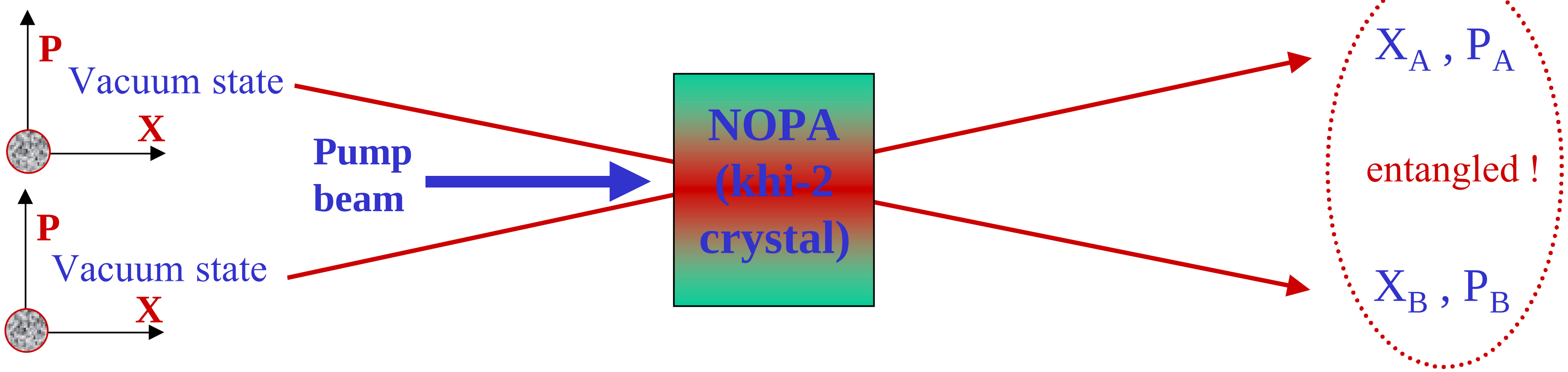
1. Combine two orthogonally squeezed beams



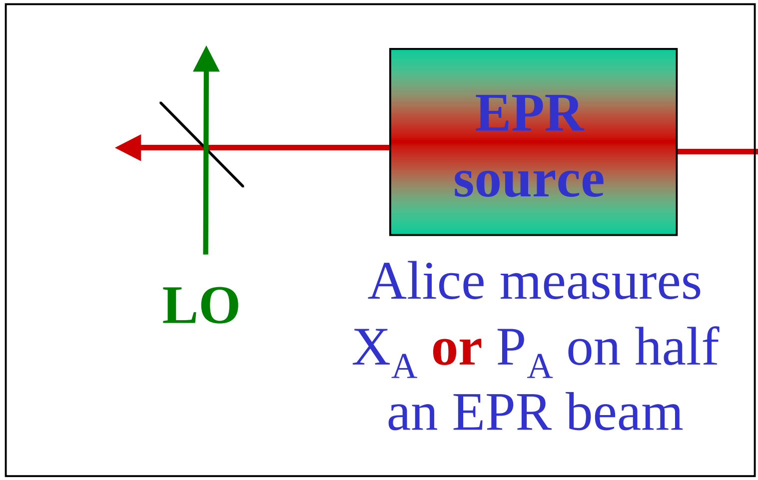
$$X_C = (X_A + X_B)/\sqrt{2}$$
$$P_C = (P_A + P_B)/\sqrt{2}$$
$$X_D = (X_A - X_B)/\sqrt{2}$$
$$P_D = (P_A - P_B)/\sqrt{2}$$

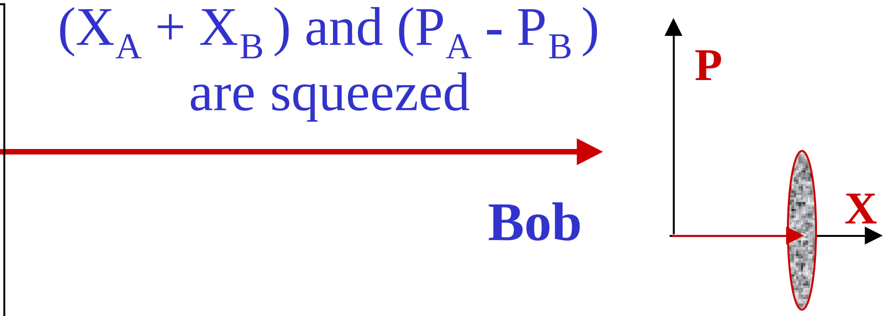
OK !

