



Quantum Optics and Quantum Communications using Gaussian and Non-Gaussian States of the Light

Philippe Grangier

Laboratoire Charles Fabry de l'Institut d'Optique,
UMR 8501 du CNRS, 91127 Palaiseau, France



Content of the Talk

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 !)

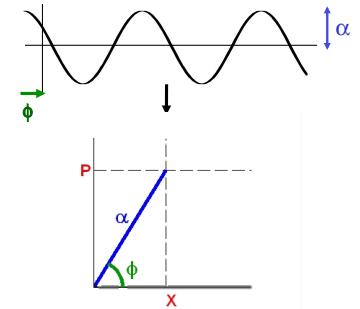
1. Entanglement for continuous variable quantum networks
2. Teleportation of Schrödinger's cats
3. Storing non-Gaussian states : single photon quantum memory

Quantum description of light

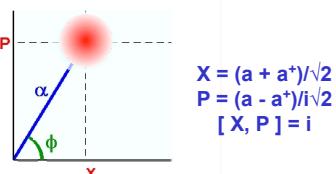
Discrete	Photons	Continuous	Wave
----------	---------	------------	------

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...

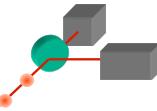
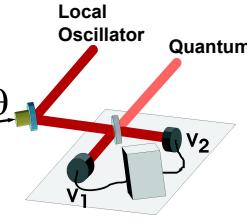
Quantum description of light

Parameters :	Discrete	Photons	Continuous	Wave
	Number of photons n		Amplitude & Phase (polar) Quadratures $X & P$ (cartesian)	
	Coherences $\langle n p m \rangle$			

Quantum description of light

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

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  Local Oscillator Quantum state θ $V_1 - V_2 \propto E_{OL}E_{EQ}(\theta)$ $\propto X_\theta = X \cos\theta + P \sin\theta$ Interference, then subtraction of photocurrents :

Homodyne detection

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

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

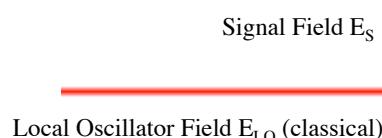
$$I_1 - I_2 = |E_{LO}|(E_S e^{-i\theta_{LO}} + E_S^* e^{i\theta_{LO}})$$

X meas.

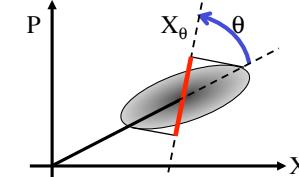
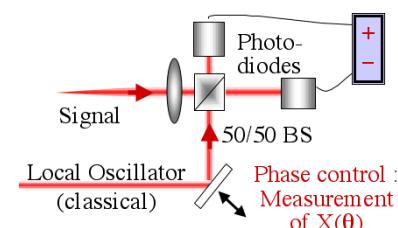
P meas.

X and P do not commute :
Heisenberg relation

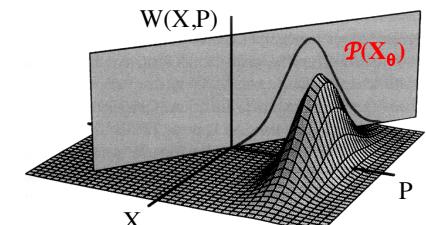
$$V(X) V(P) \geq N_0^2$$



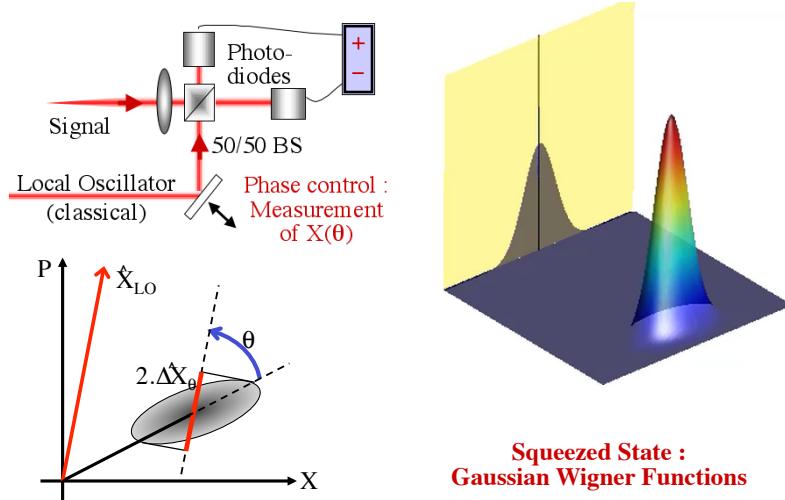
Homodyne detection, Wigner Function and Quantum Tomography



- Quasiprobability density : Wigner function $W(X,P)$
- Marginals of $W(X, P)$
 \Rightarrow Probability distributions $P(X_\theta)$
- Probability distributions $P(X_\theta)$
 $\Rightarrow W(X, P)$ (quantum tomography)



Homodyne detection, Wigner Function and Quantum Tomography



Non-Gaussian States

Basic question :

Consider a single photon : can we measure its amplitude & phase? quadratures X & P?

Single mode light field

Photons

n photon state

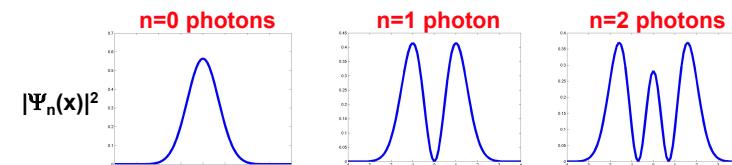
Probability $P_n(X)$

Harmonic oscillator

Quanta of excitation

nth eigenstate

Probability $|\Psi_n(x)|^2$

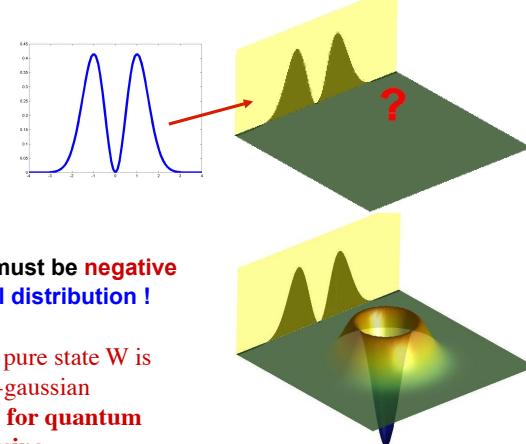


Non-Gaussian States

Basic question :

Consider a single photon : can we measure its amplitude & phase? quadratures X & P?

