Secure Communications with Quantum Continuous Variables

Philippe Grangier

Laboratoire Charles Fabry, Institut d'Optique, CNRS,

Université Paris Saclay, 91127 Palaiseau

Collaborations with Sorbonne Université (LIP6), INRIA,

Nokia Bell Labs, exail, THALES

Content of the Talk

Part 1 - Light is quantum ! and propagates far away

1.1 Discrete and continuous quantum descriptions of light

1.2 A nice tool : the Wigner function

Part 2 - Quantum Key Distribution : DV and CV

2.1 Alice, Bob, and Eve

2.2 Experimental implementations of CVQKD

Part 3 - Towards quantum networks

3.1 Overcoming channel losses : trusted nodes, satellites, repeaters

3.2 Looking to the future : deterministic photon-photon interactions

Quantum description of light

Discrete  Photons

Continuous  Wave

A single "mode" of the

quantized electromagnetic field

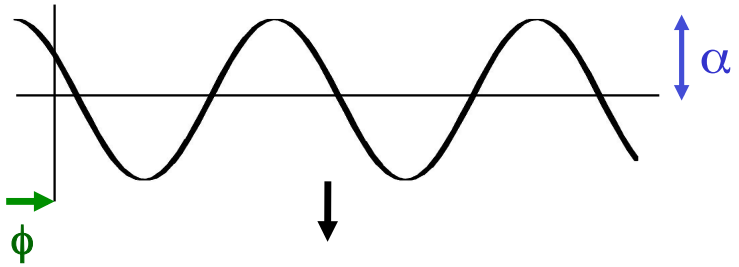
(a plane wave, or a "Fourier transform limited" pulse) is described as a

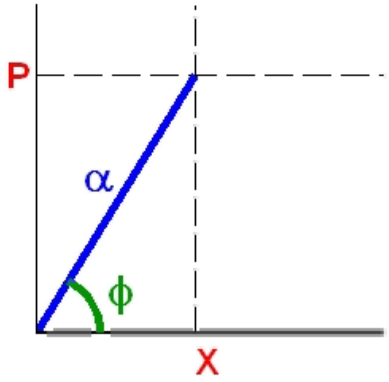
quantized harmonic oscillator :

operators a, a^+, N = a^+ a, etc...

Quantum description of light

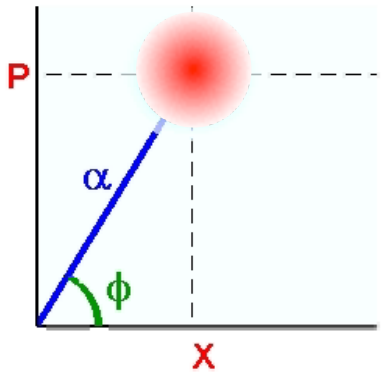
	Discrete Photons	Continuous Wave
Parameters :	Number of photons n Destruction operators a Creation operators a^+ Number operator $N = a^+a$	Amplitude & Phase (polar) Quadratures X & P (cartesian)



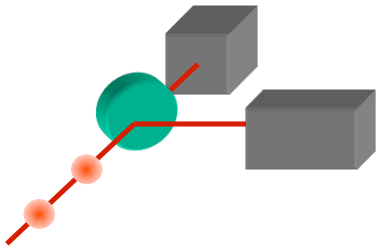
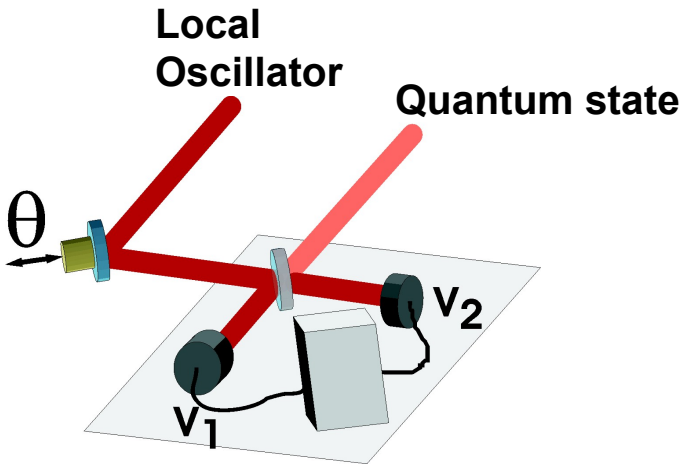


$X = (a + a^+)/\sqrt{2}$
$P = (a - a^+)/i\sqrt{2}$
$[X, P] = i$

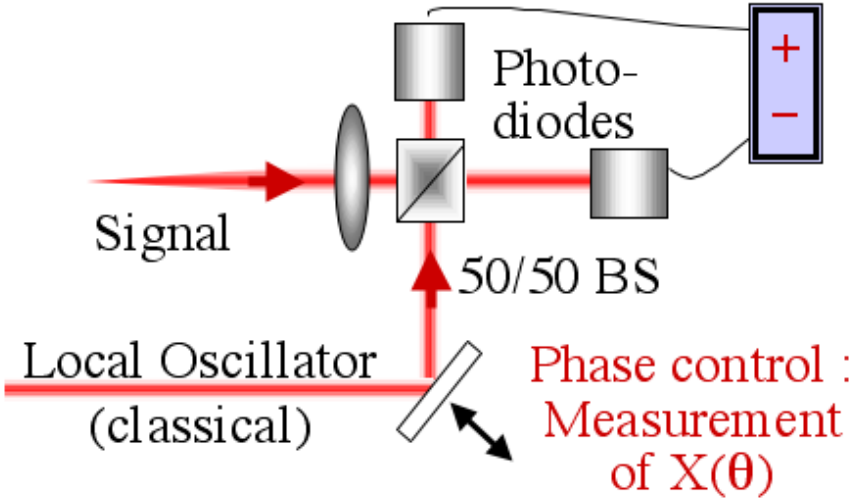
Quantum description of light

	Discrete Photons	Continuous Wave
Parameters :	**Number & Coherence**	**Amplitude & Phase (polar)** **Quadratures X & P (cartesian)**
Representation:	**Density matrix** $\rho = \begin{bmatrix} \rho_{0,0} & \rho_{0,1} & \rho_{0,2} & \cdots \\ \rho_{1,0} & \rho_{1,1} & \rho_{1,2} & \cdots \\ \rho_{2,0} & \rho_{2,1} & \rho_{2,2} & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{bmatrix}$ **Coherences** $< n \mid \rho \mid m >$	**Wigner function W(X,P)**  $X = (a + a^{+})/\sqrt{2}$ $P = (a - a^{+})/i\sqrt{2}$ $[X, P] = i$ **Heisenberg :** $\Delta X . \Delta P \geq 1/2$ ~~**measurement of both X and P**~~ **measurement of** $X_\theta = X \cos\theta + P \sin\theta$

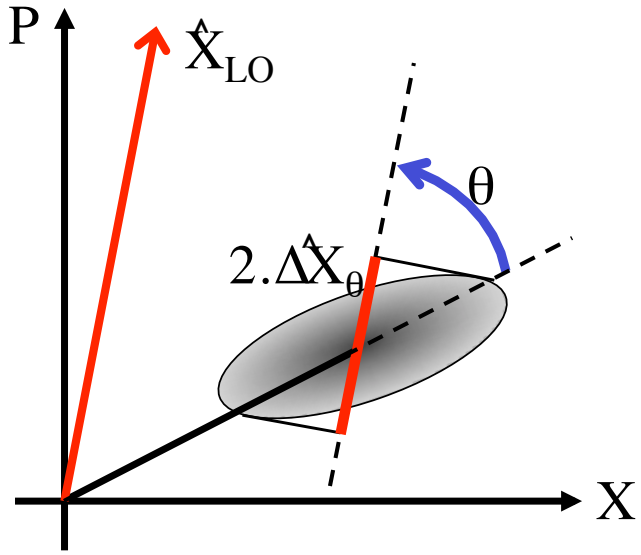
Quantum description of light

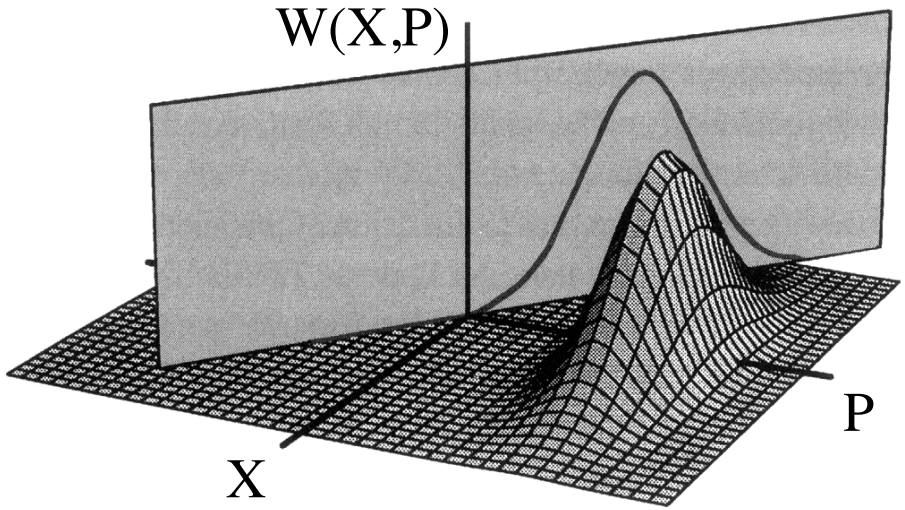
	Discrete  Photons	Continuous  Wave
Parameters :	Number & Coherence	Amplitude & Phase (polar) Quadratures X & P (cartesian)
Representation:	Density matrix	Wigner function W(X,P)
Measurement :	Counting : APD, VLPC, TES... 	Demodulation : Homodyne detection  Interference, then subtraction of photocurrents : $V_1 - V_2 \propto E_{OL}E_{EQ}(\theta)$ $\propto X_\theta = X\cos\theta + P\sin\theta$