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

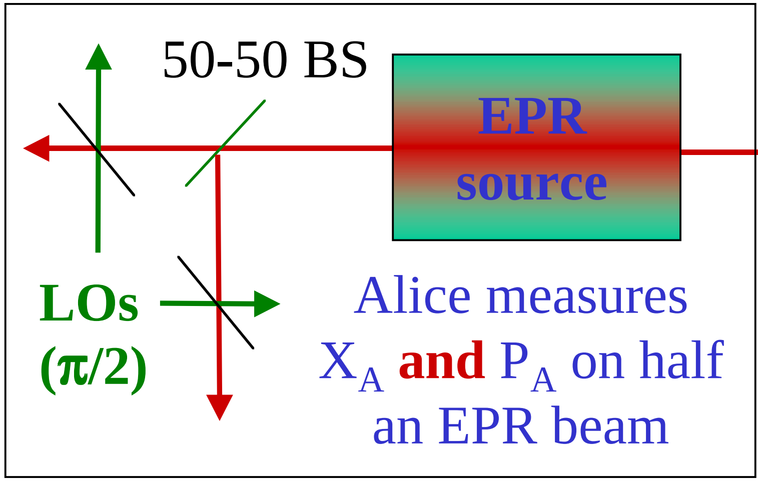


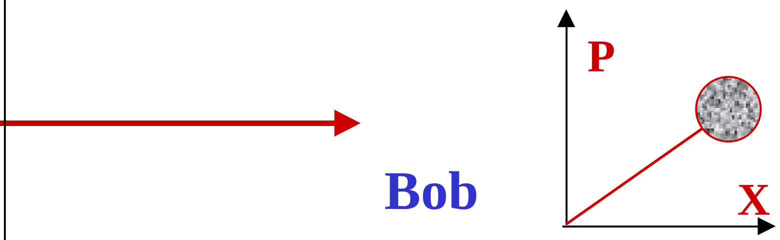
EPR versus coherent protocol





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





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

EPR protocol equivalent to our coherent state protocol !

Cf BB84 vs entangled pair (Ekert) protocol

Entanglement condition

Institut d'Optique

QIPC

Assume EPR beams with squeezing s = 1/V, and equivalent noises :

$$N_{eqA} = N_0 (1 - T_A) / T_A \quad \text{(no excess noise on Alice's side!)}$$
$$N_{eqB} = N_0 (1 - T_{line}) / T_{line} + N_{exc}$$

The criterion for entanglement (Peres-Horodecki for gaussian continuous variables : Duan et al, Simon) is independant of T_{line} , T_A, and V and writes :

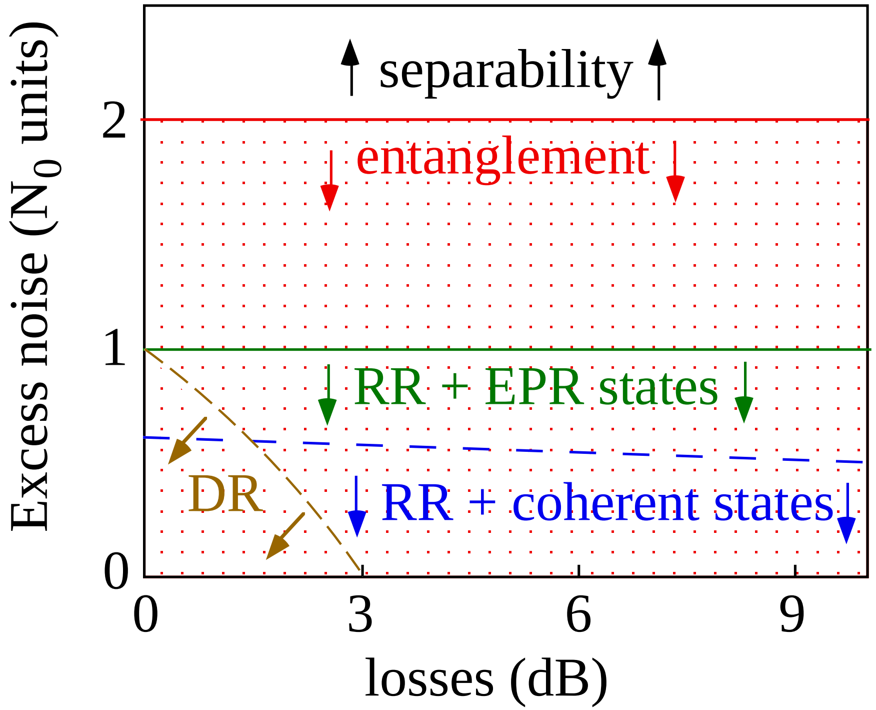
$$N_{exc} < 2 \ N_0$$

On the other hand, the security thresholds for both direct reconciliation and reverse reconciliation coherent states protocols require :

$$N_{exc} < N_0$$

Well within the entanglement region !

Security of coherent states QKD



DR : Direct Reconciliation
RR : Reverse Reconciliation

The DR and RR coherent states protocols are well within the « virtual entanglement » region !

Hint for unconditional security ?

Security of coherent states QKD

QIPC

Series of security proofs based on « virtual entanglement » :

* Proof of security against individual gaussian attacks
F. Grosshans et al., Nature **421**, 238 (2003)

* Proof of security against arbitrary finite-size attacks
(individual gaussian attacks are actually optimal ! same secret rates)
F. Grosshans and N.J. Cerf, PRL **92**, 047905 (2004)

* Proof of security against arbitrary collective attacks
(one can distill entangled qubits using CSS codes; secret rates ?)
S. Iblisdir, G. Van Assche, N.J. Cerf, PRL **93**, 170502 (2004)

* Other approaches for collective attacks (OK for losses < 1.9 dB) :
F. Grosshans, PRL **94**, 020504 (2005)
M. Navascuès and A. Acin, PRL **94**, 020505 (2005)

Cryptography vs entanglement

QIPC

Entanglement is NOT required for cryptographic security
(only the channel ability to transmit entanglement is required !)
… so is entanglement really useful ?