Can the Wigner function of a Fock state n = 1 (with all projections have zero value at origin) be positive everywhere ?



NO ! The Wigner function must be negative It is not a classical statistical distribution !

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)

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

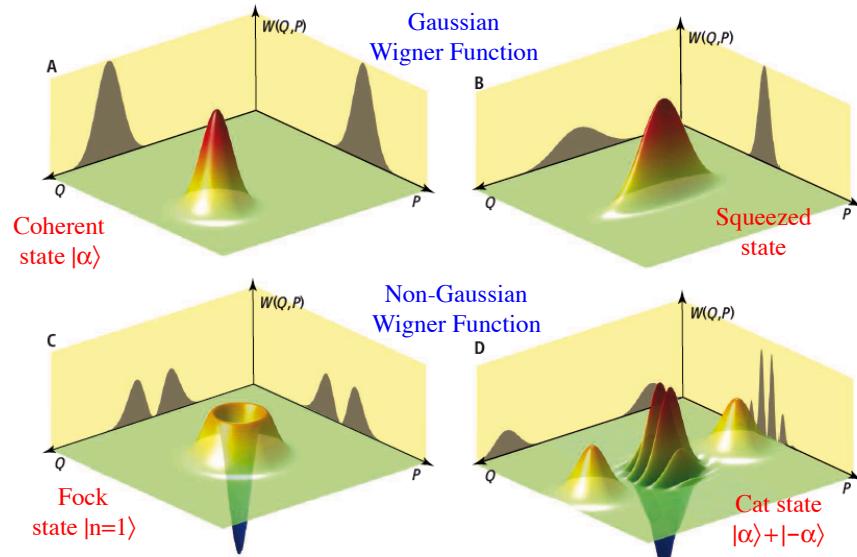
where $\hat{p} = |1\rangle\langle 1|$ and N_0 is the variance of the vacuum noise :

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

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

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



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

Make It Quantum and Continuous

Philippe Grangier PERSPECTIVES SCIENCE VOL 332 15 APRIL 2011

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 Ourjoumtsev¹, Hyunseok Jeong², Rosa Tualle-Brouri¹ & Philippe Grangier¹

Teleportation of Nonclassical Wave Packets of Light

Noriyuki Lee,¹ Hugo Benisty,¹ Yuichi Takeo,¹ Shuntaro Takeda,¹ James Webb,²
Florian Minnemann,² Akira Furusawa^{1*}

15 APRIL 2011 VOL 332 SCIENCE

Small sample, many more papers !



Content of the Talk



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 !)

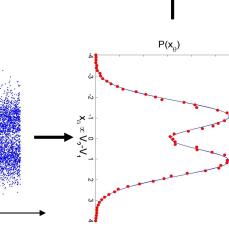
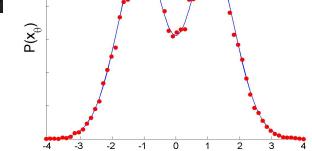
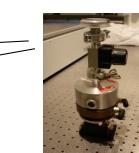
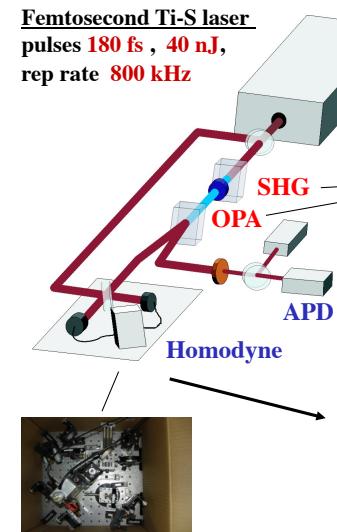
1. Continuous variable quantum cryptography : principles
2. Continuous variable quantum cryptography : implementations

Part 3 : Towards quantum networks (non-Gaussian !)

1. Entanglement for continuous variable quantum networks
2. Teleportation of Schrödinger's cats
3. Storing non-Gaussian states : single photon quantum memory

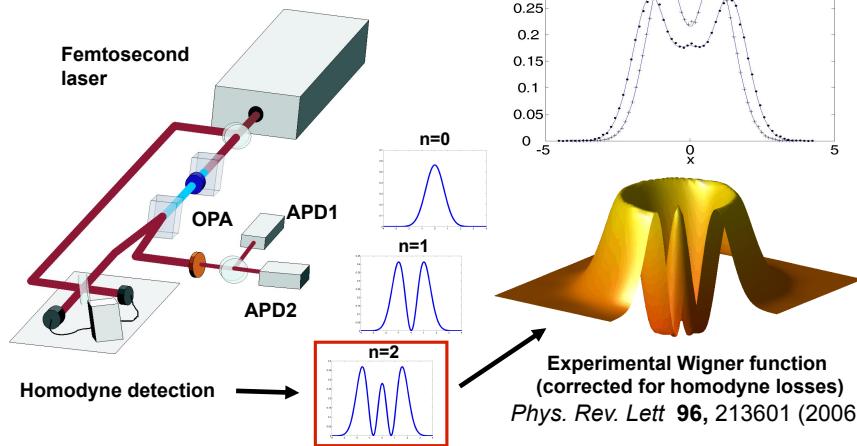


Experimental Set-up



Resource : Two-Photon Fock States

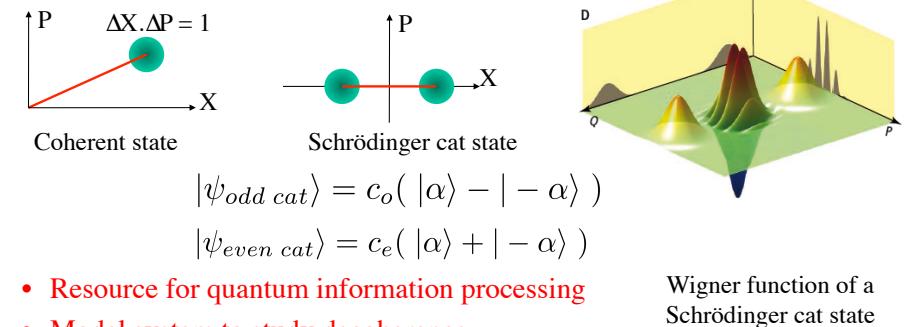
$$|\psi\rangle = \sum \lambda^n |n, n\rangle$$



