Quantum Optics and Quantum Information with Continuous Variables

Philippe Grangier

Laboratoire Charles Fabry de l'Institut d'Optique, UMR 8501 du CNRS, 91127 Palaiseau, France
Part 1: Gaussian and non-Gaussian states
1. Homodyne detection and quantum tomography
2. Generating non-Gaussian Wigner functions: kittens, cats and beyond

Part 2: Continuous variable quantum cryptography (Gaussian !)
1. Continuous variable quantum cryptography: principles
2. Continuous variable quantum cryptography: implementations

Part 3: Towards quantum networks (non-Gaussian !)
1. Entanglement for continuous variable quantum networks
2. Deterministic photon-photon interactions
### « Discrete » vs « continuous » Light

<table>
<thead>
<tr>
<th>Light is:</th>
<th><strong>Discrete</strong>Photons</th>
<th><strong>Continuous</strong>Wave</th>
</tr>
</thead>
<tbody>
<tr>
<td>We want to know:</td>
<td>their <strong>Number</strong> &amp; <strong>Coherence</strong></td>
<td>its <strong>Amplitude</strong> &amp; <strong>Phase</strong> (polar) its <strong>Quadratures X &amp; P</strong> (cartesian)</td>
</tr>
<tr>
<td>We describe it with:</td>
<td><strong>Density matrix</strong> $\rho_{n,m}$</td>
<td><strong>Wigner function</strong> $W(X,P)$</td>
</tr>
<tr>
<td>We measure it by:</td>
<td><strong>Counting</strong>: APD, VLPC, TES...</td>
<td><strong>Demodulating</strong>: Homodyne Detection</td>
</tr>
<tr>
<td>« Simple » States</td>
<td><strong>Fock States</strong></td>
<td><strong>Gaussian States</strong></td>
</tr>
</tbody>
</table>
Coherent (Homodyne) Detection, Wigner Function and Quantum Tomography

- Quasiprobability density:
  - Wigner function $W(X,P)$
- Marginals of $W(X,P)$
  => Probability distributions $P(X)$
- Probability distributions $P(X)$
  => $W(X,P)$ (quantum tomography)
Non-Gaussian States

Basic question:

Consider a single photon: can we speak about its amplitude & phase? quadratures $X$ & $P$?

Single mode light field

- Photons
- $n$ photon state
- Probability $P_n(X)$

Harmonic oscillator

- Quanta of excitation
- $n$th eigenstate
- Probability $|\Psi_n(x)|^2$

$n=0$ photons

$n=1$ photon

$n=2$ photons

$|\Psi_n(x)|^2$
Can the Wigner function of a Fock state $n = 1$ (with all projections having zero value at origin) be positive everywhere?
Non-Gaussian States

Basic question:

Consider a single photon: can we speak about its quadratures $X$ & $P$?

NO!

The Wigner function must be negative

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

Many interesting properties for quantum information processing
Wigner function of a single photon state? (Fock state n = 1)

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

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

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

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:

\[
\langle q | 1 \rangle = \frac{q}{(2\pi)^{1/4} N_0^{3/4}} e^{-\frac{q^2}{4N_0}}
\]

one gets finally:

\[
W_{1}(q, p) = -\frac{1}{2\pi N_0} e^{-\frac{r^2}{2N_0}} \left( 1 - \frac{r^2}{N_0} \right) \quad r^2 = q^2 + p^2
\]
Coherent state $|\alpha\rangle$

Squeezed state

Fock state $|n=1\rangle$

Cat state $|\alpha + |-\alpha\rangle$

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

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

Generating Optical Schrödinger Kittens for Quantum Information Processing
Alexei Ounjoumtev, Rosa Tualle-Brouri, Julien Laurat, Philippe Grangier

Experimental demonstration of quantum memory for light
Brian Julsgaard¹, Jacob Sherson¹, J. Ignacio Cirac³, Jaromír Fiurášek¹ & Eugene S. Polzik¹

