Quantum cloning and key distribution with continuous variables of light

Nicolas Cerf

Centre for Quantum Information and Communication

Université Libre de Bruxelles

“Franco-Belgian” collaboration

Centre for Quantum Information and Communication
Ecole Polytechnique, Université Libre de Bruxelles

Nicolas Cerf, Jaromir Fiurasek, Raul Garcia-Patron, Evgueni Karpov, Sofyan Iblisdir, Julien Niset, Gilles Van Assche

Laboratoire Charles Fabry de l’Institut d’Optique, CNRS, Orsay

Rosa Brouri, Philippe Grangier, Frédéric Grosshans, Jerôme Lodewick, Alexei Ourjoumtsev, Jérôme Wenger

Quantum continuous variables

Thrust: Use, as an information carrier, a physical quantity that has a continuous spectrum instead of a binary spectrum

Focus on optical quantum continuous variables ...

* Quantization of the electromagnetic field:
  - Discrete degree of freedom (polarization of a single photon)
  - Continuous degree of freedom (amplitude of quadrature X or P)

* Advantages :
  - Use of standard telecommunication techniques
  - No need for single-photon sources and/or detectors
  - Prospect for higher data rates and simpler processing tools

* Disadvantages :
  - Vacuum noise (shot noise)
  - Sensitivity to optical losses (limits the achievable range)

Optical continuous variables

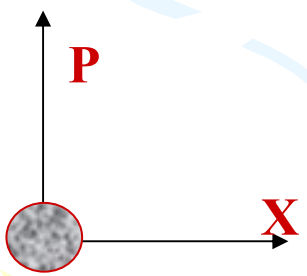
Triggered by the success of continuous-variable quantum teleportation (theoretical concept in 1997, experimental demonstration in 1998)

Light field: $X \cos(\omega t) + P \sin(\omega t)$

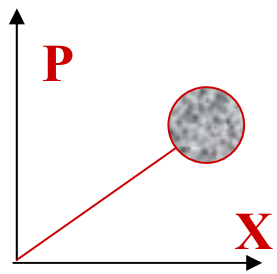
Classical optics: X and P are quadrature components
Quantum optics: X and P are non-commuting variables

$V(X)\, V(P) \geq N_0^2$ (N_0 = shot-noise variance unit)

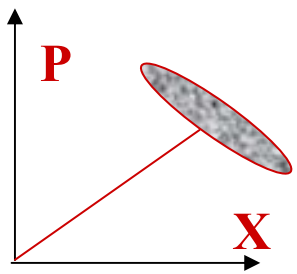
Convenient representation : phase space



Vacuum state

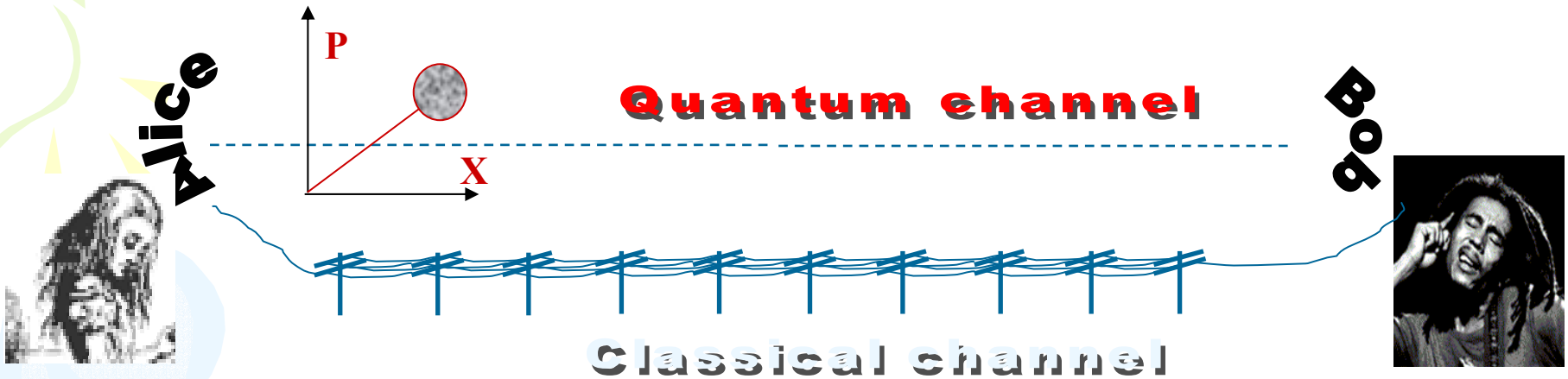


Coherent state



Squeezed state

Continuous-variable quantum key distribution



Principle of quantum key distribution :