« Schrödinger's Cat » state

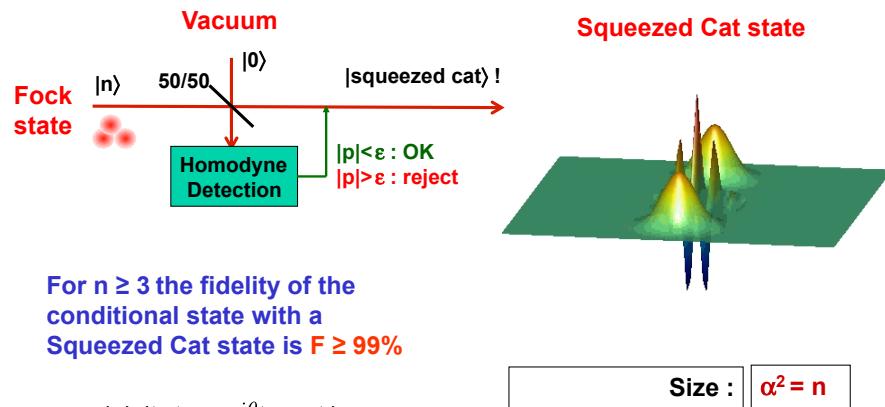


- Classical object in a quantum superposition of distinguishable states
 - “Quasi - classical” state in quantum optics : coherent state $|\alpha\rangle$

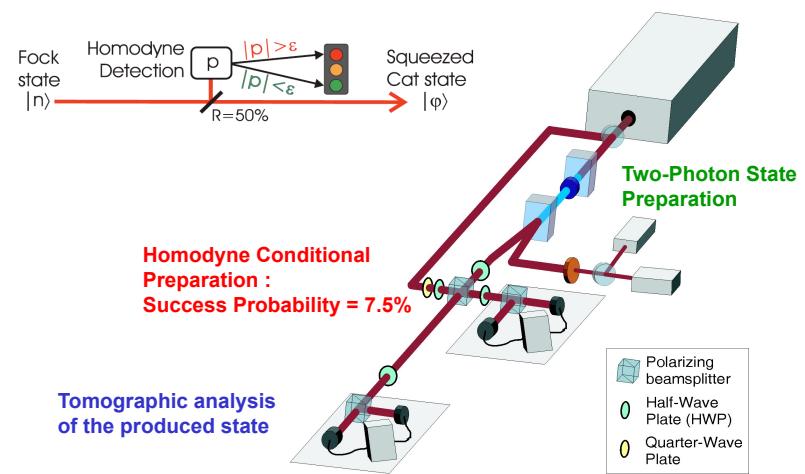


How to create a Schrödinger’s cat ?

Suggestion by Hyunseok Jeong, calculations by Alexei Ourjoumtsev :

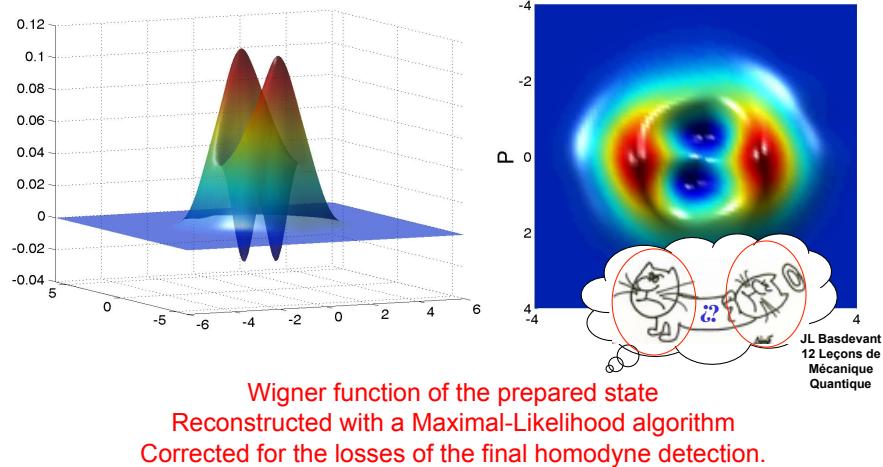


Squeezed Cat State Generation



Experimental Wigner function

A. Ourjoumtsev et al, Nature 448, 784 (2007)



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



Content of the Talk



Part 1 : Gaussian and non-Gaussian states

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

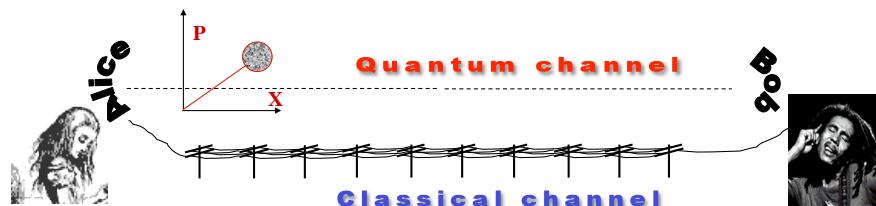
Part 2 : Continuous variable quantum cryptography (Gaussian !)

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. Teleportation of Schrödinger's cats
3. Storing non-Gaussian states : single photon quantum memory

Coherent States Quantum Key Distribution



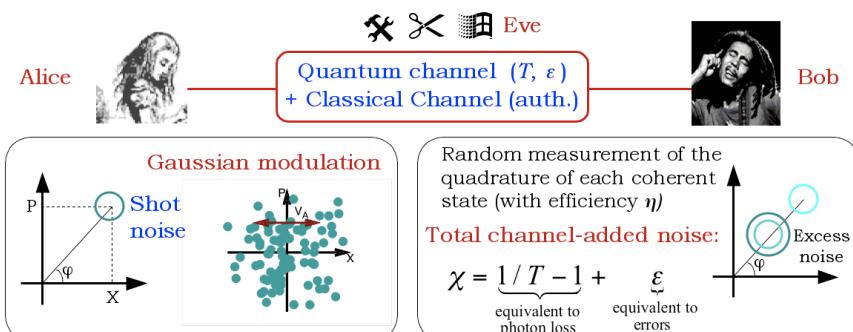
* Essential feature : quantum channel with non-commuting quantum observables
-> not restricted to single photon polarization or phase !