* Practical advantages of « actual » EPR beams vs. coherent states :

- The random values needed by Alice (encoding) and Bob (decoding) do not have to be externally generated (possibly by another quantum process), but they are produced by the protocol itself (« the key does not exist beforehand »).

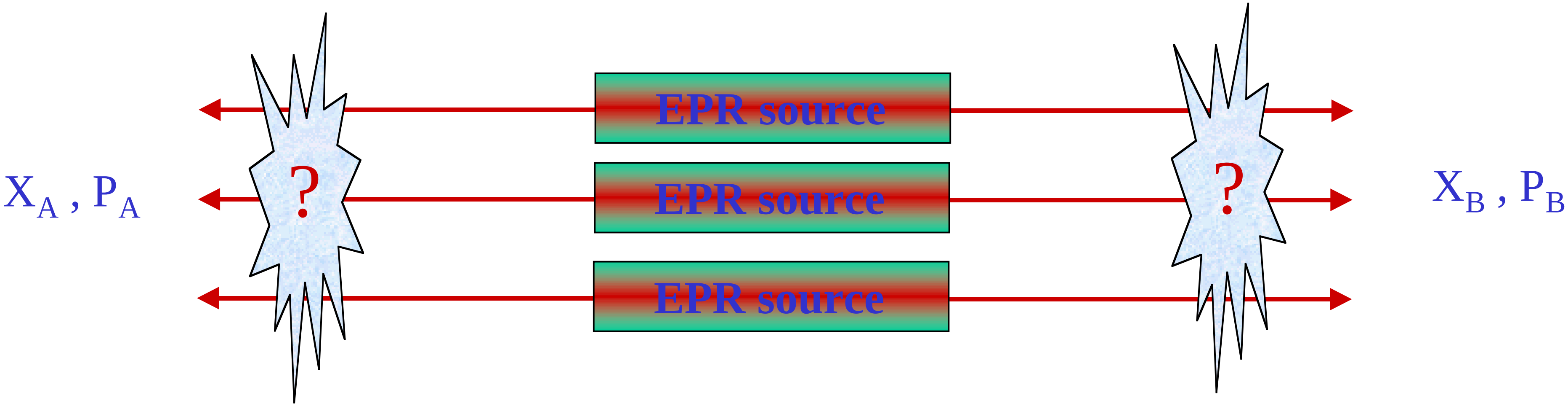
- A « true » EPR protocol is more robust with respect to excess noise than a coherent state protocol (but the bit rates are the same if no excess noise).

* Fundamental advantage of « actual » EPR beams vs. coherent states ?

Entanglement distillation procedures and quantum repeaters !

Quantum repeaters and non-gaussian states

QIPC



Is it possible to carry some operation on several EPR beams
to increase the final entanglement ?

Theorem (Eisert, Cirac…):
This cannot be done if all states and all operations are gaussian !
« Degaussification » is required

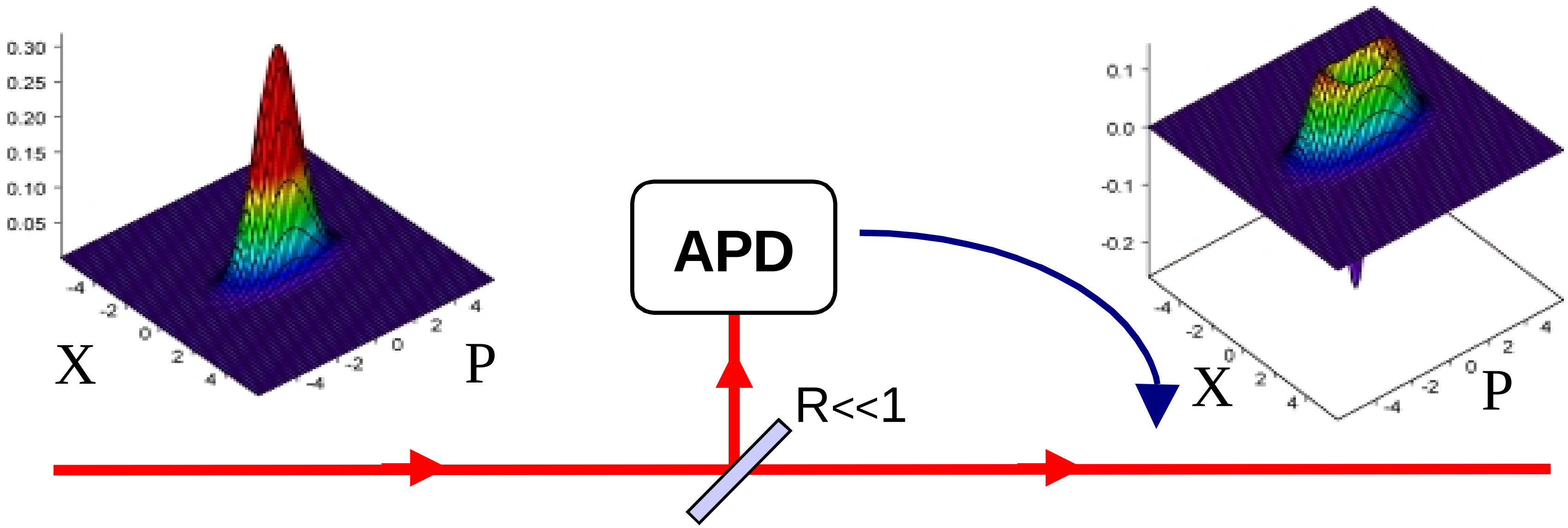
How to get a simple non-gaussian processing ?