Quantum teleportation between light and matter
Jacob F. Sherson¹,², Hanna Krauter¹, Rasmus K. Olsson¹, Brian Julsgaard¹, Klemens Hammerer², Ignacio Cirac³ & Eugene S. Polzik¹

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 of optical ‘Schrödinger cats’ from photon number states
Alexei Ounjoumtev¹, Hyunseok Jeong², Rosa Tualle-Brouri¹ & Philippe Grangier¹

Teleportation of Nonclassical Wave Packets of Light
Noriyuki Lee¹, Hugo Benichi¹, Yuishi Takeno¹, Shuntaro Takeda¹, James Webb²
Flanor Huntinton² Akira Furusawa¹

Small sample, many more papers!
Part 1 : Gaussian and non-Gaussian states
1. Homodyne detection and quantum tomography
2. Generating non-Gaussian Wigner functions : kittens, cats and beyond

Part 2 : Continuous variable quantum cryptography
1. Continuous variable quantum cryptography : principles
2. Continuous variable quantum cryptography : implementations

Part 3 : Towards quantum networks
1. Entanglement for continuous variable quantum networks
2. Deterministic photon-photon interactions
« 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

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

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

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

Wigner function of a Schrödinger cat state
How to create a Schrödinger’s cat?

Suggestion by Hyunseok Jeong, calculations by Alexei Ourjoumtsev:

For \( n \geq 3 \) the fidelity of the conditional state with a Squeezed Cat state is \( F \geq 99\% \)

\[
S(r)\left( |\alpha\rangle + e^{i\theta} | - \alpha\rangle \right)
\]
Femtosecond Ti-S laser pulses 180 fs, 40 nJ, rep rate 800 kHz

Experimental Set-up
Resource: Two-Photon Fock States

\[ |\psi\rangle = \sum \lambda^n |n, n\rangle \]

Femtosecond laser

Homodyne detection

OPA

APD1

APD2

Experimental Wigner function (corrected for homodyne losses)

Squeezed Cat State Generation

Homodyne Conditional Preparation:
Success Probability = 7.5%

Tomographic analysis of the produced state

Two-Photon State Preparation
Experimental Wigner function


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…
Content of the Tutorial

Part 1: Gaussian and non-Gaussian states
1. Homodyne detection and quantum tomography
2. Generating non-Gaussian Wigner functions: kittens, cats and beyond

Part 2: Continuous variable quantum cryptography
1. Continuous variable quantum cryptography: principles
2. Continuous variable quantum cryptography: implementations

Part 3: Towards quantum networks
1. Entanglement for continuous variable quantum networks
2. Deterministic photon-photon interactions
* 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 state continuous variables QKD protocol

- Key information encoded in both quadratures of a coherent state

\[ \chi = \frac{1}{T} - 1 + \varepsilon \]

equivalent to photon loss

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

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

$$I_{AB} = \frac{1}{2} \log_2 \left[ 1 + \frac{V(\text{signal})}{V(\text{noise})} \right]$$

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

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

(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.

Reminder: $I(X; Y) = H(X) - H(X | Y) = H(Y) - H(Y | X) = H(X) + H(Y) - H(X; Y)$
Security of coherent state CV-QKD: collective attacks

For both individual and collective attacks, Gaussian attacks are optimal. Alice and Bob consider Eve’s attacks Gaussian and estimate her information using the Shannon quantity $I_{BE}$ or the Holevo quantity $\chi_{BE}$.