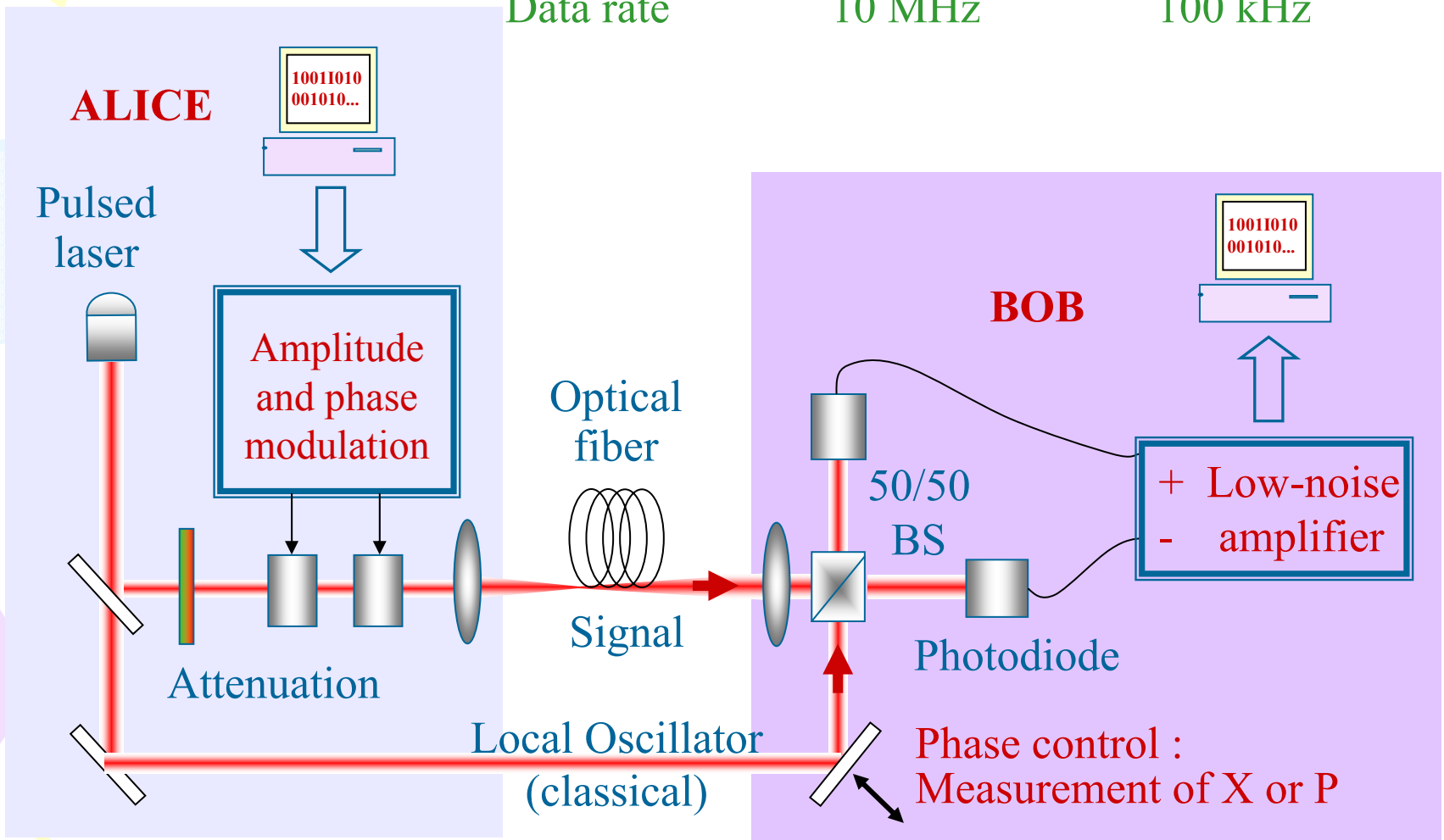
* The eavesdropper (Eve) has unlimited computational power and technological resources; she is only limited by the laws of quantum physics!

Distinct features of our protocol :

* The non-commuting variables are the quadrature components X and P
* The transmitted light made of 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



Quantum cloning w. continuous variables

- Cloning of a pair of canonical continuous variables (x,p)
  - Limits on optimal cloning (minimum noise)
  - Gaussian cloning transformation
  - Optical implementation
- Gaussian cloners with multiple inputs and outputs
  - Bound on the fidelity based on concatenation
- Non-Gaussian cloning of continuous variables
  - General displacement- and rotation-covariant cloner
  - Optical implementation of a non-Gaussian cloner
  - Maximum cloning fidelity for Gaussian states
- Application to continuous-variable QKD

Cloning 2 canonically conjugate variables

(x, p) = two quadrature components of a light mode

$[x, p] = i \Rightarrow x$ and p cannot be both measured perfectly

$\Rightarrow$ states $|x\rangle$ and $|p\rangle$ cannot be cloned perfectly

Look for an optimal *imperfect* cloner...