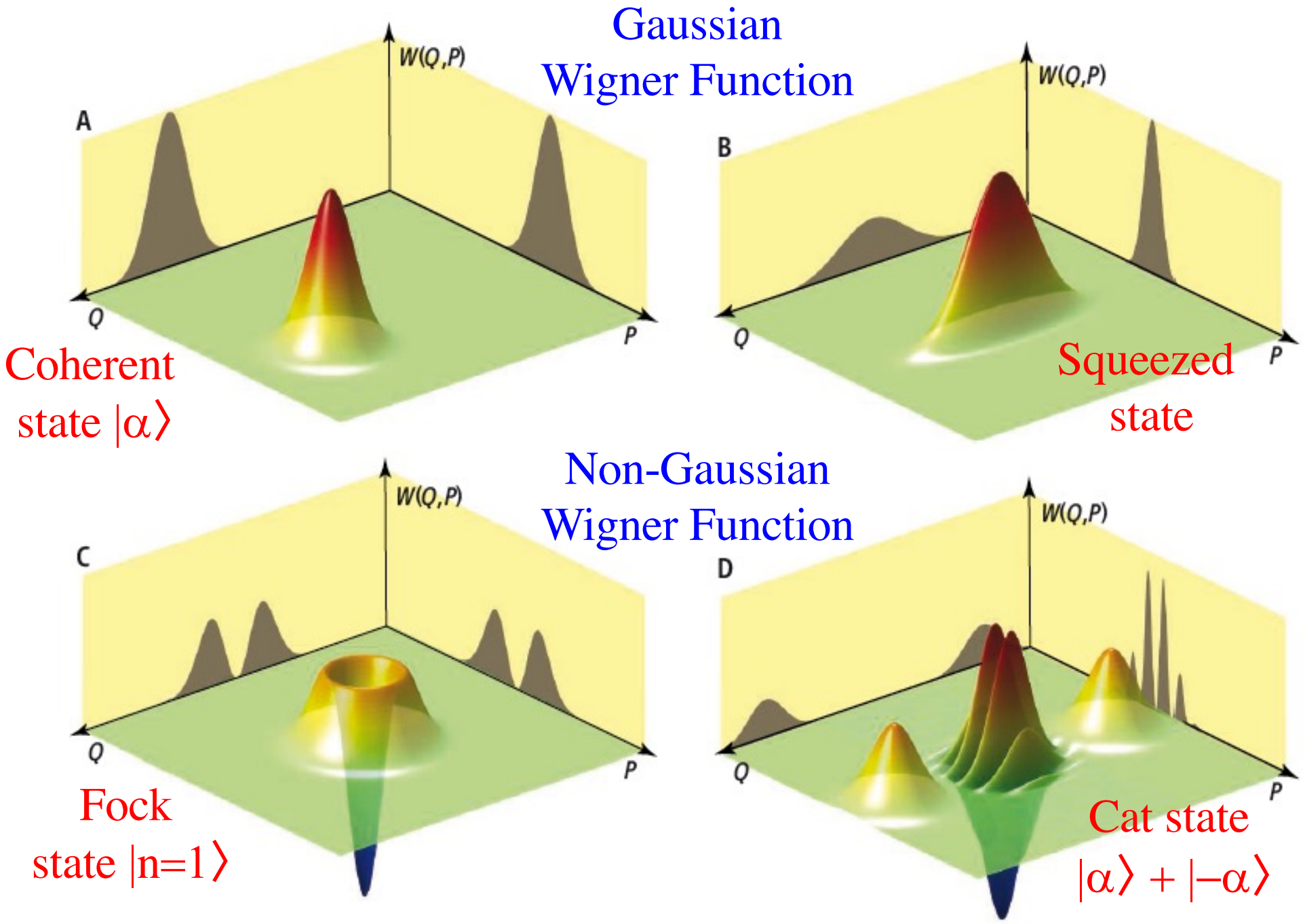
Homodyne detection, Wigner Function and Quantum Tomography



- **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)



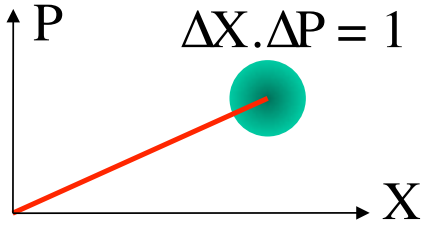




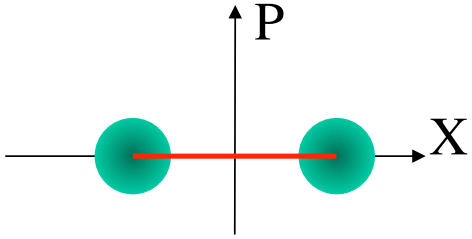
P. Grangier, "Make It Quantum and Continuous", Science (Perspective) 332, 313 (2011)

« Schrödinger's Cat » state

- Classical object in a quantum superposition of distinguishable states
- "Quasi - classical" state in quantum optics : coherent state $|\alpha\rangle$