-> Design of Continuous-Variable QKD protocols where :

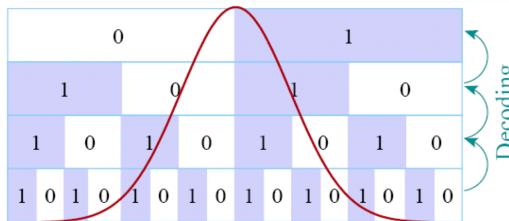
- * The non-commuting observables are the quadrature operators X and P
- * The transmitted light contains weak coherent pulses (about 10 photons) with a gaussian modulation of amplitude and phase
- * The detection is made using shot-noise limited homodyne detection

Coherent state continuous variables QKD protocol

- Key information encoded in both quadratures of a coherent state



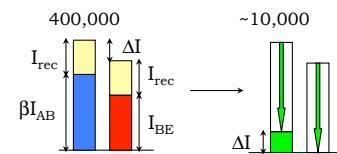
Reconciliation of correlated Gaussian variables



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

- Each level has a different error rate
- Non-independent levels
- Error correction performed using multi-level iterative soft decoding with LDPC codes

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



Security of coherent state CV-QKD protocol

- Security initially proven against (arbitrary) individual attacks :
 F. Grosshans et al, Nature 421, 238 (2003)
 F. Grosshans and N. J. Cerf, Phys. Rev. Lett. 92, 047905 (2004)
- Then security proven against arbitrary collective attacks :
 F. Grosshans, Phys. Rev. Lett. 94, 020504 (2005)
 M. Navasqués and A. Acín, Phys. Rev. Lett. 94, 020505 (2005)
- 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 χ_{BE}
 M. Navasqués et al, Phys. Rev. Lett. 97, 190502 (2006)
 R. García-Patrón et al, Phys. Rev. Lett. 97, 190503 (2006)

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

R. Renner and J.I. Cirac, Phys. Rev. Lett. 102, 110504 (2009)

Recent results :

Finite size effects : A. Leverrier, F. Grosshans and P. Grangier, Phys. Rev. A 81, 062343 (2010)
 Composable security proof : A. Leverrier, Phys. Rev. Lett. (2014)



Content of the Talk



Part 1 : Gaussian and non-Gaussian states

- Homodyne detection and quantum tomography
- Generating non-Gaussian Wigner functions : kittens, cats and beyond

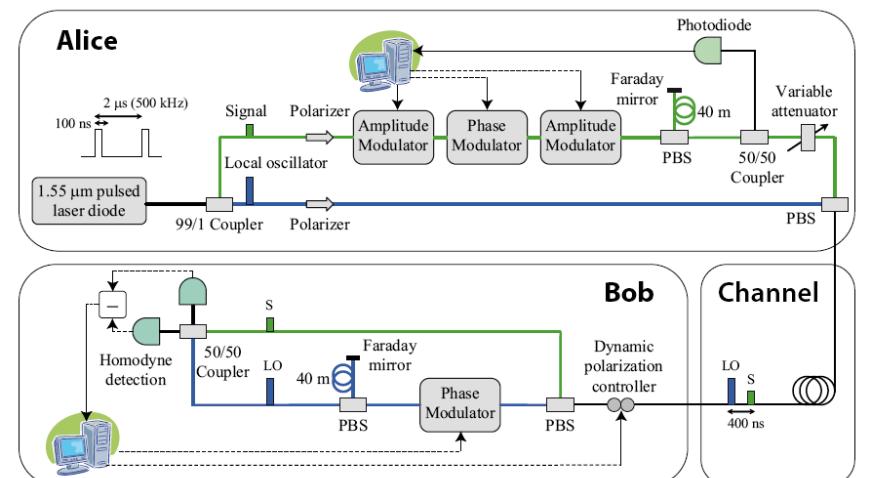
Part 2 : Continuous variable quantum cryptography (Gaussian !)

- Continuous variable quantum cryptography : principles
- Continuous variable quantum cryptography : implementations

Part 3 : Towards quantum networks (non-Gaussian !)

- Entanglement for continuous variable quantum networks
- Teleportation of Schrödinger's cats
- Storing non-Gaussian states : single photon quantum memory

All-fibered CVQKD @ 1550 nm

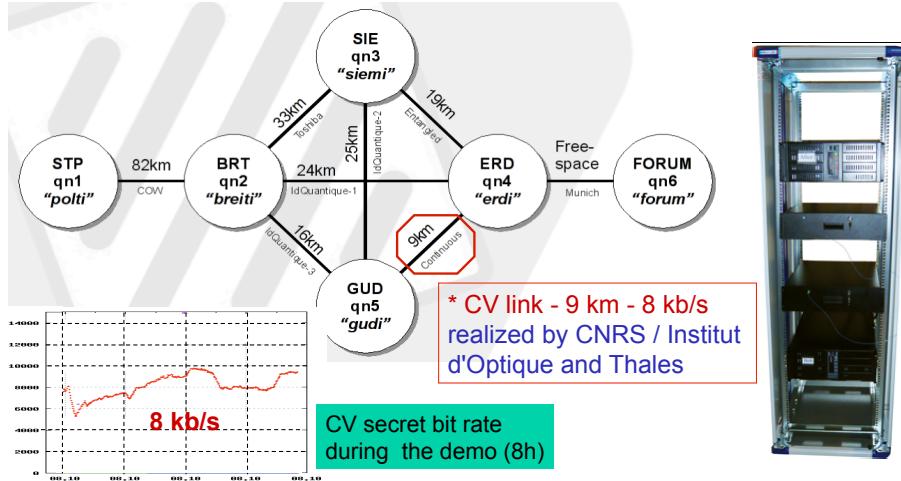


Field test of a continuous-variable quantum key distribution prototype
 S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouli and P. Grangier
 New J. Phys. 11 No 4, 04502 (April 2009)