« Degaussification » of a squeezed state

Naive view : degaussification = photon substraction
(one single photon in the APD beam)

Wigner function

Wigner function



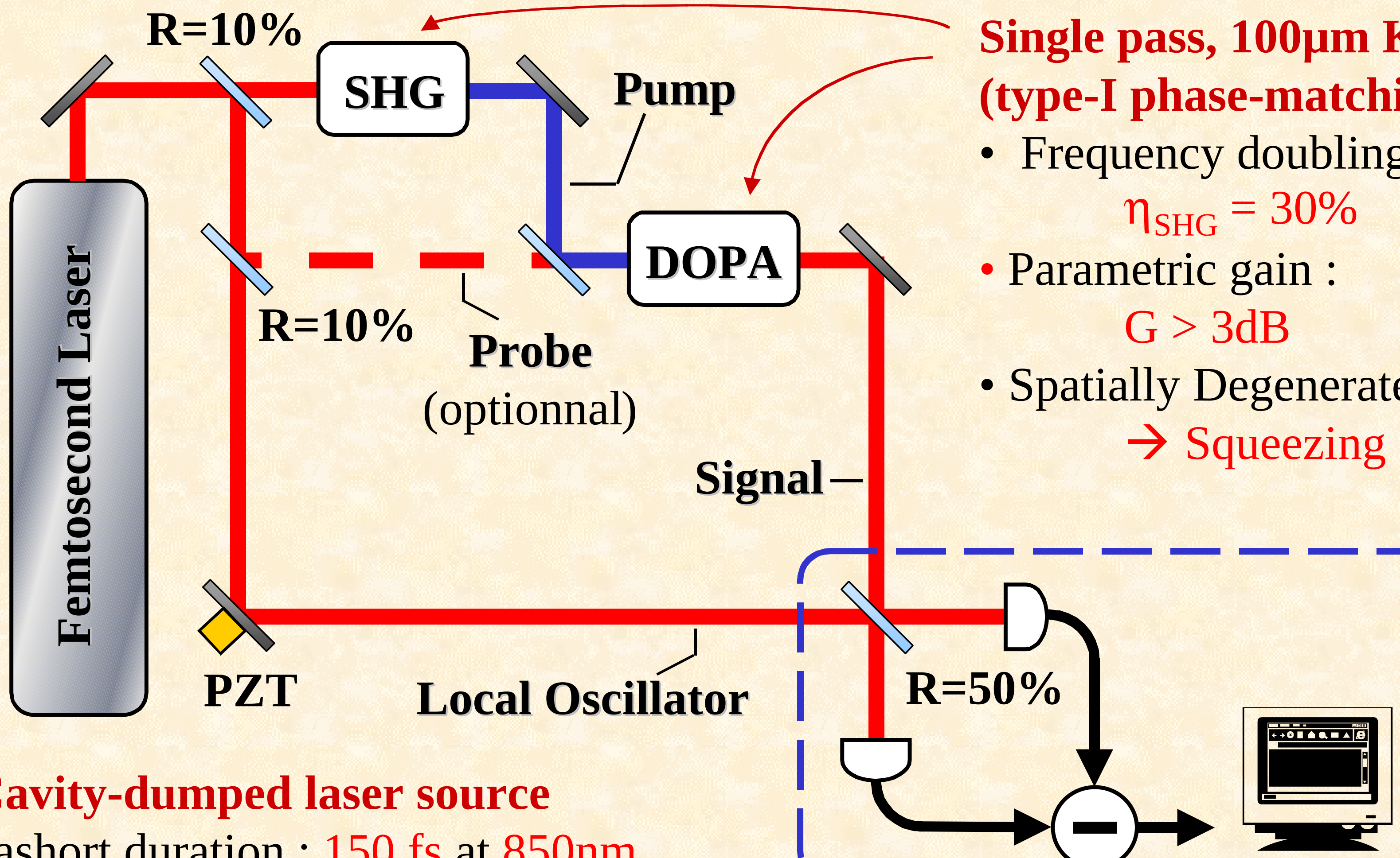
Squeezed vacuum :
$\alpha |0\rangle + \beta |2\rangle + \gamma |4\rangle + \ldots$

Non-gaussian state :
$\beta|1\rangle + \sqrt{2}\,\gamma\,(1-R)\,|3\rangle + \ldots$

Experimental set-up

Jérôme Wenger et al.