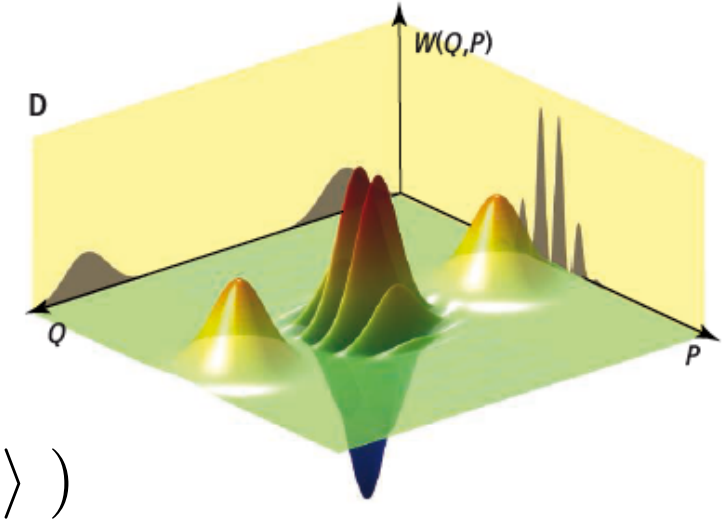
Coherent state



Schrödinger cat state

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

$$|\psi_{even\ cat}\rangle = c_e(\ |\alpha\rangle + |-\alpha\rangle\ )$$

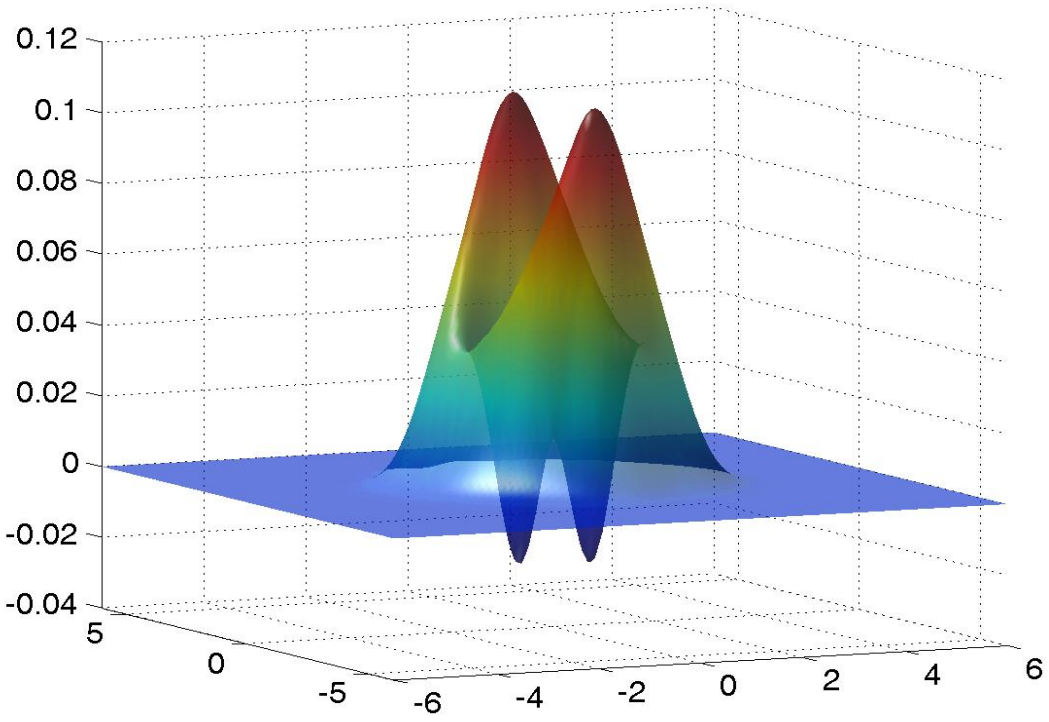


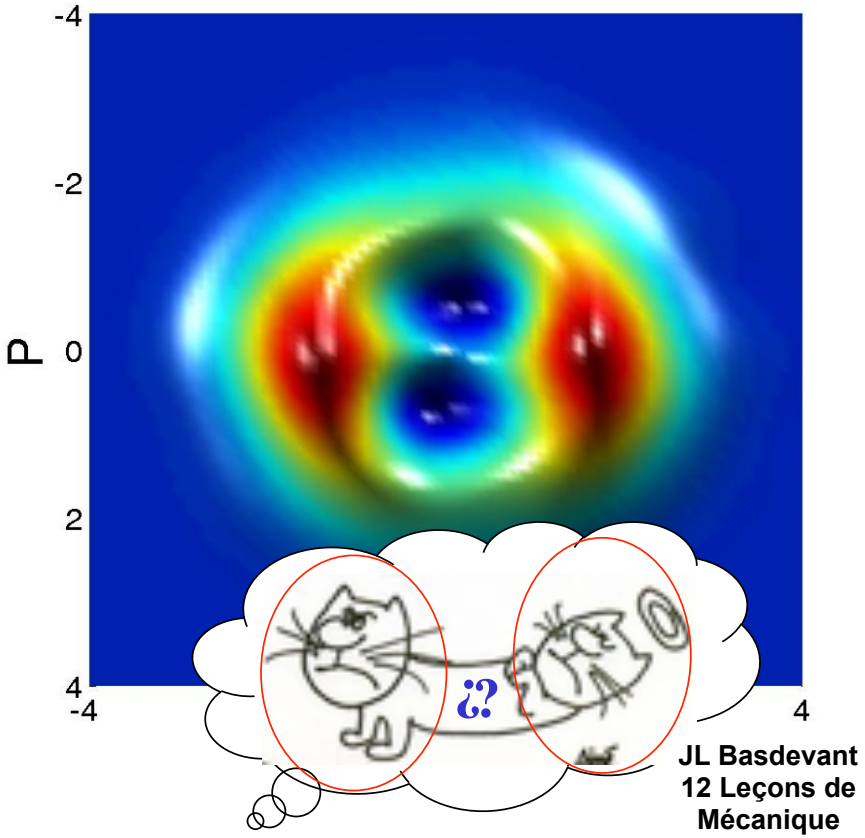
Wigner function of a Schrödinger cat state

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

Experimental Wigner function

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





JL Basdevant
12 Leçons de
Mécanique
Quantique

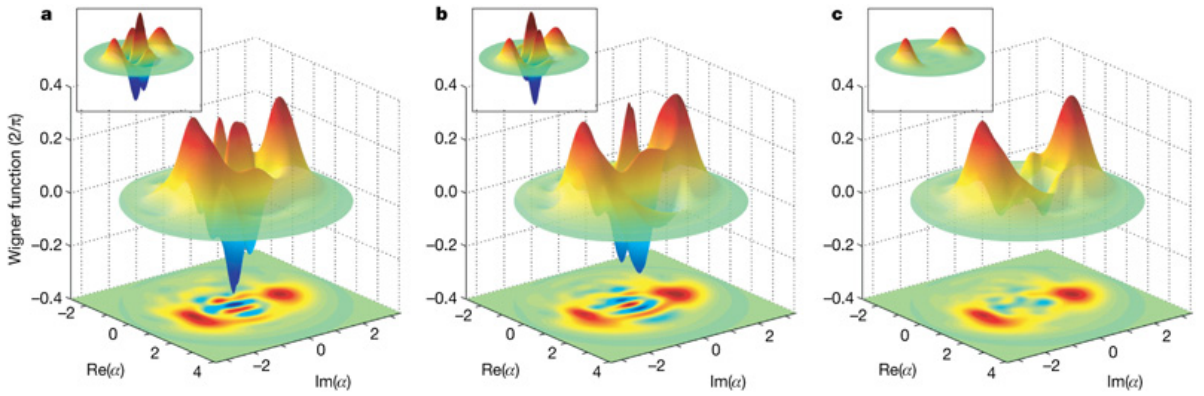
Wigner function of the prepared state
Reconstructed with a Maximal-Likelihood algorithm
Corrected for the losses of the final homodyne detection.

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

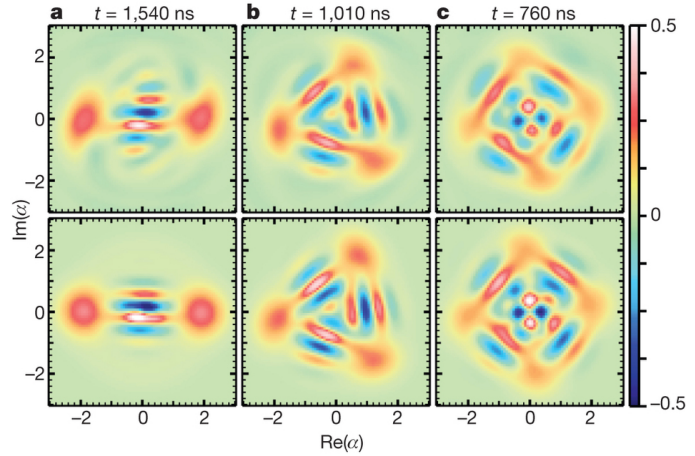
Schrödinger cats with microwaves in superconducting cavities

Some examples...

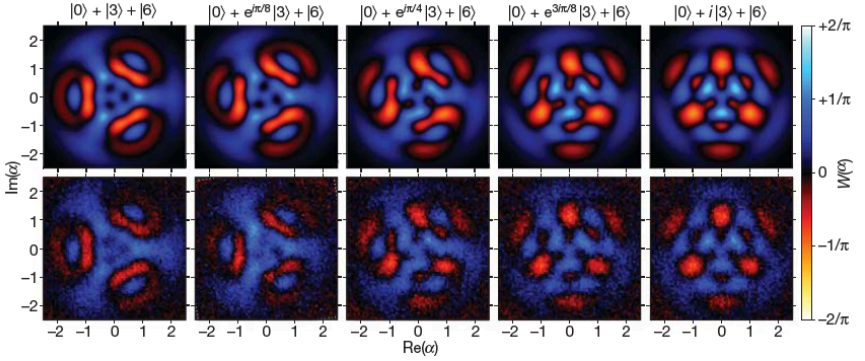
Serge Haroche group
(cacity QED, Paris)
Nature 455, 510 (2008)



Rob Schoelkopf group
(circuit QED, Yale)
Nature 495, 205 (2013)
Cats with 2, 3 or 4 "legs"...



John Martinis group
(circuit QED, Santa Barbara)
Nature 459, 546 (2009)
Quantum state synthetizer



ENS / INRIA / ALICE&BOB electromagnetic cat codes

Exponential suppression of bit-flips in a qubit encoded in an oscillator

Raphaël Lescanne[1,2], Marius Villiers[1,2], Théau Peronnin[3], Alain Sarlette[2], Matthieu Delbecq[1], Benjamin Huard[3], Takis Kontos[1], Mazyar Mirrahimi[2], Zaki Leghtas[4,1,2]

[1] *Laboratoire de Physique de l'Ecole Normale Supérieure, ENS, Université PSL, CNRS, Sorbonne Université, Université Paris-Diderot, Sorbonne Paris Cité, Paris, France*

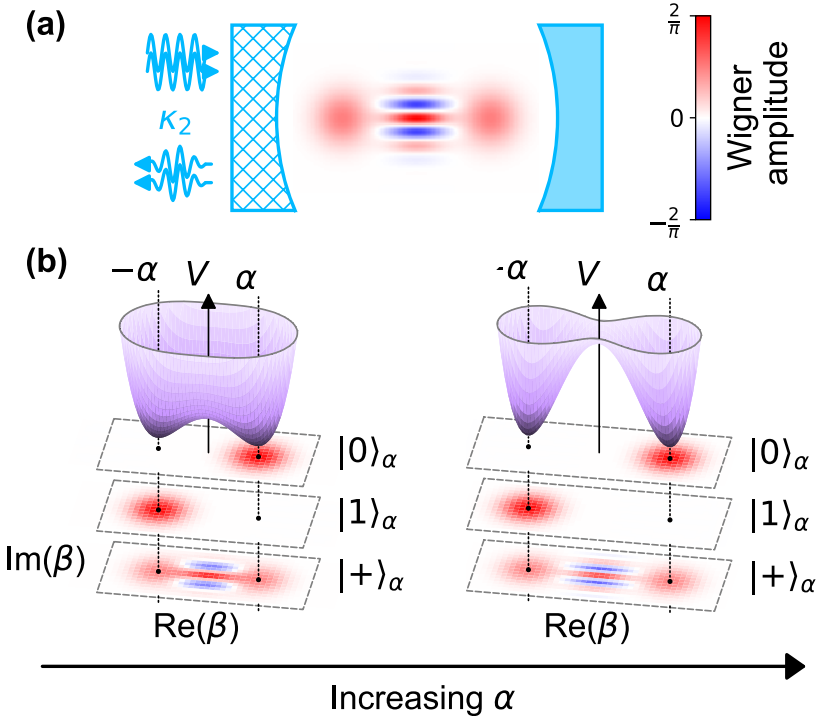
[2] *QUANTIC team, INRIA de Paris, 2 Rue Simone Iff, 75012 Paris, France*

[3] *Université Lyon, ENS de Lyon, Universitée Claude Bernard Lyon 1, CNRS, Laboratoire de Physique, F-69342 Lyon, France and*

[4] *Centre Automatique et Systèmes, Mines-ParisTech, PSL Research University, 60, bd Saint-Michel, 75006 Paris, France*

We encode a qubit in the field quadrature space of a superconducting resonator endowed with a special mechanism that dissipates photons in pairs. This process pins down two computational states to separate locations in phase space. As we increase this separation, we measure an exponential decrease of the bit-flip rate while only linearly increasing the phase-flip rate.

https://arxiv.org/abs/1907.11729



Content of the Talk

Part 1 - Light is quantum ! and propagates far away.

