QUANTUM CRYPTOGRAPHY

QUANTUM COMPUTING

Philippe Grangier, Institut d'Optique, Orsay

1. Quantum cryptography :

   from basic principles to practical realizations.

2. Quantum computing :

   a conceptual revolution hard to materialize

Institut d'Optique

QIPC / S4P

QUANTUM CRYPTOGRAPHY

A. Beveratos[1], A. Villing[1], F. Grosshans[1], J. Wenger[1], T. Gacoin[2], N. Cerf [3], G. Van Assche[3], R. Brouri[1], J.-P. Poizat[1] and P. Grangier[1]

1 Laboratoire Charles Fabry de l'Institut d'Optique, UMR 8501 du CNRS, F-91403 Orsay Cedex

2 Laboratoire de Physique de la matière condensée, Ecole Polytechnique, F-91128 Palaiseau

3 Ecole Polytechnique, Université Libre de Bruxelles, Belgique

Overview

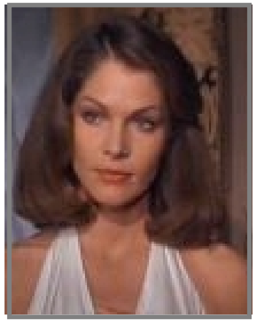
1. Basic principles of quantum key distribution
   (quantum cryptography)

2. Quantum key distribution
   using single photons « on demand »

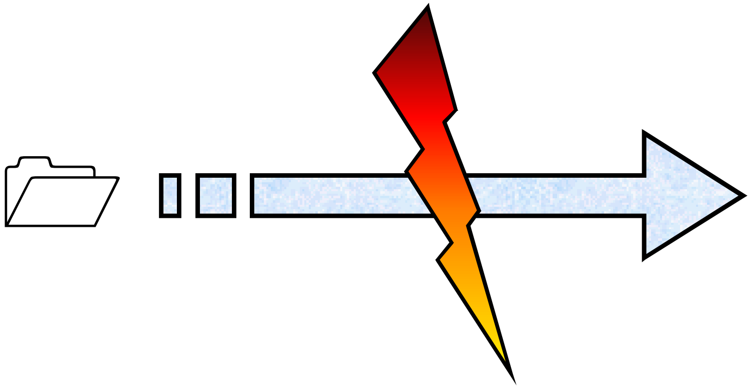
3. Quantum key distribution
   using gaussian-modulated coherent states

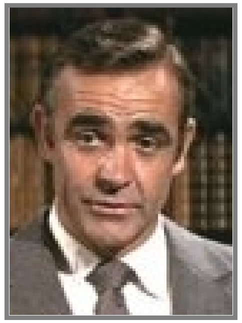
The characters

Eve



Alice

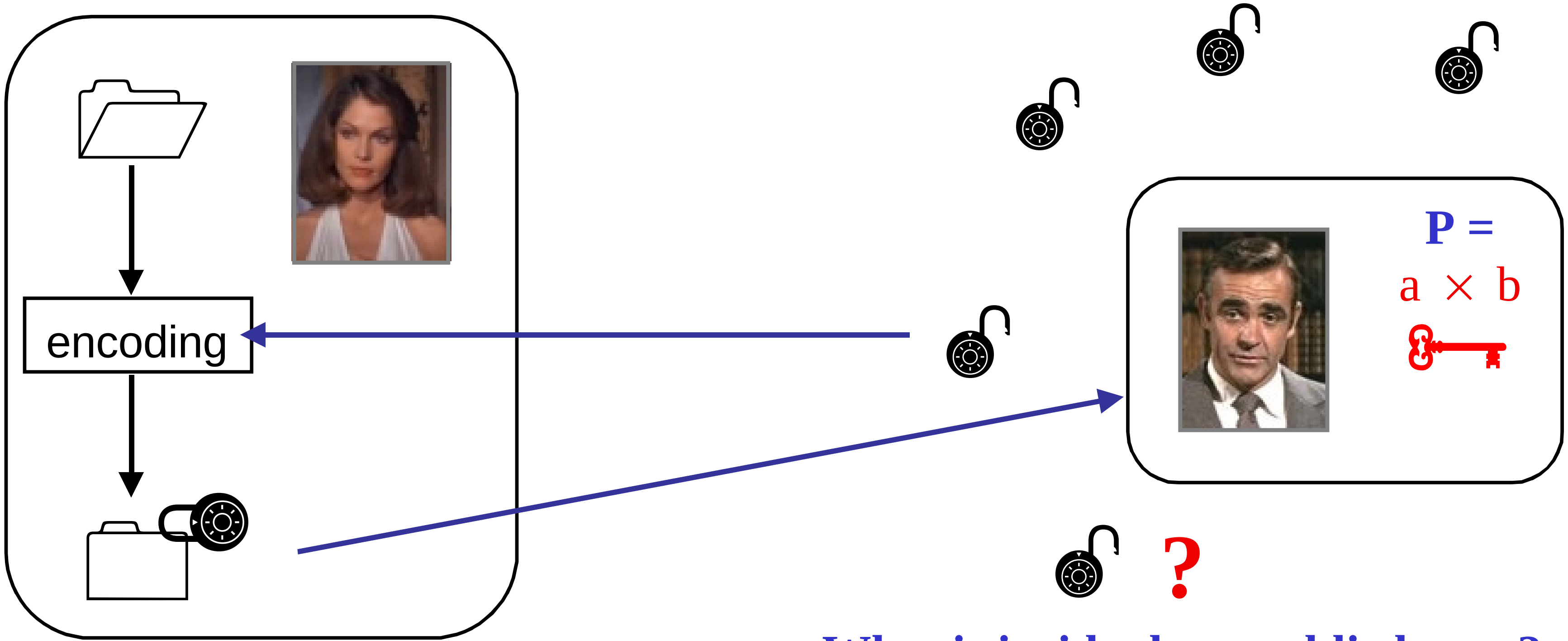




Bob

Public key cryptosystems

Rivest, Shamir et Adelman (RSA, 1978)



What is inside the « public key » ?

the product P of two large numbers :

factorization very difficult to perform !