QIPC



Single pass, 100µm $KNbO_3$ (type-I phase-matching)

- Frequency doubling : $\eta_{SHG} = 30\%$
- Parametric gain : G > 3dB
- Spatially Degenerated → Squeezing

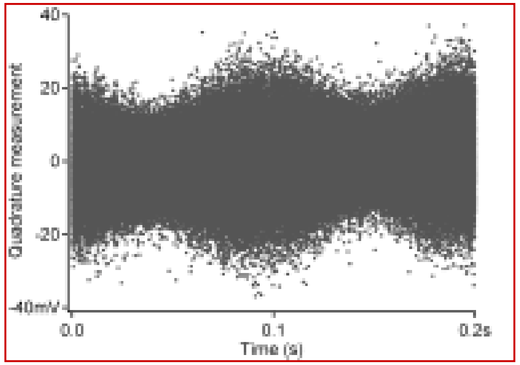
Cavity-dumped laser source

- Ultrashort duration : 150 fs at 850nm
  - Nearly Fourier-Transform limited
- High energy : 75nJ / pulse @ 790kHz

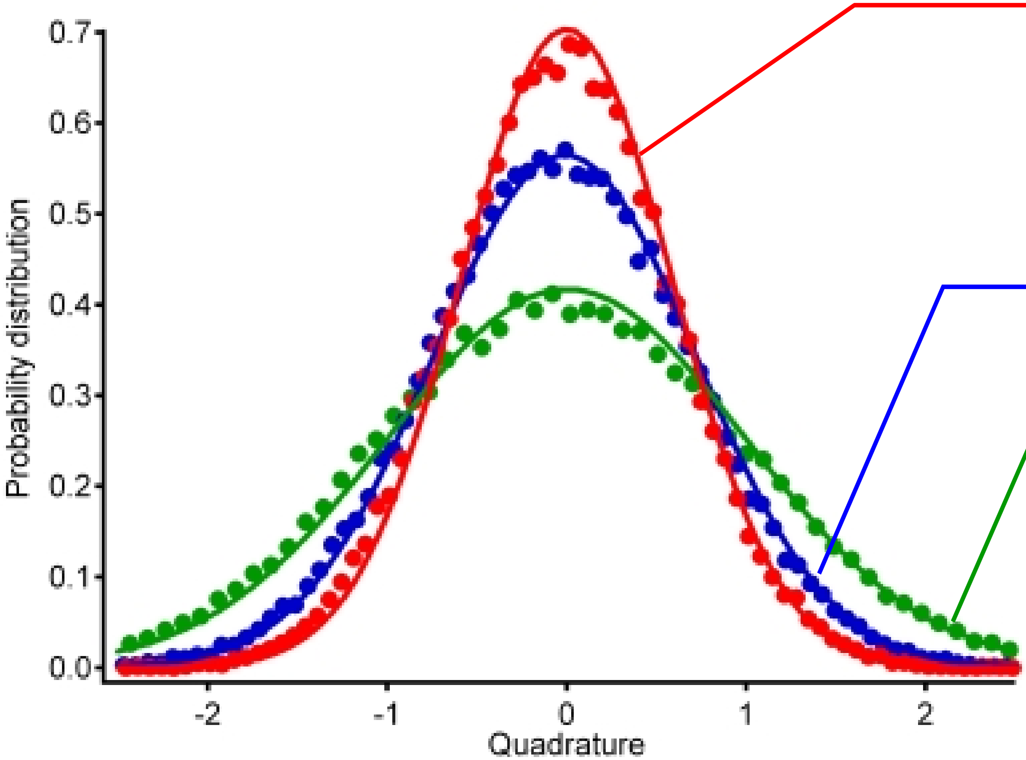
Pulsed Homodyne Detection

Time-domain, overall efficiency : 75%

Pulsed Squeezed State Characterization



Time-domain analysis
Scan of the LO phase

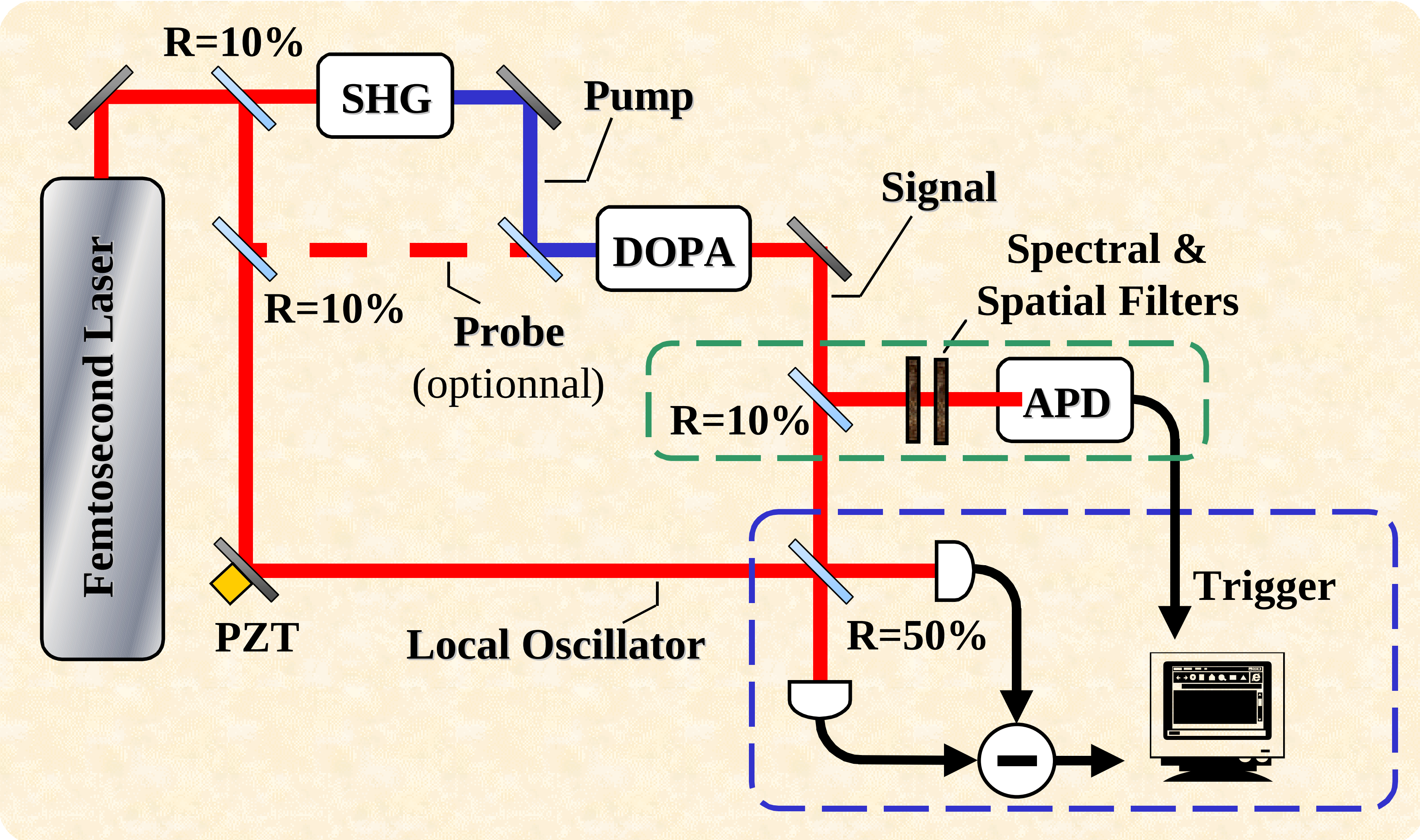


Squeezed quadrature
-1.9dB below SNL (no correction)
[-2.7dB corrected for losses]

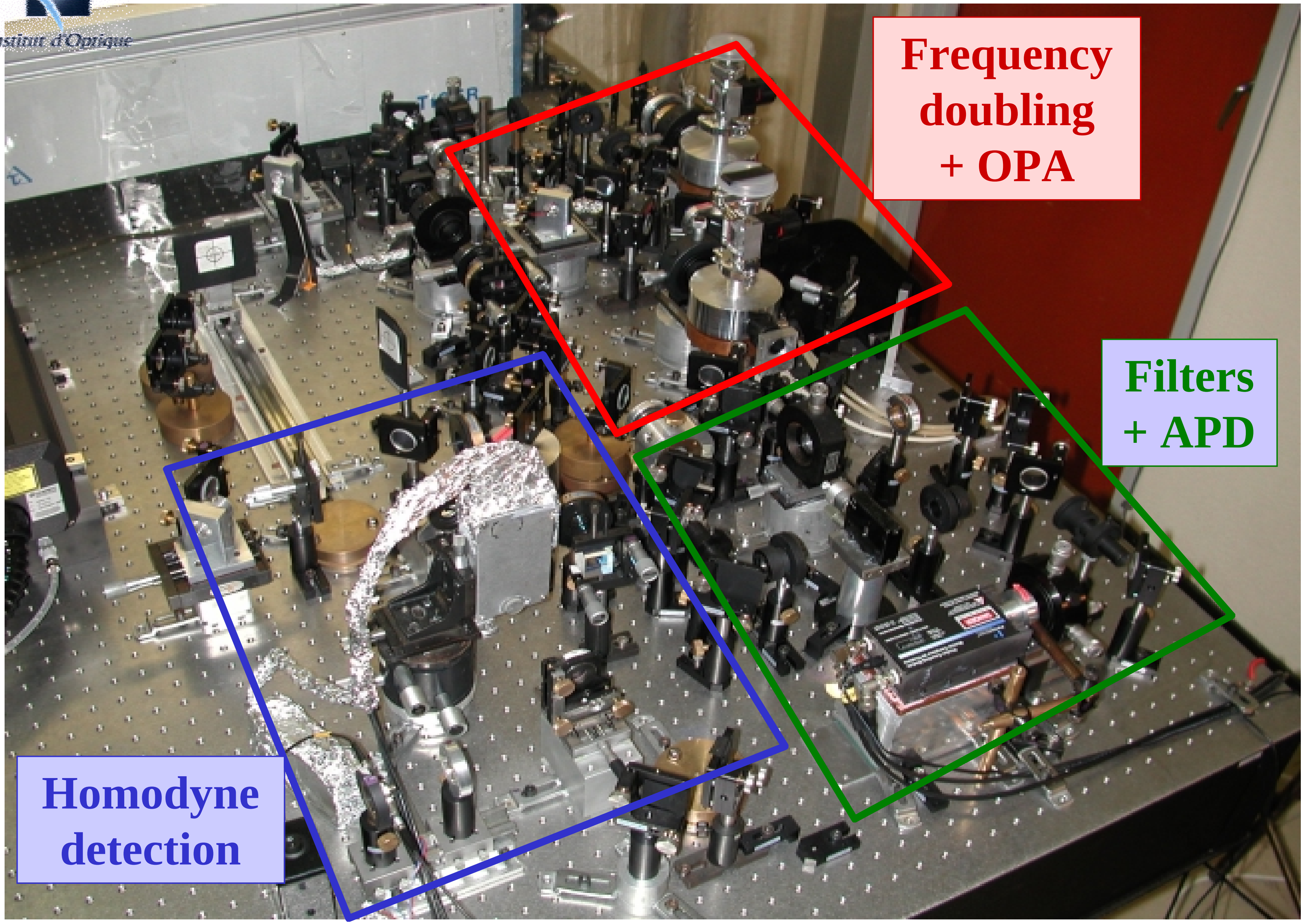
Shot Noise Level (SNL)