1.1 Discrete and continuous quantum descriptions of light

1.2 A nice tool : the Wigner function

Part 2 - Quantum Key Distribution : DV and CV

2.1 Alice, Bob, and Eve

2.2 Experimental implementations of CVQKD

Part 3 - Towards quantum networks

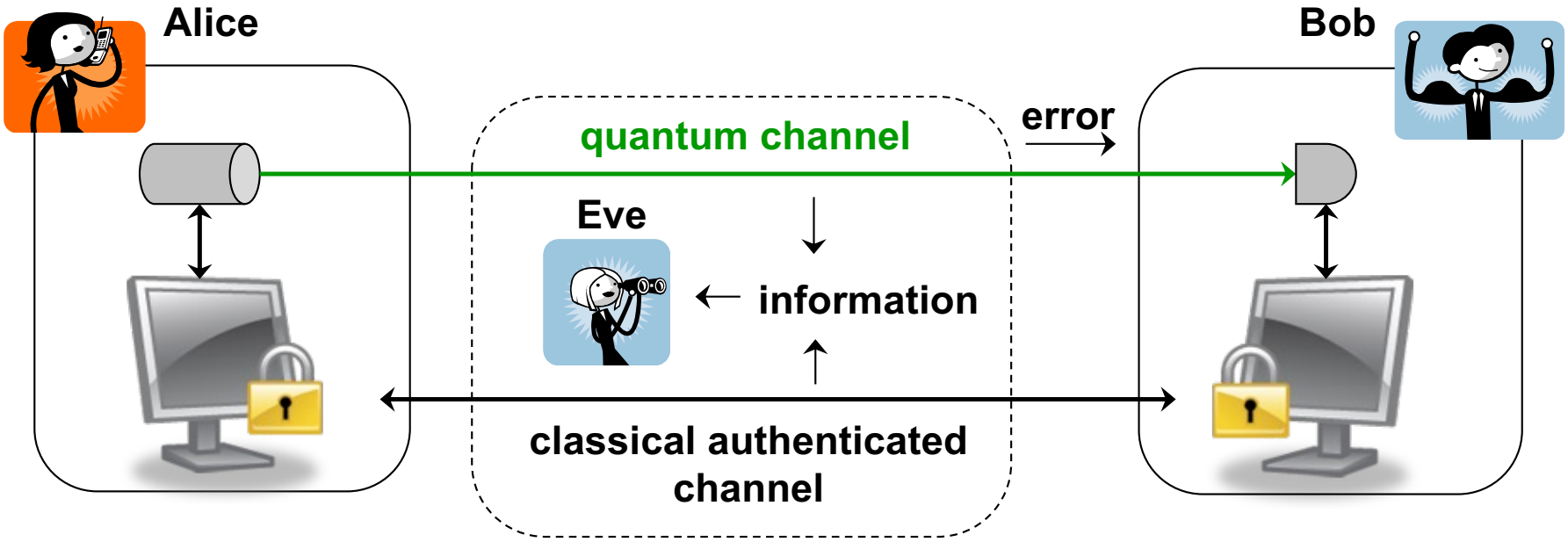
3.1 Overcoming channel losses : trusted nodes, satellites, repeaters

3.2 Looking to the future : deterministic photon-photon interactions

INSTITUT d'OPTIQUE GRADUATE SCHOOL

Secure quantum communications

Quantum key distribution allows secret message exchange with information-theoretic security → guaranteed against an all-powerful eavesdropper



Key information is encoded in photonic carriers

Analysis of errors due to Eve's measurements leads to secret key

Future-proof, unconditionally secure solution to the key distribution problem

INSTITUT d'OPTIQUE GRADUATE SCHOOL

Discrete and continuous-variable QKD

	Discrete variables	Continuous variables
Key encoding	Photon polarization, phase, time arrival	Electromagnetic field quadratures
Detection	Single-photon	Coherent (homodyne/heterodyne)
Post processing	Key readily available	Complex error correction
Security	General attacks, finite-size, side channels	General attacks, finite-size, side channels
	BB84, Decoy state, Coherent One Way, Differential Phase Shift, (M)DI protocols	CV-QKD (one or two-way, Gaussian or discrete modulation, post selection), (M)DI protocols

CV allow for easy implementation with standard telecom components:

no photon counters, no cooling, coherent detection

V. Scarani et al, Rev. Mod. Phys. 2009
E. Diamanti and A. Leverrier, Entropy 2015

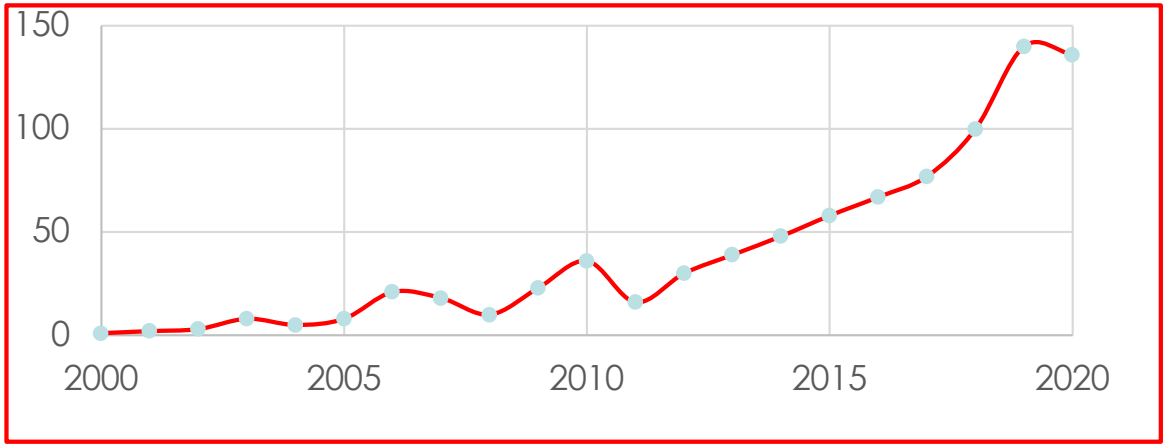
F. Xu et al, Rev. Mod. Phys. 2020
S. Pirandola et al, Adv. Opt. Phot. 2020

REVIEWS OF MODERN PHYSICS

Secure quantum key distribution with realistic devices

Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan
Rev. Mod. Phys. **92**, 025002 – Published 26 May 2020

CVQKD : number of publication per year (from Web of Science)



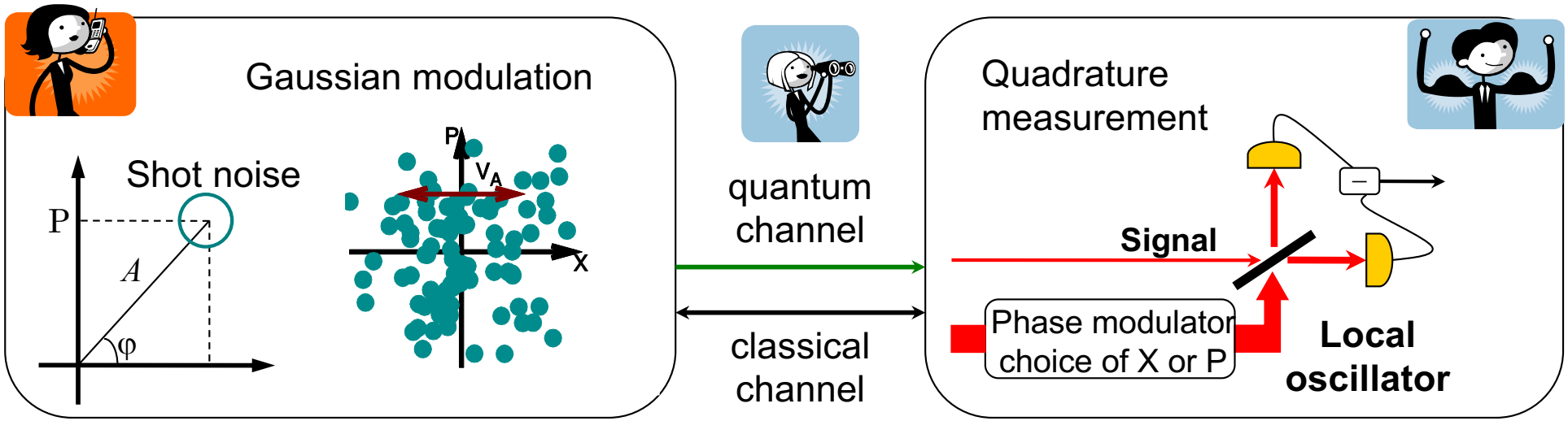
CVQKD : some recent experiments and their performance.