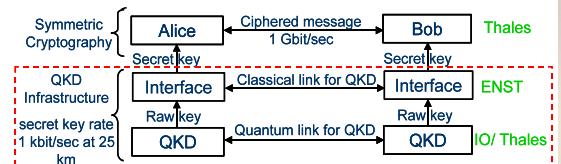
The SECOQC Quantum Back Bone



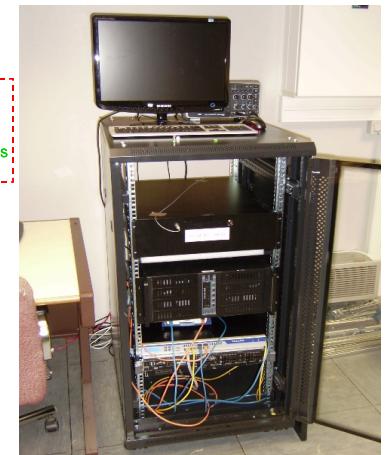
Real-size demonstration of a **secure quantum cryptography network**
by the European Integrated Project SECOQC, Vienna, 8 october 2008



Symmetric Encryption with QUantum key REnewal SEQUEURE



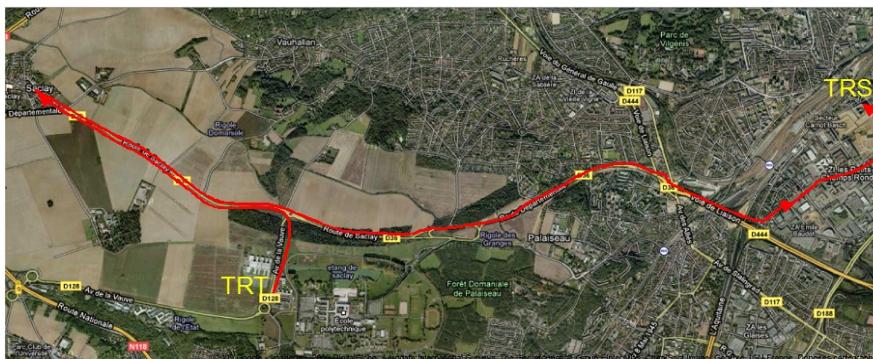
■ Thales : Mistral Gbit



SEQUURE THALES TELECOM ParisTech INSTITUT d'OPTIQUE GRADUATE SCHOOL SECURENET

Field implementation

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



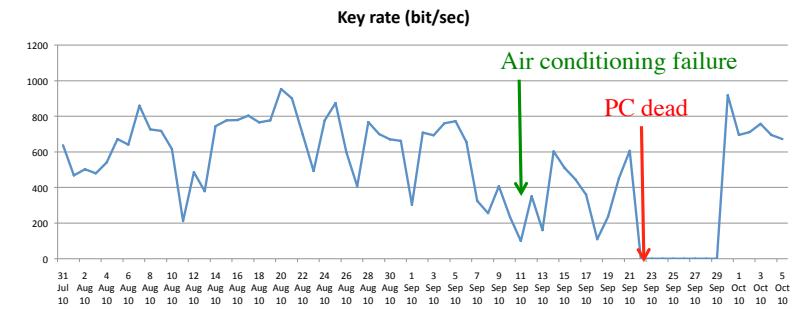
SEQUURE THALES

TELECOM ParisTech INSTITUT d'OPTIQUE GRADUATE SCHOOL

SECURENET

Results

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



See <http://www.demo-sequeure.com>

SEQUURE THALES

TELECOM ParisTech INSTITUT d'OPTIQUE GRADUATE SCHOOL

SECURENET

Post-processing at SeQureNet



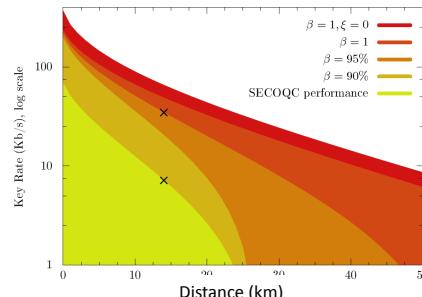
Last version (commercial device, 80 km) :
P. Jouguet et al, Nature Phot. 7, 378 (2013)

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 (80 km) !**



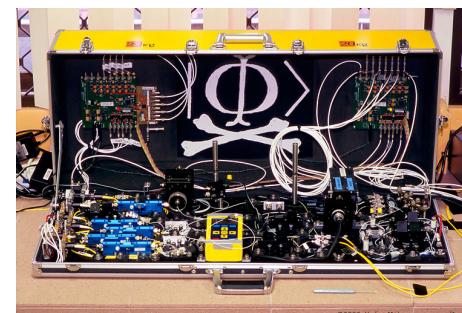
CYGNUS (commercial product)

- 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)

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

- 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 Chai, 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, Zheneshen 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)

|Φ⟩ Quantum Hacking



- 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)



Content of the Talk



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. Teleportation of Schrödinger's cats
3. Storing non-Gaussian states : single photon quantum memory

Long distance quantum communications

How to fight against line losses ?

~~Amplification~~



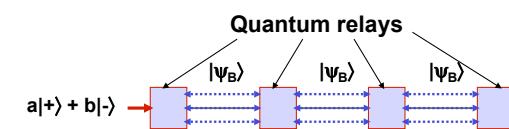
Long distance quantum communications

How to fight against line losses ?

~~Amplification~~



1. Exchange of entangled states



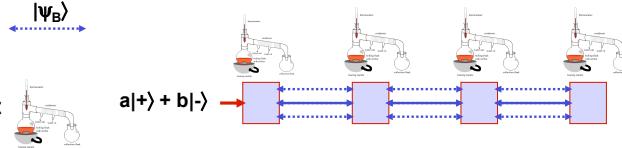
Long distance quantum communications

How to fight against line losses ?

~~Amplification~~



1. Exchange of entangled states



2. Entanglement distillation

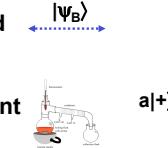
Long distance quantum communications

How to fight against line losses ?