Symmetric

Covariant with respect to Weyl-Heisenberg displacements

Same error variance for x and p quadrature

Minimize the cloning noise variance

Limits on optimal cloning

Cloning and mesuring x on one clone and p on the other clone cannot beat the optimal joint measurement of x and p.

$$X_1 = x + \tilde{x}_1 \qquad X_2 = x + \tilde{x}_2$$
$$P_1 = p + \tilde{p}_1 \qquad P_2 = p + \tilde{p}_2$$

$$[X_1, P_2] = \underbrace{[x, p]}_{=i} + \underbrace{[x, \tilde{p}_2]}_{=0} + \underbrace{[\tilde{x}_1, p]}_{=0} + [\tilde{x}_1, \tilde{p}_2] = 0$$

$$\Delta\tilde{x}_1 \, \Delta\tilde{p}_2 \geq \tfrac{1}{2} |\langle [\tilde{x}_1, \tilde{p}_2] \rangle| = 1/2$$
$$\Delta\tilde{p}_1 \, \Delta\tilde{x}_2 \geq \tfrac{1}{2} |\langle [\tilde{p}_1, \tilde{x}_2] \rangle| = 1/2$$

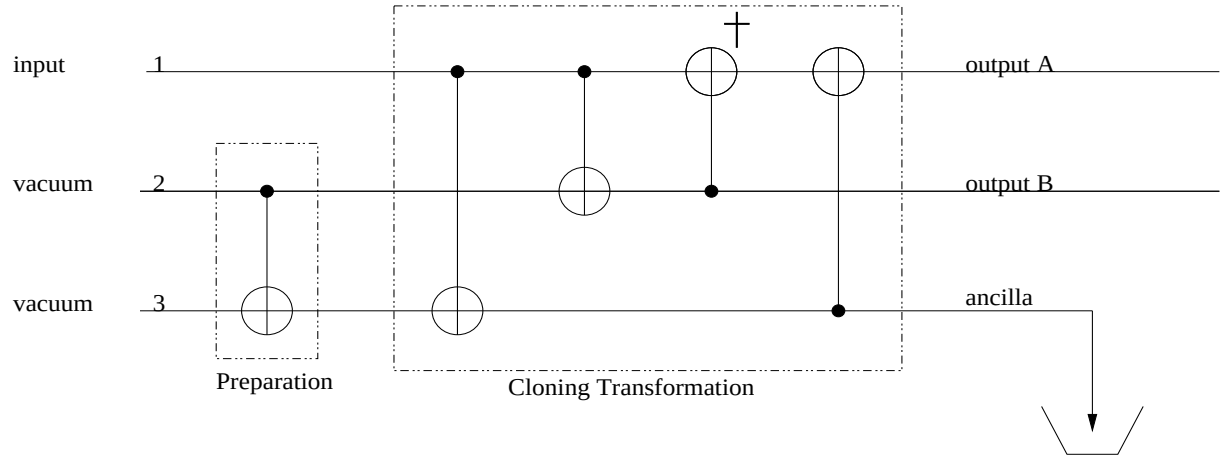
Symmetric Gaussian cloner:

$\Delta\tilde{x}_1^2 = \Delta\tilde{p}_1^2 = \Delta\tilde{x}_2^2 = \Delta\tilde{p}_2^2 = 1/2$ (minimum added noise)

This cloning transformation is

$$\hat{U}_{1,2,3} = e^{-i(\hat{x}_3 - \hat{x}_2)\hat{p}_1} e^{-i\hat{x}_1(\hat{p}_2 + \hat{p}_3)}$$

with $|\psi_{\text{prep}}\rangle = e^{-i\hat{x}_2\hat{p}_3}|0_{\text{vac}}\rangle|0_{\text{vac}}\rangle$



where $\text{C}-\text{NOT}\ |a\rangle\ |b\rangle = |a\rangle\ |a+b\rangle$.

Transformation in Schrödinger picture:

$$|0_{\text{vac}}\rangle = \frac{1}{\pi^{1/4}} \int dz\ e^{-z^2/2}\ |z\rangle$$

$$|\psi_{\text{prep}}\rangle = \frac{1}{\sqrt{\pi}} \int dy\ dz\ e^{-(y^2+z^2)/2}\ |z\rangle\ |y+z\rangle$$

$$|x\rangle|\psi_{\text{prep}}\rangle \longrightarrow \frac{1}{\sqrt{\pi}} \int dy\ dz\ e^{-(y^2+z^2)/2} \times |x+y\rangle\ |x+z\rangle\ |x+y+z\rangle$$