Reference	Clock rate	Distance/loss	Key rate (bps)	Year	Notes
(Jouguet *et al.*, 2013b)	1MHz	80.5km	∼250	2013	Full implementation
(Qi *et al.*, 2015)	25MHz	—	—	2015	Local LO
(Soh *et al.*, 2015)	250KHz	—	—	2015	Local LO
(Huang *et al.*, 2015a)	100MHz	25km	100K	2015	Local LO
(Pirandola *et al.*, 2015)	10.5MHz	4dB	0.1	2015	CV MDI-QKD
(Huang *et al.*, 2015b)	50MHz	25km	∼1M	2015	High key rate
(Kumar *et al.*, 2015a)	1MHz	75km	490	2015	Coexistence with classical
(Zhang *et al.*, 2019b)	5MHz	50km	5.8K	2019	Field test
(Zhang *et al.*, 2020)	5MHz	202.8km[‡]	6.2	2020	Long distance

[‡]Ultra-low loss fiber

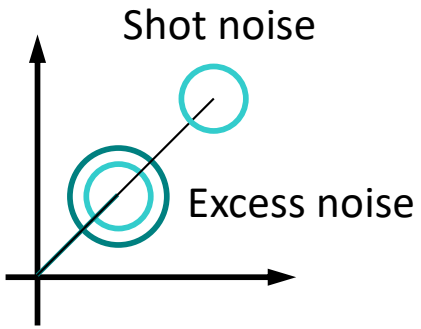
Coherent state CVQKD

- Alice encoding: random modulation of amplitude and phase of coherent states
- Bob measurement: random choice of quadrature of each coherent state with a homodyne detection system
- Classical error correction and privacy amplification



F. Grosshans et al, Nature 2003

CVQKD protocol security

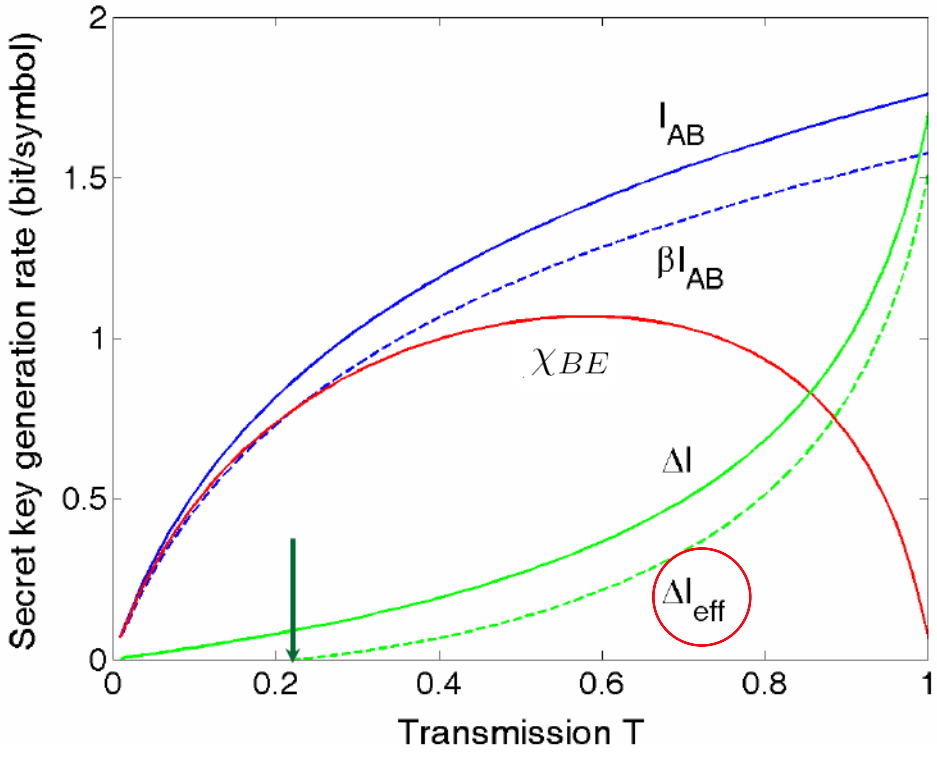


- Coherent states are modified by losses and excess noise
- These are introduced by Eve and degrade the signal-to-noise ratio (SNR) → Alice and Bob make **noise variance measurements → bound on Eve's information** χ_{BE}

Given Alice-Bob mutual information I_{AB} and χ_{BE}, the secret key rate is :

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

where the efficiency β of the key extraction algorithms (data → bits) limits the communication distance



Best proofs so far : composable security
for arbitrary coherent attacks in finite-size regime
See e.g. Anthony Leverrier, PRL **114**, 070501 (2015) & **118**, 200501 (2017)

Content of the Talk

Part 1 - Light is quantum ! and propagates far away.

1.1 Discrete and continuous quantum descriptions of light

1.2 A nice tool : the Wigner function

Part 2 - Quantum Key Distribution : DV and CV

2.1 Alice, Bob, and Eve

2.2 Experimental implementations of CVQKD

Part 3 - Towards quantum networks

3.1 Overcoming channel losses : trusted nodes, satellites, repeaters

3.2 Looking to the future : deterministic photon-photon interactions

Implementations of CVQKD links

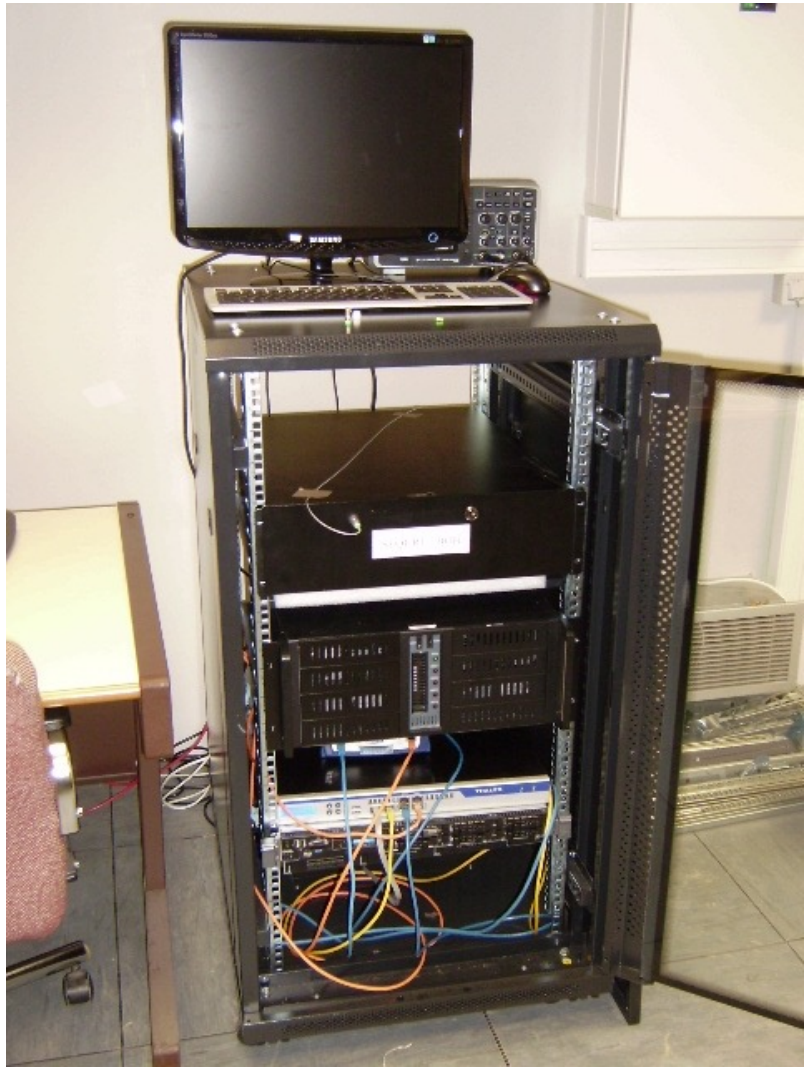
Real-size demonstrations of **secure CV quantum cryptography links** :

* European Project SECOQC, Vienna, 2008 :
Full QKD network with 6 nodes, 8 links
CVQKD link 9 km, 8 kbit/s

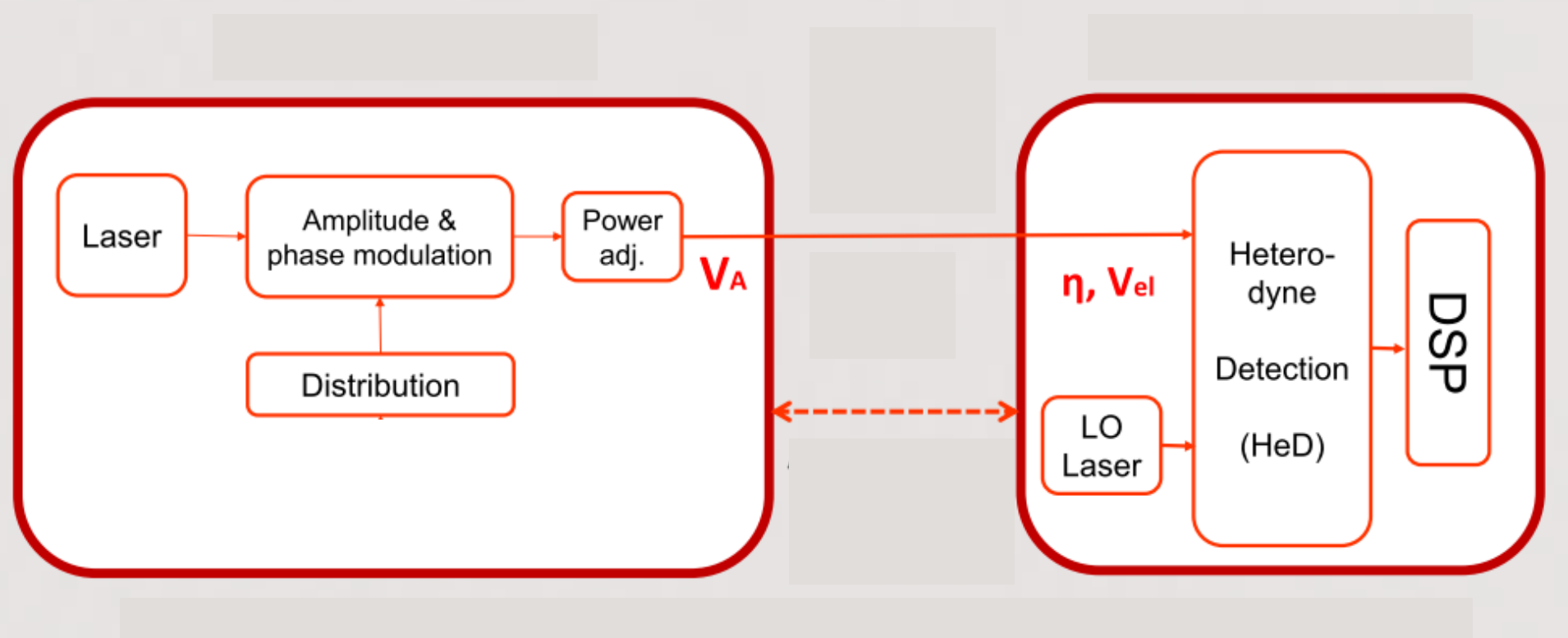
* ANR Project SEQURE, Paris, 2012 :
CVQKD link 12 km, 500 bit/s
Automated link with encryptor « Mistral »