~~Amplification~~



1. Exchange of entangled states

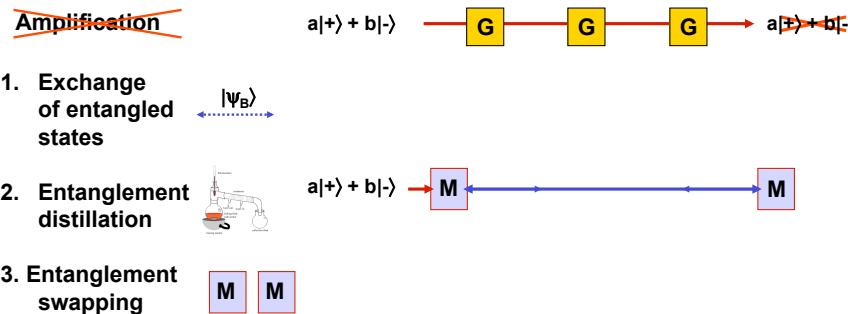


2. Entanglement distillation



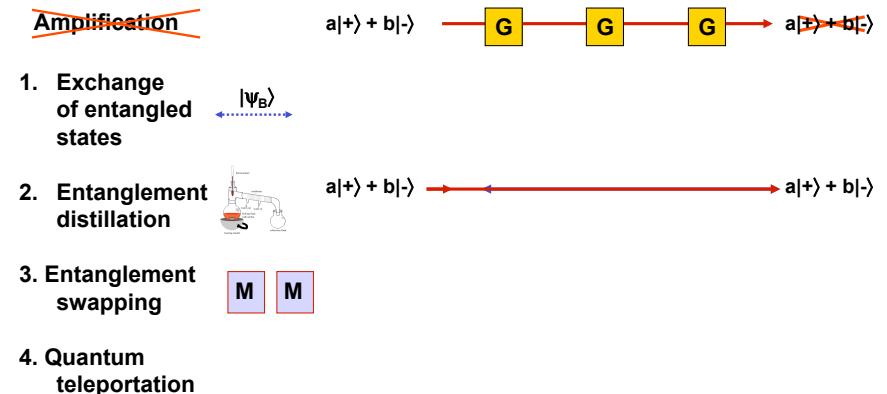
Long distance quantum communications

How to fight against line losses ?



Long distance quantum communications

How to fight against line losses ?



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



Content of the Talk



QIPC

Part 1 : Gaussian and non-Gaussian states

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

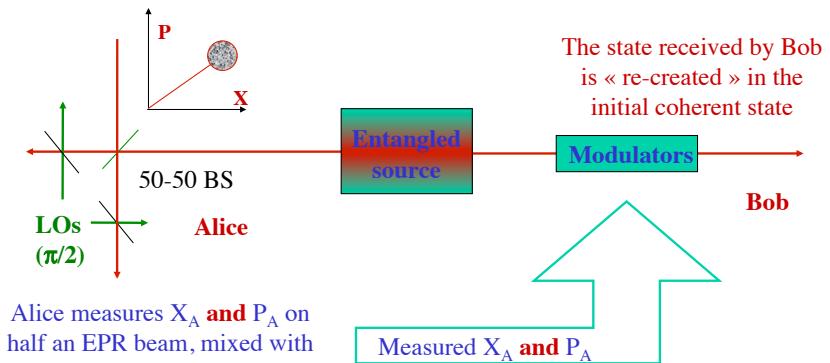
Part 2 : Continuous variable quantum cryptography (Gaussian !)

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. Teleportation of Schrödinger's cats
3. Storing non-Gaussian states : single photon quantum memory

Quantum teleportation of coherent states



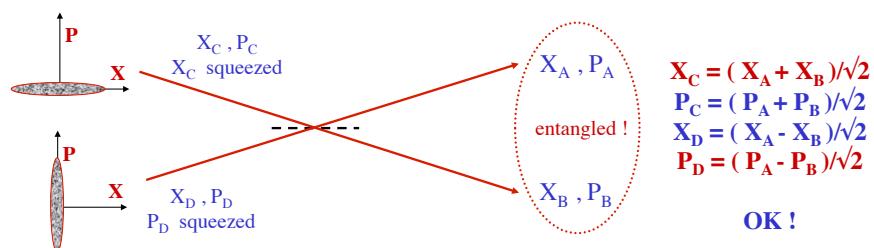
Alice measures X_A and P_A on half an EPR beam, mixed with an unknown coherent state

Experiments :

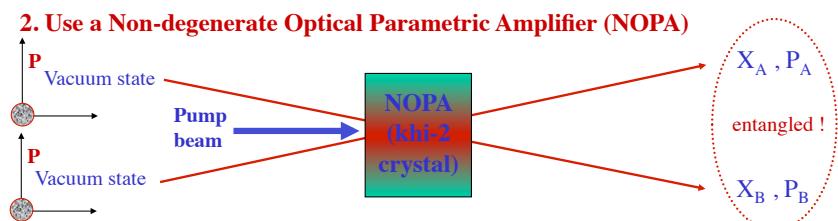
- A. Furusawa et al, Science **282**, 706 (1998)
- W. Bowen et al, Phys. Rev. A **67**, 032302 (2003)
- T.C. Zhang et al, Phys. Rev. A **67**, 033802 (2003)

How to produce CV entangled beams ?

1. Combine two orthogonally squeezed beams



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

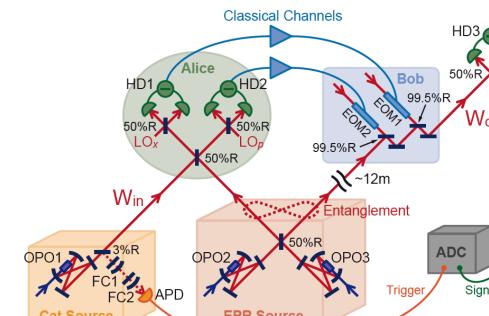


Quantum teleportation of cat states

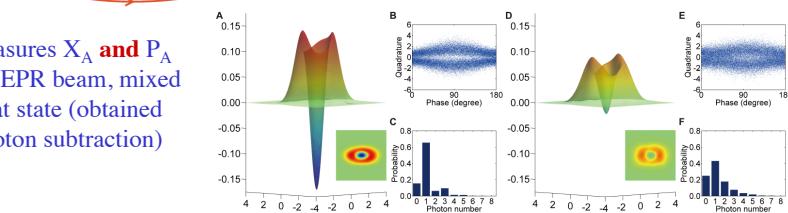
The state received by Bob is « re-created » in the initial cat state (with some loss in fidelity : $0.75 \Rightarrow 0.45$)

Experiment : N. Lee et al, Science 332, 330-333 (2011).