This machine effects Gaussian-distributed x-errors and p-errors on the input state $|\psi\rangle$:

$$\rho_{A,B} = \frac{1}{\pi}\int dx\ dp\ e^{-(x^2+p^2)}\ \hat{D}(x,p)|\psi\rangle\langle\psi|\hat{D}^\dagger(x,p)$$

with $\hat{D}(x,p) = e^{-ix\hat{p}}e^{ip\hat{x}}$ displacement operator

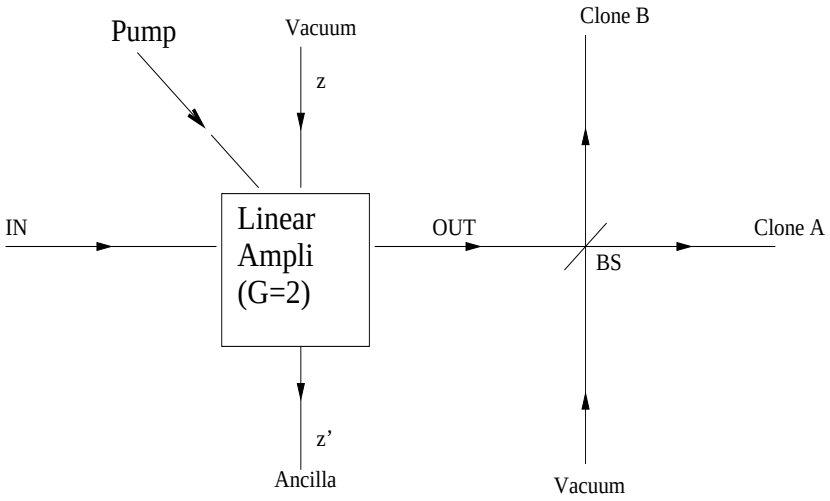
The error variances in x and p are the same:

$$\sigma^2 = 1/2 \qquad (optimal\ Gaussian\ cloner)$$

The fidelity when cloning a coherent state $|\alpha\rangle$ is calculated by using $\langle\alpha|\alpha+\beta\rangle = e^{-|\beta|^2}$

$$\begin{aligned} f &= \langle\alpha|\rho_{A,B}|\alpha\rangle \\ &= \frac{2}{\pi}\int d^2\beta\ e^{-2|\beta|^2}|\langle\alpha|\alpha+\beta\rangle|^2 \\ &= \frac{1}{1+\sigma^2} \\ &= 2/3 \end{aligned}$$

Optical implementation



N.B. Cloning-induced noise originates from vacuum fluctuations of the ancilla modes

$$\hat{a}_{\mathsf{out}} = \sqrt{2}\,\hat{a}_{\mathsf{in}} + \hat{a}_z^\dagger$$
$$\hat{a}_{z'} = \sqrt{2}\,\hat{a}_z + \hat{a}_{\mathsf{in}}^\dagger$$

$$\hat{a}_A = (\hat{a}_{\mathsf{out}} + \hat{a}_{\mathsf{vac}})/\sqrt{2} = \hat{a}_{\mathsf{in}} + (\hat{a}_z^\dagger + \hat{a}_{\mathsf{vac}})/\sqrt{2}$$
$$\hat{a}_B = (\hat{a}_{\mathsf{out}} - \hat{a}_{\mathsf{vac}})/\sqrt{2} = \hat{a}_{\mathsf{in}} + (\hat{a}_z^\dagger - \hat{a}_{\mathsf{vac}})/\sqrt{2}$$

$$\langle \hat{a}_A \rangle = \langle \hat{a}_B \rangle = \langle \hat{a}_{\mathsf{in}} \rangle$$
$$\langle \hat{a}_{z'} \rangle = \langle \hat{a}_{\mathsf{in}} \rangle^*$$

$$\Delta x_A{}^2 = \Delta p_A{}^2 = \Delta x_B{}^2 = \Delta p_B{}^2 = \tfrac{1}{2} + \tfrac{1}{2}$$
$$\Delta x_{z'}{}^2 = \Delta p_{z'}{}^2 = \tfrac{1}{2} + 1$$

Gaussian cloner with multiple in/outputs

Cloner which produces M approximate clones with the same Gaussian-distributed errors in x and p when provided with N replicas of $|\psi\rangle$.

The minimum error variance is

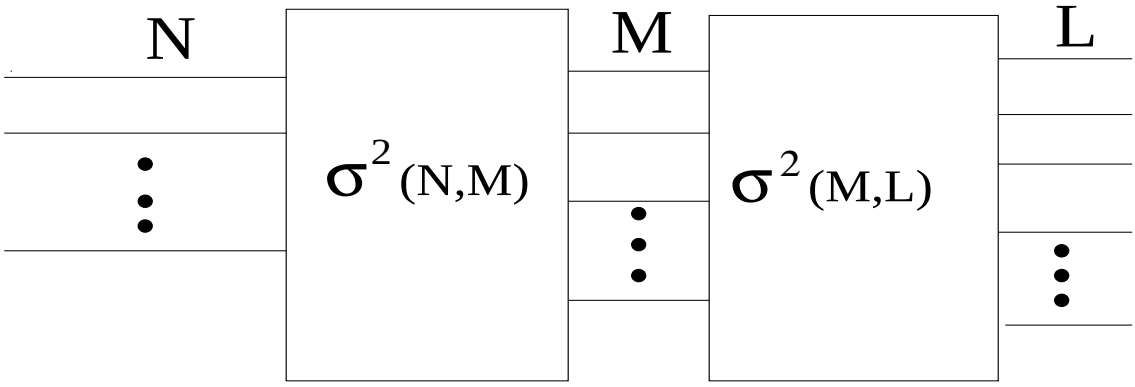
$$\sigma^2(N, M) = \frac{1}{N} - \frac{1}{M}$$

The cloning fidelity for coherent states is

$$f_{N,M} = \frac{MN}{MN + M - N}$$

N	M	$f_{N,M}$
1	2	2/3
1	3	3/5
1	∞	1/2
N	N	1
N	$2N$	$2N/(2N+1)$
N	∞	$N/(N+1)$

Proof: Consider two concatenated cloners



We have $\sigma^2(N,L) = \sigma^2(N,M) + \sigma^2(M,L)$.