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

Error correcting codes efficiency

- Errorless bit strings must be extracted from noisy continuous data
- Binning + error correction with very efficient LDPC codes, efficiency $\beta < 1$

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

Alice-Bob mutual information : $I_{AB}$
Available after error correction : $\beta I_{AB}$

Eve-Bob mutual information :
$\chi_{BE}$ (Holevo : collective attacks)

Imperfect correction efficiency induces a limit to the secure distance
Security of coherent state CV-QKD protocol

- Security initially proven against (arbitrary) individual attacks:

- Then security proven against arbitrary collective attacks:

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

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

Content of the Tutorial

Part 1: Gaussian and non-Gaussian states
1. Homodyne detection and quantum tomography
2. Generating non-Gaussian Wigner functions: kittens, cats and beyond

Part 2: Continuous variable quantum cryptography
1. Continuous variable quantum cryptography: principles
2. Continuous variable quantum cryptography: implementations

Part 3: Towards quantum networks
1. Entanglement for continuous variable quantum networks
2. Deterministic photon-photon interactions
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)
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)
Symmetric Encryption with QUantum key REnewal
SEQURE

- Thales : Mistral Gbit
Field implementation

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

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

See http://www.demo-secure.com
Post-processing at SeQureNet

Last version (commercial device, 80 km) :

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 !

=> $\beta$ is improved from 89% to 95% for any SNR : longer distance (80 km)

![Graph showing key rate vs distance](image)

CYGNUS (commercial product)
• Several recent examples of “quantum hacking” (e.g. Vadim Makarov et al.)
• Exploits weaknesses in single photon detectors
• Will NOT work against CVQKD (PIN photodiodes, linear regime)
• Hackers will have to work harder...
• ... and Trojan attacks will not make it (work under way, SQN + U. Erlangen)
Many other works on CVQKD! <= Theory and Experiments:
(incomplete list!)
Part 1: Gaussian and non-Gaussian states
1. Homodyne detection and quantum tomography
2. Generating non-Gaussian Wigner functions: kittens, cats and beyond

Part 2: Continuous variable quantum cryptography
1. Continuous variable quantum cryptography: principles
2. Continuous variable quantum cryptography: implementations

Part 3: Towards quantum networks
1. Entanglement for continuous variable quantum networks
2. Deterministic photon-photon interactions
Need to share highly entangled states (cryptography..)

Problem : losses

Solution : Entanglement Distillation :

But impossible to distill Gaussian entanglement with Gaussian means

⇒ use non-gaussian operations !
(such as photon subtraction)
How to create entanglement at a large distance?

Two main approaches

Alice \rightarrow Victor \rightarrow Bob

(Distillation)

Entangled states

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

Exemple:

Mostly limites by losses

Alice \rightarrow OPA \rightarrow Victor \rightarrow Bob

Joint measurement

Victor \rightarrow Entangled states

Mostly limited by noise

Alice \rightarrow 50/50 \rightarrow Victor \rightarrow DOPA

Bob \rightarrow APD \rightarrow R \ll 1

Exemple:

Mostly limites by losses

Alice \rightarrow Victor \rightarrow Bob

(Distillation)

Entangled states

Mostly limited by noise

In the present state of technology, this is much more efficient for distances ~ 100 km
Remote entanglement of cat states using "delocalized" photon subtraction
Main advantage of this scheme: almost insensitive to transmission losses!
(the non-local cats are never transmitted in the line)

Non-local photon subtraction:
\[ |c_{-}\rangle_1 = |\alpha\rangle_1 - |\alpha\rangle_1 \]
\[ |c_{-}\rangle_2 = |\alpha\rangle_2 - |\alpha\rangle_2 \]

Direct transmission:
\[ |c_{-}\rangle = |\alpha\sqrt{2}\rangle - |\alpha\sqrt{2}\rangle \]

Fidelity for 10 dB losses:
\[ F = 0.4 \]  
\[ F = 0.003 \]
Experiment
A. Ourjoumtsev et al, Nature Physics, 5, 189, 2009

Experimental set-up
Two-mode probability distributions
(two phases $\phi$ and $\theta$...)
Full two-mode tomography:

\[ P(x_1, \theta, x_2, \phi) \]

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

Entanglement: \( N = 0.25 \pm 0.04 \)

Almost insensitive to losses in the quantum channel!