*** Many other demonstrations worldwide :**
- **Japan, China, Europe within the Quantum Flagship project CiViQ**

Complete SEQURE Bob set-up

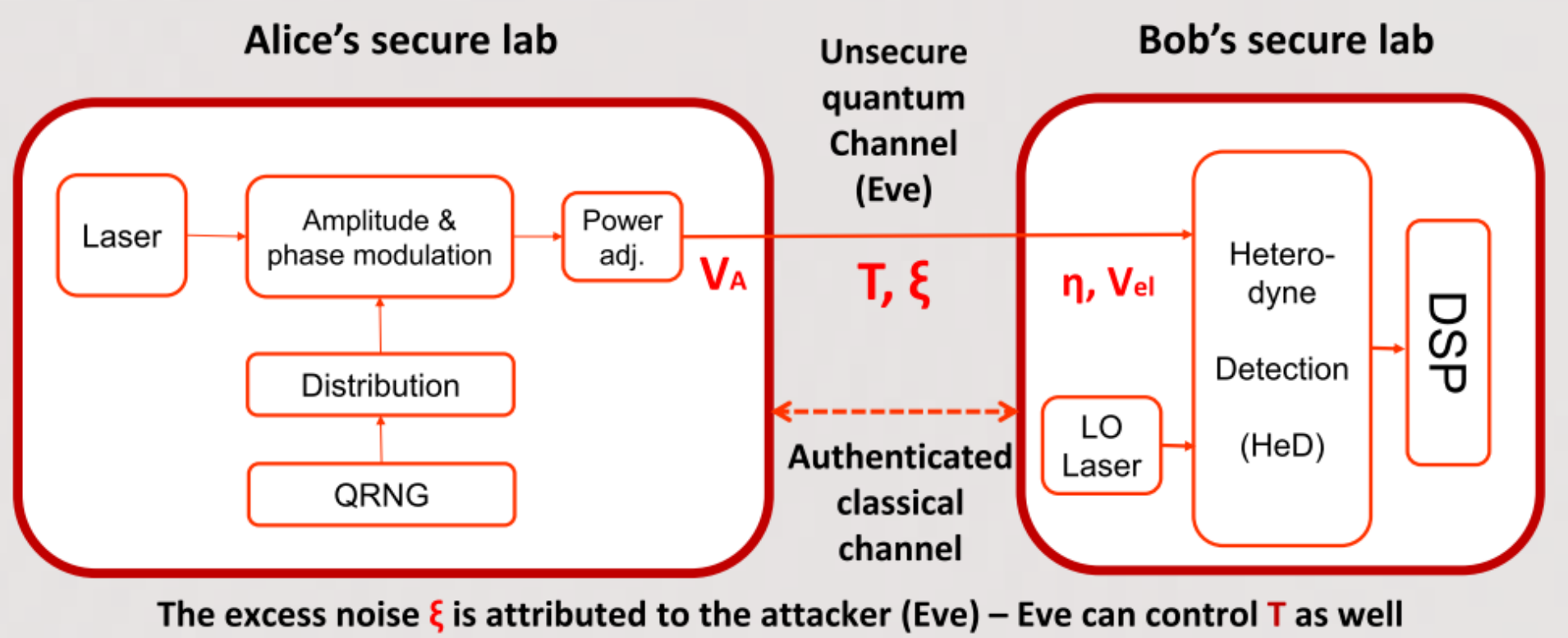


General scheme for coherent telecom



- Independent lasers for signal and local oscillator (LO)
- Commercial coherent detectors (dual polarization heterodyne : ICR)
- Signal recovery : Digital Signal Processor (DSP)

General scheme for coherent telecom



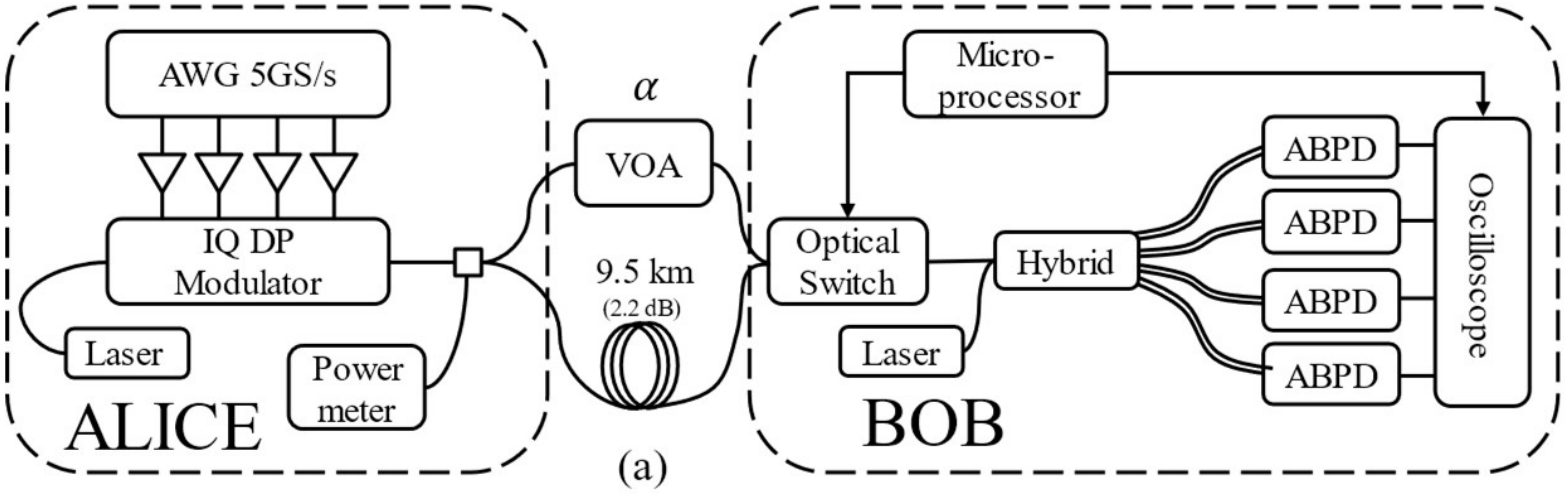
- Narrow bandwidth lasers for signal & LO (e.g. Pure Photonics, ~15 kHz)
- Commercial coherent detectors (dual polarization heterodyne : ICR)
- Home-made DSP, running on a computer

Experiment

High-Rate Continuous Variable Quantum Key Distribution Based on Probabilistically Shaped 64 and 256-QAM

François Roumestan[(1)], Amirhossein Ghazisaeidi[(1)], Jérémie Renaudier[(1)], Luis Trigo Vidarte[(2)], Eleni Diamanti[(2)], and Philippe Grangier[(3)]

[(1)] Nokia Bell Labs, Paris-Saclay, route de Villejust, F-91620 Nozay, France, francois.roumestan@nokia.com
[(2)] Sorbonne Université, CNRS, LIP6, 4 place Jussieu, F-75005 Paris, France
[(3)] Université Paris-Saclay, IOGS, CNRS, Laboratoire Charles Fabry, 2 avenue Fresnel, F-91127 Palaiseau, France



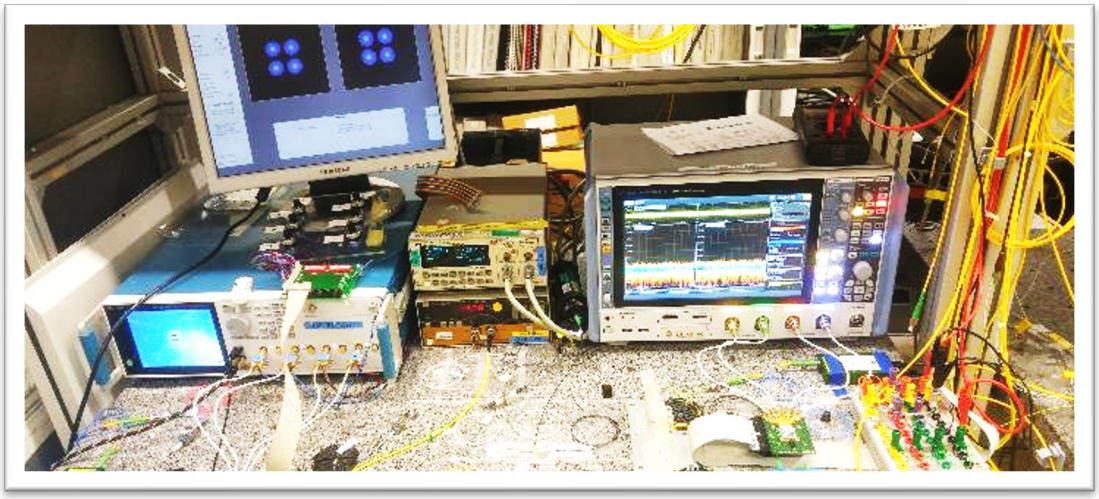
Dual polarization, Nyquist pulses, 600 Mbaud, real LO with 10 kHz bandwith lasers