For $L = \infty$ and considering optimal cloners

$$\underbrace{\sigma^2_{opt}(N,\infty)}_{1/N} \leq \sigma^2(N,M) + \underbrace{\sigma^2_{opt}(M,\infty)}_{1/M}$$

$$\Rightarrow \quad \sigma^2(N,M) \geq 1/N - 1/M$$

This bound is saturated by the Gaussian cloner

High-rate continuous-variable QKD

using Gaussian-modulated coherent light pulses

Nicolas J. Cerf, Gilles Van Assche

Université Libre de Bruxelles, Brussels, Belgium

Rosa Brouri, Philippe Grangier, Frédéric Grosshans, Jérôme Wenger

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

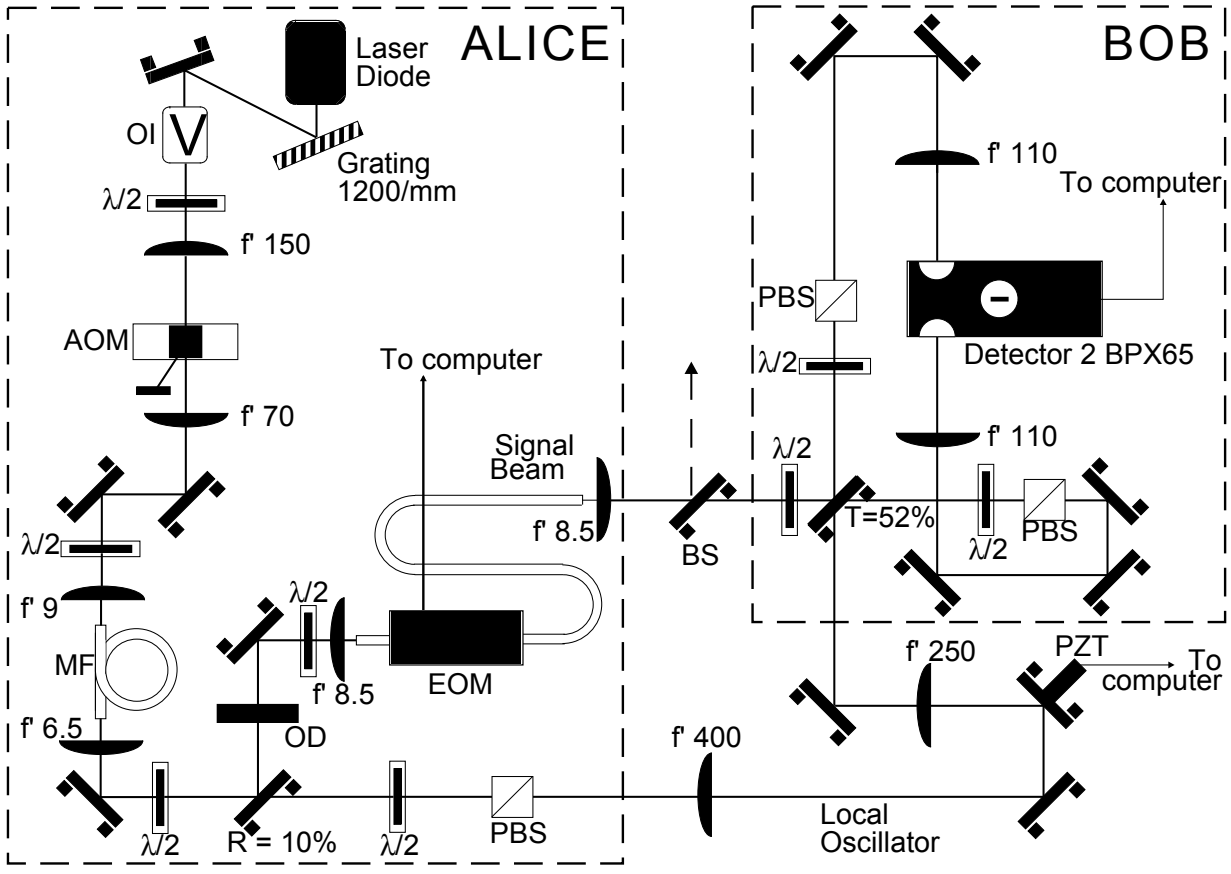
Some “key” ideas

- Key encoded in e-m field amplitudes (x or p quadrature)
  $\Rightarrow$ “gaussian key elements”
- Coherent light pulses (non-orthogonal states)
  $\Rightarrow$ no need for squeezing
- Continuous raw data converted into a usable binary key
  $\Rightarrow$ “sliced” reconciliation algorithm
- Reverse reconciliation (Bob’s data serve as the key)
  $\Rightarrow$ no limit on the attainable quantum channel loss