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

Experimental set-up



Experimental set-up

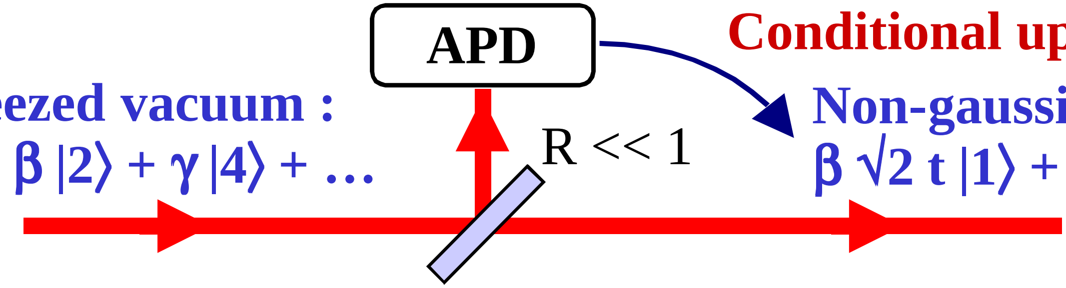


Observed non-gaussian statistics

QIPC

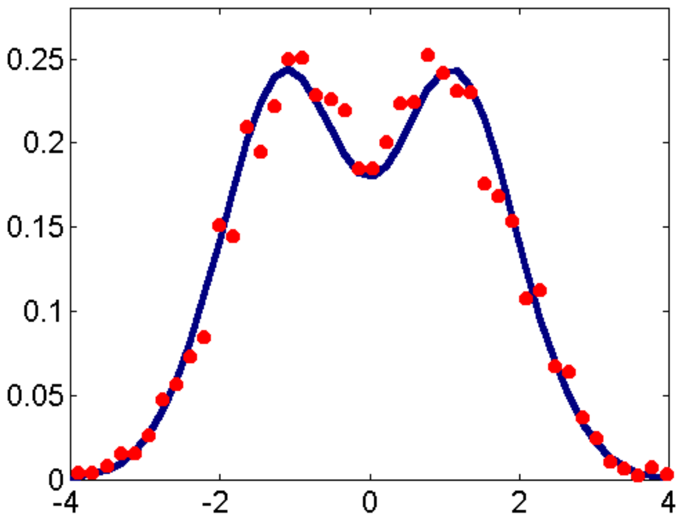
Conditional upon a click :

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

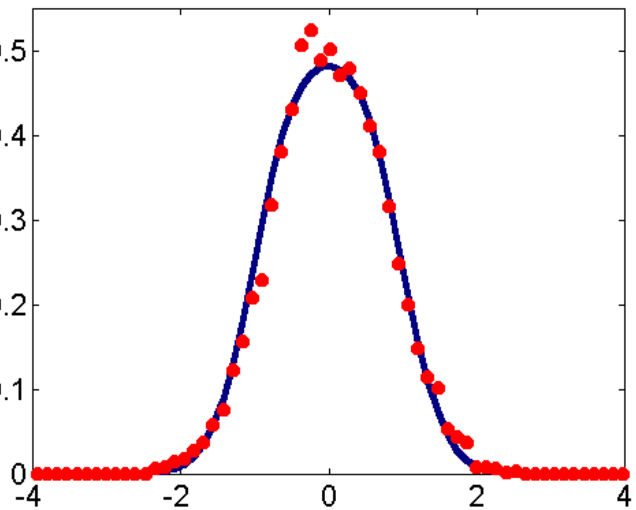


Non-gaussian state :
$\beta\,\sqrt{2}\,t\,|1\rangle + \;2\,\gamma\,t^3\,|3\rangle + \ldots$