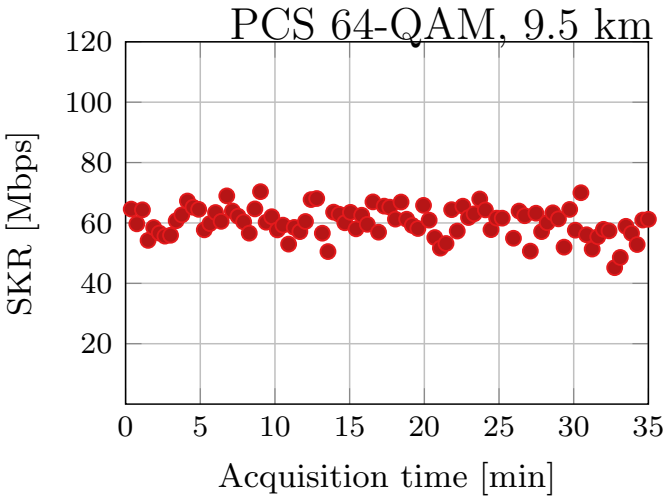
⇒ Optimized shaped constellation (close to Gaussian) + 50% QPSK pilots

⇒ Optimized Digital Signal Processing (DSP), excess noise close to 0.01 SNU

⇒ Data block of 2 10^6 symbols, separated by off periods for SNL calibration

Data processing





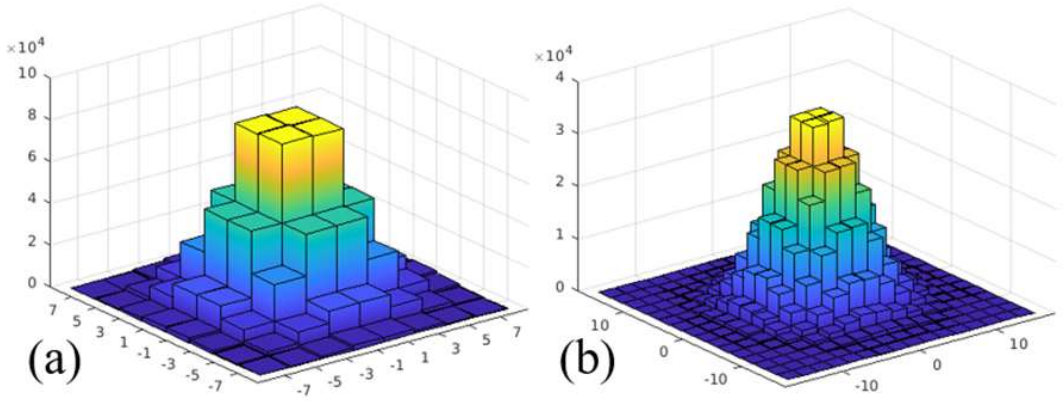
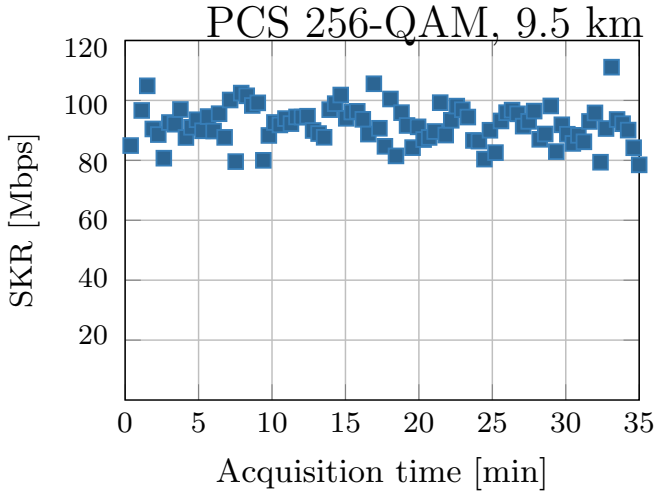


Fig. 1 Histogram of **(a)** PCS 64-QAM with $\nu = 0.0749$, **(b)** PCS 256-QAM with $\nu = 0.0294$ for 10^6 symbols.



F. Roumestan et al, Experimental Demonstration of Discrete Modulation Formats for CVQKD, arXiv:2207.11702

New project in the EuroQCI framework: QKiss

QKiss

exail THALES

Achieved objectives

- Real time opto-electronic system
- Low excess noise
- Compatible for up to 1G symbols
- High-speed interfaces

Short time objectives

- Reduce the excess noise
- Upgrade DSP
- Build a demonstrator
- Field tests in 2024

Long time objectives

- Lower excess noise
- Low SNR
- Stable system, good calibration
- Real time DSP
- Homemade components

=> Industrial CV-QKD devices by 2025

Content of the Talk

Part 1 - Light is quantum ! and propagates far away.

1.1 Discrete and continuous quantum descriptions of light

1.2 A nice tool : the Wigner function

Part 2 - Quantum Key Distribution : DV and CV

2.1 Alice, Bob, and Eve

2.2 Experimental implementations of CVQKD

Part 3 - Towards quantum networks

3.1 Overcoming channel losses : trusted nodes, satellites, repeaters

3.2 Looking to the future : deterministic photon-photon interactions

Overcoming channel losses

Going beyond point-to-point links towards secure quantum networks:

*** Trusted node networks:**

*** SECOQC QKD network, 2008**

* Durban South Africa network, 2010

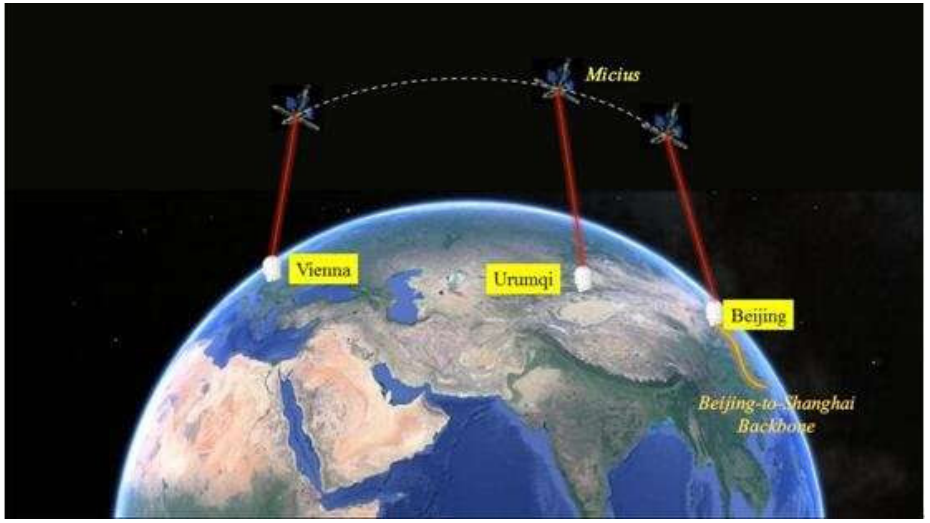
* Swiss Quantum Network, 2011

* Tokyo QKD network, 2015

* UK QC Hub (Cambridge, Bristol)

* 2000 km, 60-node network in China

* Planned EU-wide testbed (EuroQCI)



*** Satellite communications:**

* MICIUS satellite : intercontinental QKD (China-Austria)

* European Space-QUEST initiative:

Fundamental physics and quantum communications, S. Joshi et al, 1703.08036

*** CVQKD in space ? European projects**

Positive secret key rate in principle for Low Earth Orbit (LEO) – ground link,

including pointing, diffraction, turbulence, losses (T binning), orbit motion…

*** Ultimate solution : quantum repeaters ! require entanglement…**

Long distance quantum communications

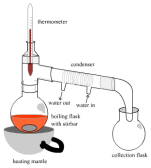
How to fight against line losses ?

~~Amplification~~

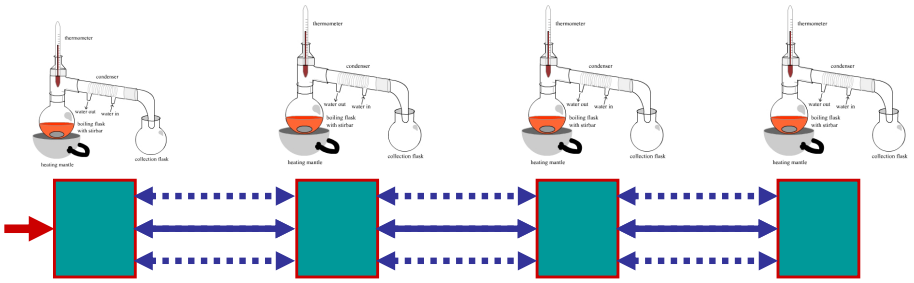
$a|+\rangle + b|-\rangle$ → G → G → G → ~~$a|+\rangle + b|-\rangle$~~

1. **Exchange of entangled states** $|\psi_B\rangle$

2. **Entanglement distillation**



$a|+\rangle + b|-\rangle$



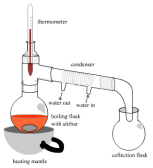
Long distance quantum communications

How to fight against line losses ?

~~Amplification~~

$a|+\rangle + b|-\rangle$ — G — G — G — ~~$a|+\rangle + b|-\rangle$~~

1. Exchange of entangled states $|\psi_B\rangle$

2. Entanglement distillation 

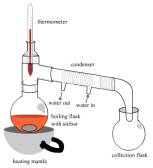
$a|+\rangle + b|-\rangle$ — ■ — M — M — ■

Long distance quantum communications

How to fight against line losses ?