… but still far from a quantum repeater!

\[ T_{filters \& \ APD} \sim 10\% : \sim 100 \text{ km optical fiber} \]
Bell measurements are deterministic for entangled cats using only BS and photon counters!

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

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)
Content of the Tutorial

Part 1: Gaussian and non-Gaussian states
1. Homodyne detection and quantum tomography
2. Generating non-Gaussian Wigner functions: kittens, cats and beyond

Part 2: Continuous variable quantum cryptography
1. Continuous variable quantum cryptography: principles
2. Continuous variable quantum cryptography: implementations

Part 3: Towards quantum networks
1. Entanglement for continuous variable quantum networks
2. Deterministic photon-photon interactions
Photon – photon interactions

* **Basic question we want to address**: is it possible to design and manipulate (dispersive and deterministic) **photon-photon interactions**?

**Non-classical state generation**

- **Self-Kerr effect**: $|n \rangle \rightarrow (e^{i\varphi})^{n(n-1)/2} |n \rangle$

  B. Yurke & D. Stoler, PRL 57, 13 (1986)

  - We want $\varphi = \pi$ per photon (aJ !)

**Control-phase gate**

- **Cross-Kerr effect** $|n \rangle |m \rangle \rightarrow (e^{i\varphi})^{nm} |n \rangle |m \rangle$

* **Present approaches**:

  - **measurement-induced non-linearities**, e.g. for KLM, or for producing Fock states, Schrödinger's cat states, noiseless amplification... **Nice expts but their non-deterministic character makes them hardly scalable**

  - **cavity QED**: either optical domain or microwave domain (we want optical)
Using Rydberg-Rydberg interactions

* A possible approach:
  - use Rydberg-Rydberg interactions to induce photon-photon interactions
  - photons -> (interacting) Rydberg polaritons -> photons

* Lot of ongoing work:

Theory: among recent ones, A. Gorshkov, T. Pohl, F. Bariani, M. Fleischhauer, M. Lukin, G. Kurizki, K. Moelmer & many others

Experiments: groups of C. Adams, A. Kuzmich, V. Vuletic & M. Lukin...
Single Photon from a single polariton
(DLCZ protocol)

L.M. Duan, M.D. Lukin, J.I. Cirac, and P. Zoller,
Nature 414, 413 (2001)

$^{87}\text{Rb MOT:}$
Density $\rho \approx 4 \times 10^{10} \text{ cm}^{-3}$
Cooperativity $C \approx 200$

Single Photon from a single polariton
(DLCZ protocol)

Single Photon from a single polariton (DLCZ protocol)

Single Photon from a single polariton (DLCZ protocol)

Single Photon from a single polariton (DLCZ protocol)

Single Photon from a single polariton (DLCZ protocol)

Overall detection efficiency : 55%

Corrected for detection efficiency

Overall extraction efficiency : 80%

Single Photon from a single polariton (DLCZ protocol)

Quantum memory effect: the memory time (1 µs) is limited by motional decoherence due to finite temperature (50 µK)

They did the hard work...

CVQKD team (Vienna 2008)

Franck Ferreyrol

Rosa Tualle-Brouri

Frédéric Grosshans

Non-Gaussian team (Palaiseau 2010)

Jérôme Lodewyck

Simon Fossier

Thierry Debuisschert

Eleni Diamanti

Rosa Tualle-Brouri

Marco Barbieri

Rémi Blandino
Thank you for your attention!

Valentina Parigi (post-doc, exp.)
Erwan Bimbard (PhD, exp.)
Etienne Brion (CNRS)
Alexei Ourjoumtsev (CNRS)

Rydberg polariton team

Jovica Stanojevic (post-doc, th.)
Andrey Grankin (PhD, th.)

Just arrived! : Rajiv Boddeda, Imam Usmani
Technical staff: F. Fuchs, F. Moron, A. Guilbaud
Collaboration: Pierre Pillet (LAC Orsay)

DELPHI
Deterministic Logical Photon-photon Interactions