➢ **High order terms ➔ Phase-dependent statistics**



Amplified quadrature

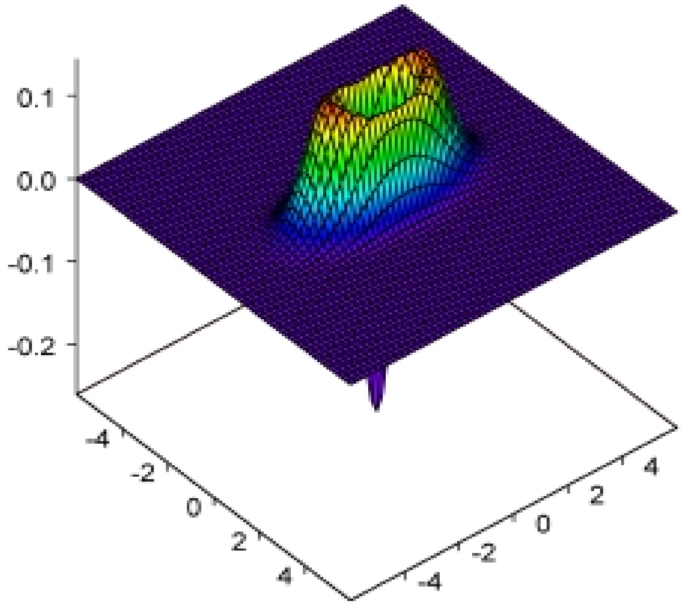


Squeezed quadrature

Wigner function of the conditioned state

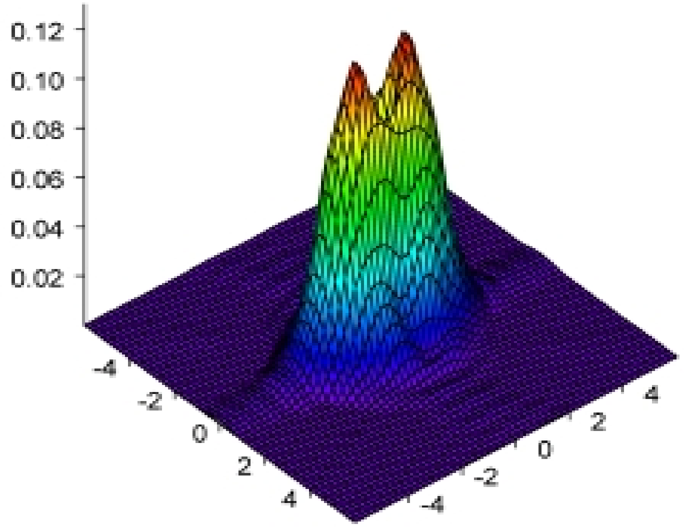
QIPC

➢ **Quantum tomography ➔ Wigner function reconstruction**



Theory : perfect detection

$W_{th}(0,0) = -0.26$



Experimental data, no correction

$W_{exp}(0,0) = 0.067$

Use of degaussification

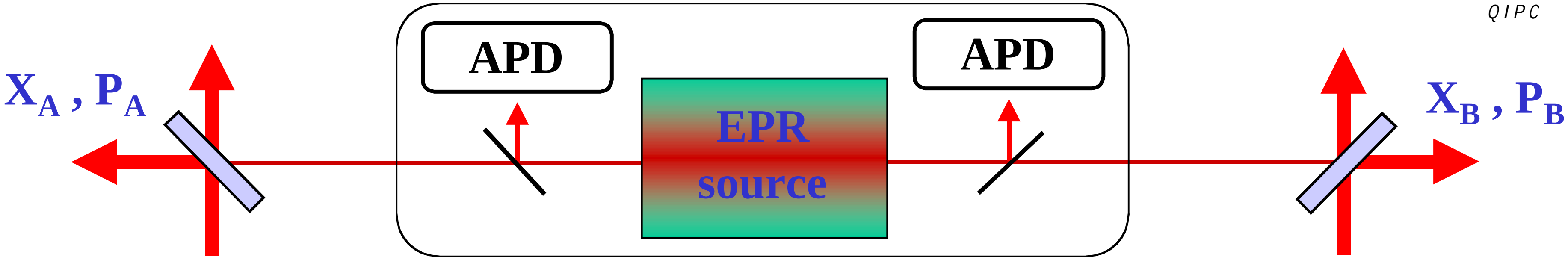
Degaussification should improve entanglement...

Can this be proven on a simple example ?

Look at Bell 's inequalities as a criterion !

A new violation of Bell 's inequalities ?

R. Garcia-Patron et al, Phys. Rev. Lett. **93**, 130409 (2004)



$(X_A + X_B)$ and $(P_A - P_B)$ are squeezed : original EPR state (1935) !

* Perform homodyne detections (XX'- XP'- PX'- PP') on each side
* « Digitize » the data by taking the sign (±) of the value of X or P
* Then compute the S parameter for Bell 's inequalities ($|S| \leq 2$)

No violation ! (the Wigner function provides a local hidden variable model !)

*** Now « degaussify » by using two APDs (« event ready » detectors)**

Violation ! $S = 2.02 > 2$ [6 dB squeezing, η(APD) = 30%, η(hom) = 95%]

« Loophole -free » test, all events are taken into account, feasible ?

Conclusion

QIPC

Security proof of coherent state QKD :

* Coherent states protocols using reverse reconciliation are secure against any (gaussian or non-gaussian) finite-size attack
* Unconditional security of these protocols has also been (almost) proven.

Coherent states QKD demonstrator : Nature **421**, 238 (2003)

* Measured secure bit transmission rates : 1.7 Mbit/sec @ 0 dB loss; 75 kbit/sec @ 3.1 dB loss
* Competitive against faint pulses ? Test @ 1550 nm under way

Conditional preparation of « squeezed » non-gaussian pulses (PRL 2004)

* Phase-dependant non-gaussian Wigner function (« squeezed volcano »)
* First step towards : entanglement distillation procedures ? new tests of Bell’s inequalities ?