Remark : the initial squeezed state is CW, not pulsed !



Alice measures X_A and P_A on half an EPR beam, mixed with a cat state (obtained from photon subtraction)



Content of the Talk



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 !)

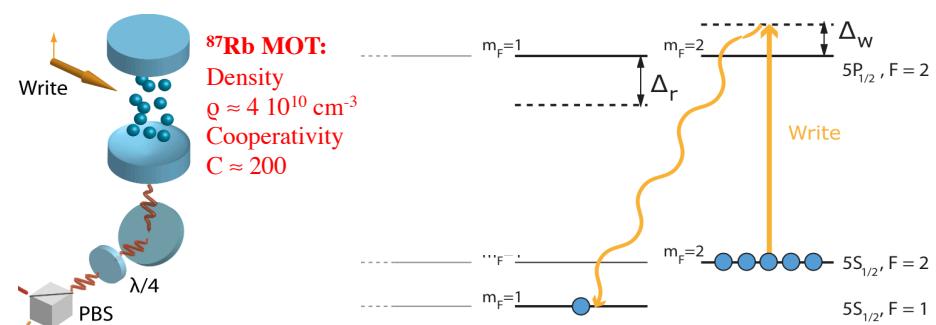
1. Continuous variable quantum cryptography : principles
2. Continuous variable quantum cryptography : implementations

Part 3 : Towards quantum networks (non-Gaussian !)

1. Entanglement for continuous variable quantum networks
2. Teleportation of Schrödinger's cats
3. Storing non-Gaussian states : single photon quantum memory

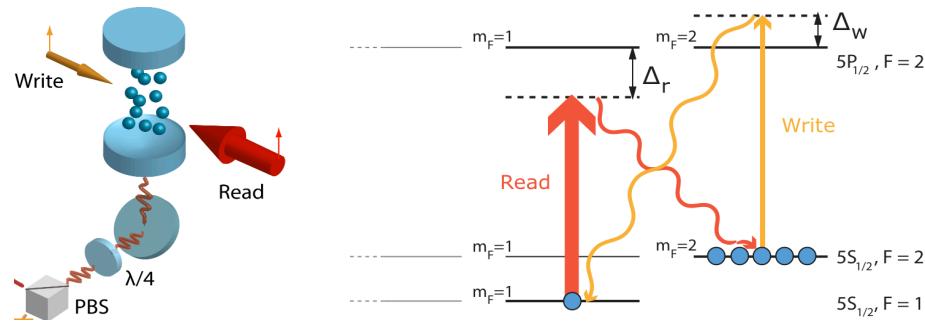
Single Photon from a single polariton (DLCZ protocol)

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



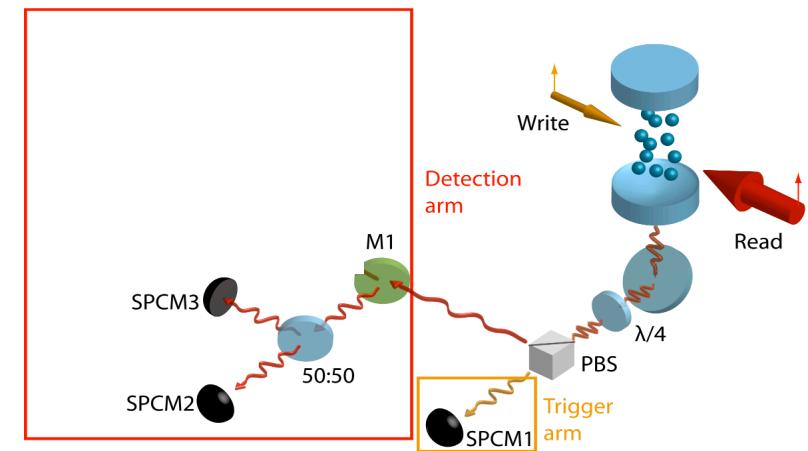
E. Bimbard et al, arXiv:1310.1228 (2013), PRL 112, 033601 (2014)

Single Photon from a single polariton (DLCZ protocol)



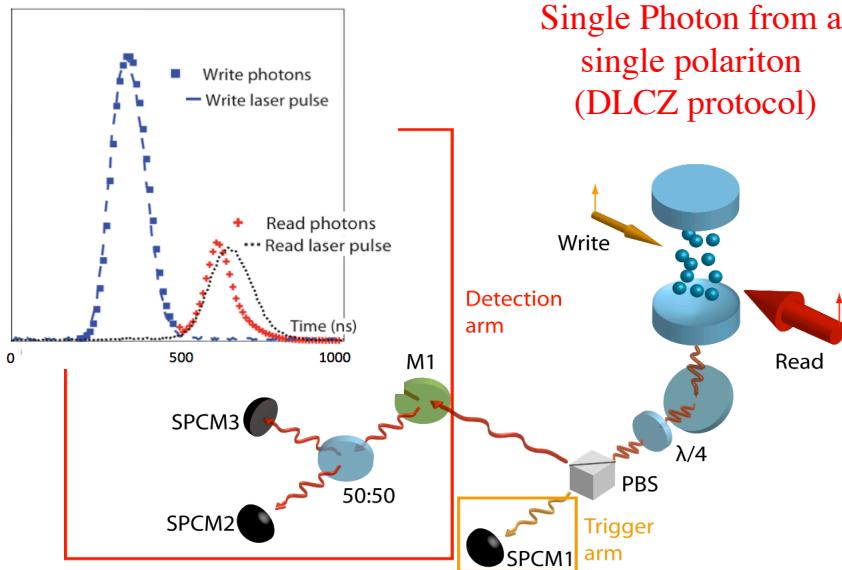
E. Bimbard et al, arXiv:1310.1228 (2013), PRL 112, 033601 (2014)

Single Photon from a single polariton (DLCZ protocol)