QUANTUM PROTOCOL IS FULLY CONTINUOUS

CLASSICAL POST-PROCESSING IS DISCRETE

Tested experimental setup



Laser diode: SDL 5412 (780nm); OI: optical isolator; AOM: acousto-optic modulator; MF: polarization maintaining fiber; OD: optical density; EOM: electro-optic amplitude modulator; PBS: polarizing beam splitter; BS: beam splitter; PZT: piezoelectric transducer

Protocol

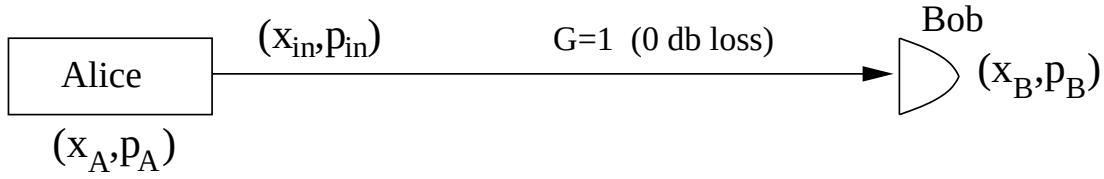
— QUANTUM —

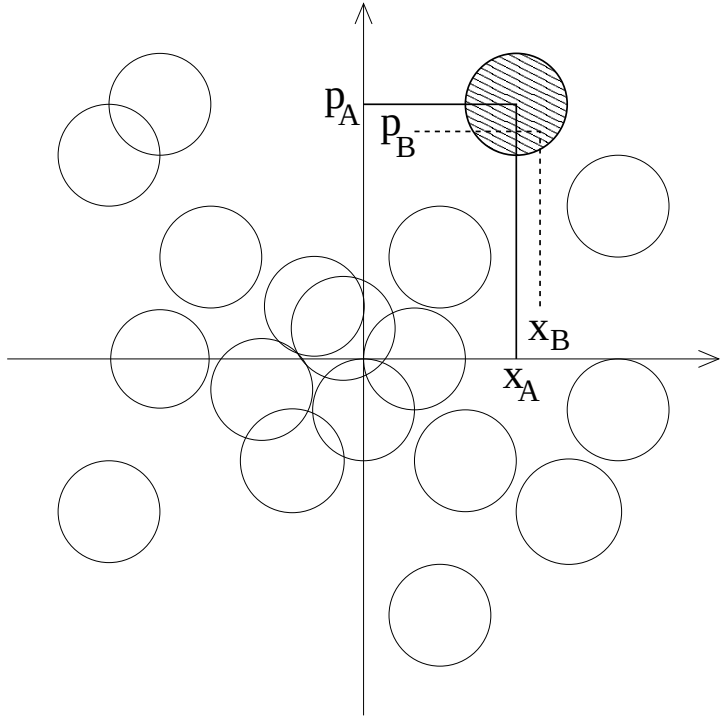
1. Alice sends $|x_A + ip_A\rangle$ with random x_A, $p_A \sim \mathcal{N}(0, V_A)$
2. Bob randomly measures either x_B or p_B
3. Bob discloses x/p bit, so Alice keeps good quadrature

— CLASSICAL —

4. Alice & Bob estimate channel loss and added noise
5. Alice & Bob reconciliate their gaussian data
   - DIRECT RECONCILIATION (DR)*: Alice sends extra bits to Bob for him to correct transmission errors*
   - REVERSE RECONCILIATION (RR)*: Bob sends extra bits to Alice for her to incorporate transmission errors*
6. Alice & Bob apply privacy amplification to wipe out Eve's estimated information about Alice (DR) or Bob (RR)

Protocol (continued)



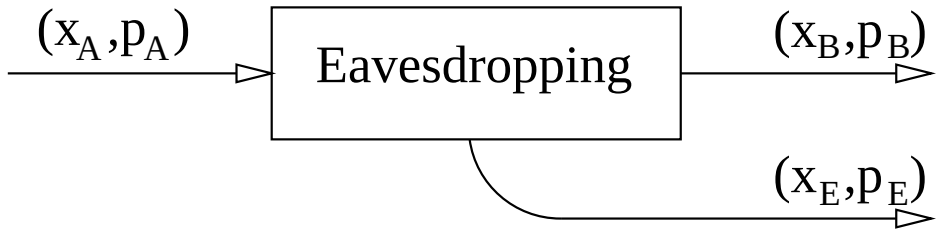


$$x_{in} = x_A + x_{vac}$$
$$p_{in} = p_A + p_{vac}$$

$$x_B = \sqrt{G}\,(x_{in} + \delta x) \qquad \text{with} \quad \langle \delta x^2 \rangle = \chi N_0$$
$$p_B = \sqrt{G}\,(p_{in} + \delta p) \qquad \text{with} \quad \langle \delta p^2 \rangle = \chi N_0$$