~~Amplification~~ $a|+\rangle + b|-\rangle$ — G — G — G — ~~$a|+\rangle + b|-\rangle$~~

1. Exchange of entangled states $|\psi_B\rangle$

2. Entanglement distillation  $a|+\rangle + b|-\rangle$ ⟵⟶ $a|+\rangle + b|-\rangle$

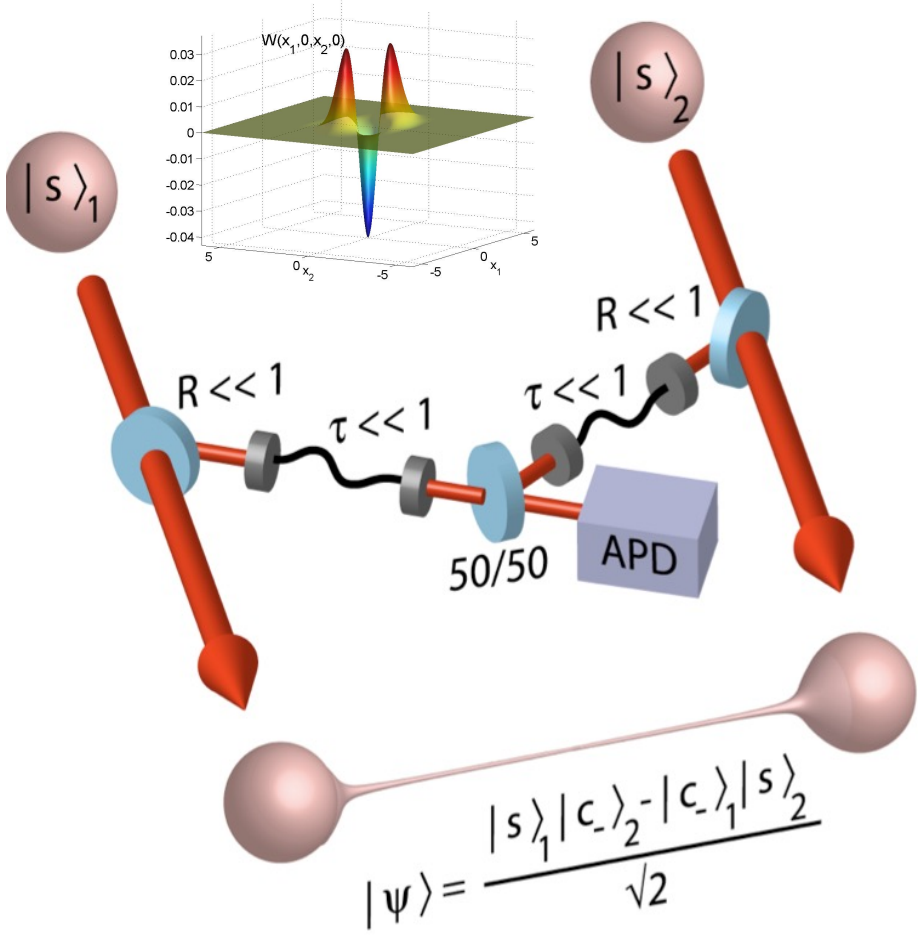
3. Entanglement swapping M M

4. Quantum teleportation

One needs to : * distribute (many) entangled states
* store them (quantum memories)
* process them (distillation)

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 :

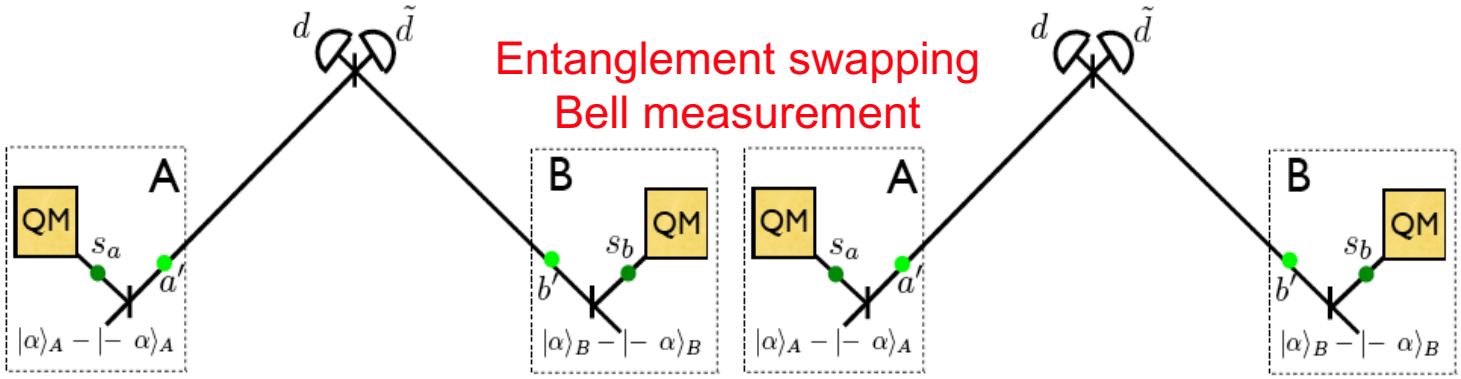
$$|\Psi\rangle = (|s\rangle_1 |cat\rangle_2 - |cat\rangle_1 |s\rangle_2)/\sqrt{2}$$

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

Experiment works fine, high remote entanglement :
A. Ourjoumtsev et al, Nature Physics, 5, 189, 2009

Quantum repeaters with entangled cats ?

N. Sangouard et al, JOSA B 27, 137 (2010)



Difficulty : Bell measurements are needed, and they are extremely sensitive to losses…

=> Low overall efficiency, not significantly better than using entangled photons :-((

What is missing ?

- **The production of the useful quantum states (qubits, cats…) should be deterministic, not conditionnal**
- **For efficient quantum processing (gates, measurements…) one would need strong interactions between individual photons**
- **OK in the microwave domain, difficult in the optical domain**
  => cavity QED or Rydberg states

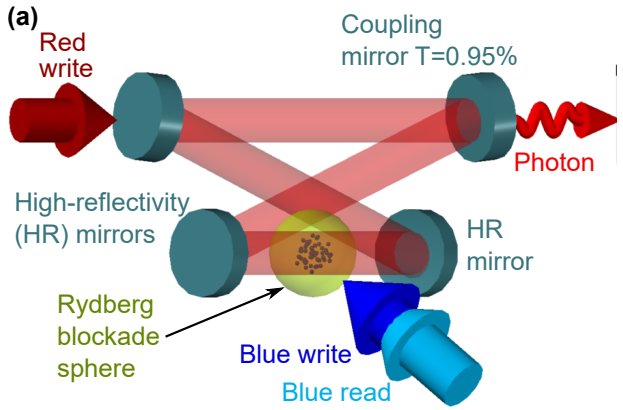
INSTITUT d'OPTIQUE GRADUATE SCHOOL

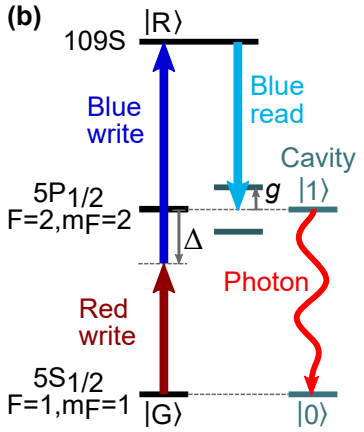
A glimpse to the future : emitting photonic qubits by superatoms

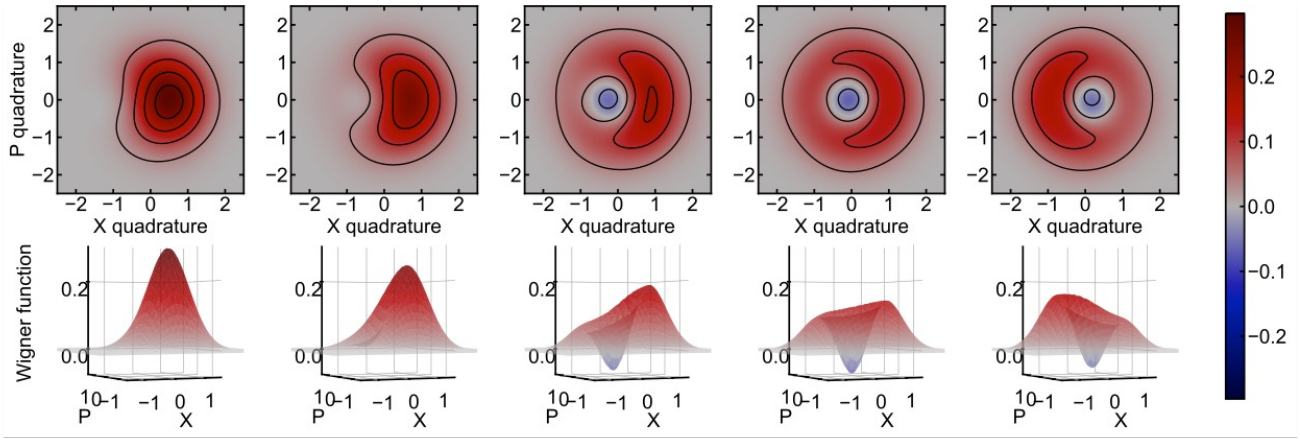
Deterministic Free-Propagating Photonic Qubits with Negative Wigner Functions

Valentin Magro, Julien Vaneecloo, Sébastien Garcia, and Alexei Ourjoumtsev*
JEIP, UAR 3573 CNRS, Collège de France, PSL University,
11, place Marcelin Berthelot, 75231 Paris Cedex 05, France

arXiv:2209.02047v1 [quant-ph] 5 Sep 2022







* Only one atom can be excited within an ensemble of 800 atoms contained in a sphere of 4.5 µm radius, due to the effect of « Rydberg blockade »
=> Rydberg superatom

* An arbitrary superposition $(\cos(\theta/2)\,|G\rangle - \sin(\theta/2)\,|R\rangle)$ of the ground and excited states can be created, and mapped on demand on the photonic superposition $(\cos(\theta/2)\,|n=0\rangle + \sin(\theta/2)\,|n=1\rangle)$ that leaves the cavity
=> Deterministic generation of photonic qubits

INSTITUT d'OPTIQUE GRADUATE SCHOOL

Thank you for your attention !