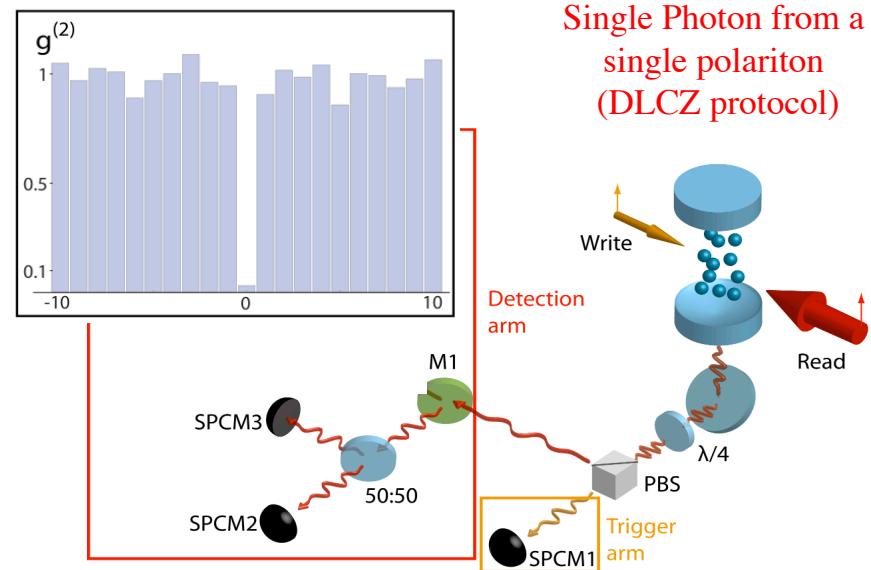
E. Bimbard et al, arXiv:1310.1228 (2013), PRL 112, 033601 (2014)

Single Photon from a single polariton (DLCZ protocol)



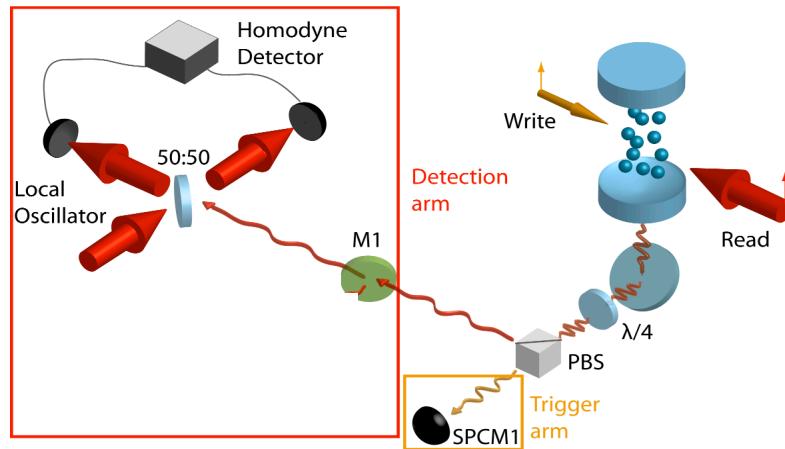
E. Bimbard et al, arXiv:1310.1228 (2013), PRL 112, 033601 (2014)

Single Photon from a single polariton (DLCZ protocol)



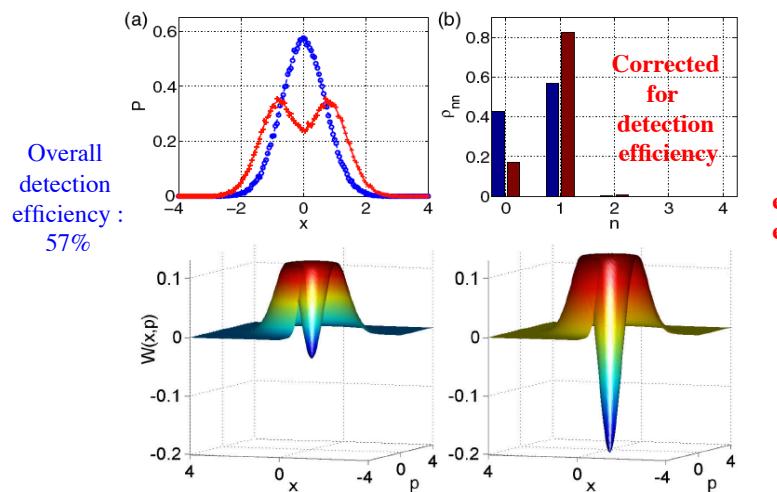
E. Bimbard et al, arXiv:1310.1228 (2013), PRL 112, 033601 (2014)

Single Photon from a single polariton (DLCZ protocol)



E. Bimbard et al, arXiv:1310.1228 (2013), PRL 112, 033601 (2014)

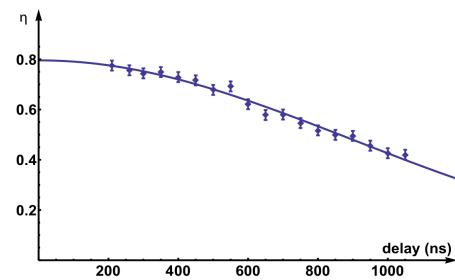
Single Photon from a single polariton (DLCZ protocol)



E. Bimbard et al, arXiv:1310.1228 (2013), PRL 112, 033601 (2014)

Single Photon from a single polariton (DLCZ protocol)

Quantum memory effect : the memory time ($1 \mu\text{s}$) is limited by motional decoherence due to finite temperature ($50 \mu\text{K}$)



$$\eta = P_{\text{Doppler}}(t) \times P_{\text{Coop}} \times P_{\text{Read}} \times P_{\text{Pumping}} \times P_{\text{Mode}} \times P_{\text{Cav}}$$

$$0.94 \times 0.97 \times 0.96 \times 0.965 \times 0.97 = 0.82 : \text{ok!}$$

E. Bimbard et al, arXiv:1310.1228 (2013), PRL 112, 033601 (2014)

Thank you for your attention !



Valentina Parigi
(post-doc, exp.)



Imam Usmani
(post-doc, exp.)



Etienne Brion
(CNRS)



Alexei Ourjoumtsev
(CNRS)



Jovica Stanojevic
(post-doc, th.)



Erwan Bimbard
(PhD, exp.)

Andrey Grankin
(PhD, th.)



Rajiv Boddeda
(PhD, exp.)

Rydberg interactions team
(Palaiseau 2014)



European
Research
Council

DELPHI
Deterministic Logical
Photon-photon Interactions