(G=channel gain, χ= equivalent input noise, N_0 = shot-noise variance)

Heisenberg-limited eavesdropping



Alice and Eve cannot jointly know more about (x_B, p_B) than allowed by the Heisenberg principle:

$$V(x_B|x_A)\,V(p_B|p_E) \geq N_0^2 \qquad V(p_B|p_A)\,V(x_B|x_E) \geq N_0^2$$

(N_0 = shot-noise variance)

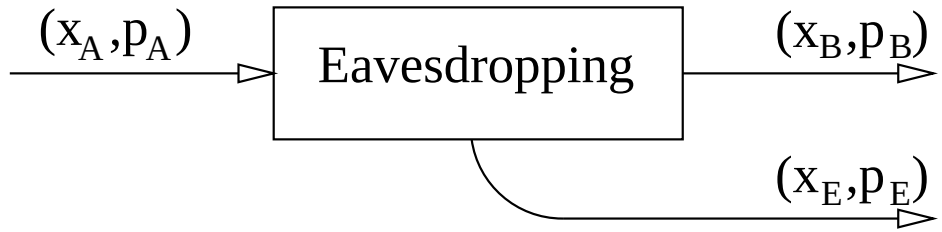
The channel parameters define the conditional variances:

$$x_B = \sqrt{G}\,(x_A + x_{vac} + \delta x) \qquad p_B = \sqrt{G}\,(p_A + p_{vac} + \delta p)$$

$$V^{\mathrm{coh}}(x_B|x_A) = G(\chi+1)N_0 \qquad V^{\mathrm{coh}}(p_B|p_A) = G(\chi+1)N_0$$

(G=channel gain, χ= equivalent input noise, N_0 = shot-noise variance)

Virtual entanglement limit



The Heisenberg relation holds regardless the way Alice prepares her ensemble (gaussian mixture of coherent states $\Leftrightarrow$ one of two entangled beams).

The channel parameters imply the limitation:

$$V(x_B|x_A) \geq G(\chi + 1/V)N_0 \qquad V(p_B|p_A) \geq G(\chi + 1/V)N_0$$

($V = 1 + V_A$= Alice's quadrature variance; χ= equivalent input noise)

Resulting bound on Eve's knowledge:

$$V(x_B|x_E) \geq \frac{N_0}{G(\chi+1/V)} \qquad V(p_B|p_E) \geq \frac{N_0}{G(\chi+1/V)}$$

Security analysis (RR)

Restricted to gaussian individual (non-collective) attacks

$$\Delta I \geq \max(\underbrace{I_{AB} - I_{AE}}_{\mathrm{DR}}, \underbrace{I_{BA} - I_{BE}}_{\mathrm{RR}})$$

$$I_{BA} = \frac{1}{2} \log_2 \left(\frac{V_B}{V_{B|A}^{\mathrm{coh}}} \right)$$

$$I_{BE} = \frac{1}{2} \log_2 \left(\frac{V_B}{V_{B|E}^{\mathrm{min}}} \right)$$

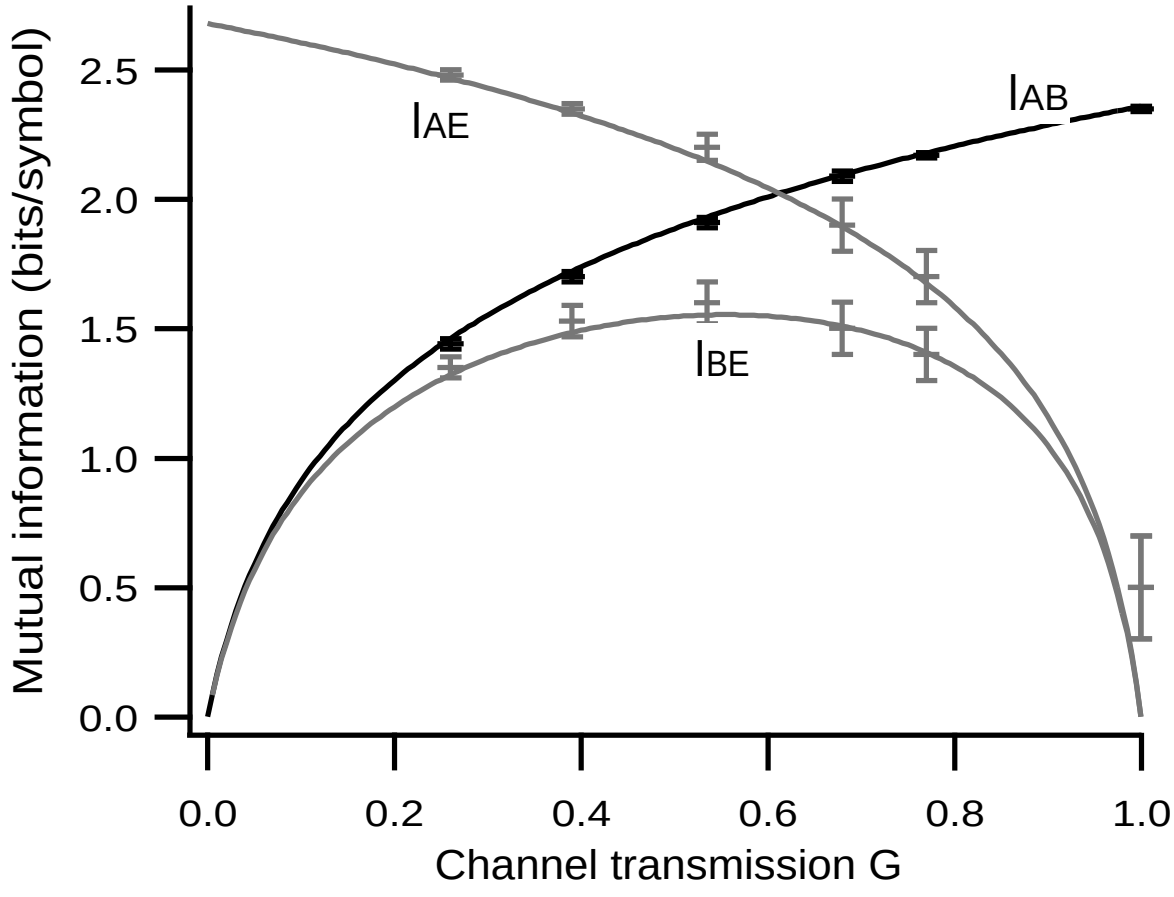
with $V_B = G(V + \chi)N_0 =$ Bob's quadrature variance

$$\Delta I_{\mathrm{RR}} = \frac{1}{2} \log_2 \left(\frac{V_{B|E}^{\mathrm{min}}}{V_{B|A}^{\mathrm{coh}}} \right) = -\frac{1}{2} \log_2 [G^2(\chi + 1)(\chi + 1/V)]$$

with $\chi = \underbrace{(1 - G)/G}_{\text{vacuum noise}} + \epsilon$ ($\epsilon =$ excess noise)

High-loss limit ($G \ll 1$): $\underline{\Delta I_{\mathrm{RR}} > 0}$ if $\epsilon < \frac{V-1}{2V} \simeq 1/2$

Information curves



◇ THE RECONCILIATION DOES NOT REACH SHANNON'S LIMIT, BUT HAS AN EFFICIENCY IN THE 70-90 % RANGE $\longrightarrow$ BOUND ON ATTAINABLE G

Practical net key rates

G	I_{AB} (bits/symbol)	RR key rate (kbps)	DR key rate (kbps)
1.00 (0 dB)	2.4	1,690 [1,920]	1,660 [1,910]
0.79 (1.0 dB)	2.2	470 [730]	270 [540]
0.68 (1.7 dB)	1.9	185 [510]	— [190]
0.49 (3.1 dB)	1.7	75 [370]	— [0]
0.26 (5.9 dB)	1.5	— [85]	— [0]

[ ] $\equiv$ IDEAL SECRET KEY RATES (ASSUMING PERFECT RECONCILIATION)

REPETITION RATE $\simeq$ 800 kHz (120 ns PULSES)

MODULATION VARIANCE $\simeq$ 30-40 $\times$ SHOT-NOISE VARIANCE

Advantage over conventional QKD

- No single-photon source needed ($\sim$ 100 photons/pulse)
- Fast homodyne detection (repetition rate $\sim$ 10 MHz)
  - *Repetition rate of single-photon detectors $\sim$ 100 kHz*
- High-dimensionality of the phase space
  - *Amplitude/phase modulation with large dynamics so that several key bits are encoded per coherent pulse*
- High secret key bit rates
  - *Practical rates $\sim 10^2 - 10^3$ kbps for low losses ($\sim$3 dB) that is, for a moderate range (~ 15 km)*

SECURE REGARDLESS THE LINE LOSS (IN PRINCIPLE!)

Eve controls Bob's errors not as well as she reads Alice's modulation

$\rightarrow$ *reverse reconciliation is better for lossy channels*

References

- F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and Ph. Grangier, Nature **421**, 239 (16 January 2003).

QUANTUM OPTICAL ASPECTS:

- F. Grosshans and Ph. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
- N. J. Cerf, M. Lévy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).

CLASSICAL PROCESSING ASPECTS:

- G. Van Assche, J. Cardinal, and N. J. Cerf, to appear in IEEE Trans. Inform. Theory, arXiv cs.CR/0107030

SECURITY ASPECTS: . . . . .