Factorisation de RSA 155 (512 bits - été 1999)

"Enigme" proposée par la compagnie RSA (www.rsa.com)
Record précédent : RSA140 (465 bits), février 1999

RSA155 = 109417386415705274218097073220403576120037329454492\
059909138421314763499842889347847179972578912673324976257528\
997818337970765372440271467435315933543338 97;

RSA155 n'est pas premier ! (calcul "probabiliste" très rapide)

Factorisation ?	**Préparation :**	9 semaines sur 10 stations de travail.
	Criblage :	3.5 mois sur 300 PCs , 6 pays
	Résultat :	**3.7 Go, stockés à Amsterdam**
	Filtrage :	9.5 jours sur Cray C916, Amsterdam
	Factorisation:	39.4 heures sur 4 stations de travail

f1 = 102639592829741105772054196573991675\
900716567808038066803341933521790711307779;
f2 = 106603488380168454820927220360012878\
679207958575989291522270608237193062808643;

f1 et f2 sont premiers, et f1 * f2 = RSA155 (calcul immédiat sur PC)

PUBLIC KEY CRYPTOSYSTEMS

- Problems :

- Mathematical demonstrations about PKC have a statistical character (the factorisation may be found easily for "unfortunate choices" of a, b)

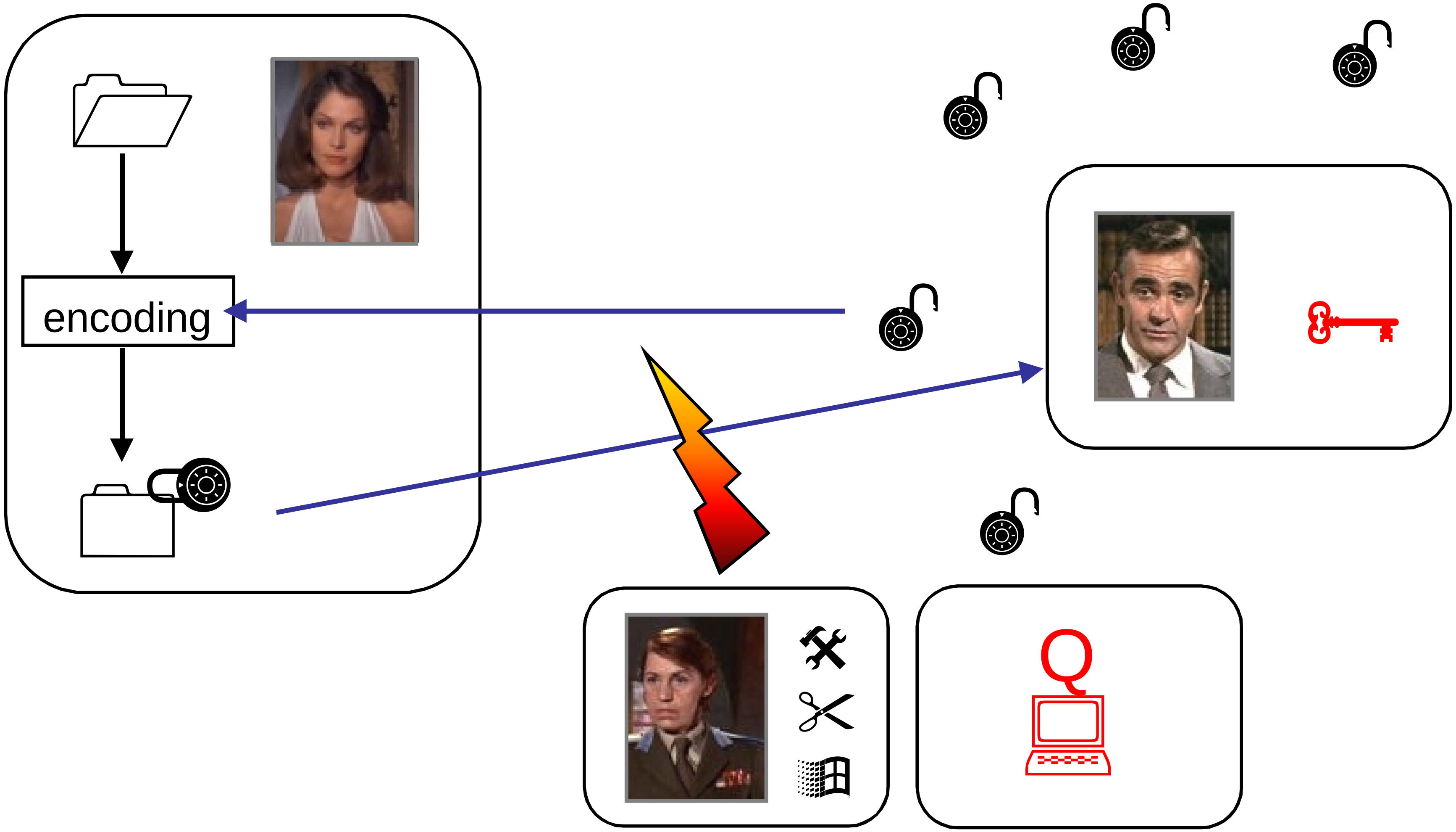
  --> "recommendations" for the choice of the prime numbers a and b

- **No absolute demonstration for security** -> better computers, better algorithms (obviously kept secret) ?

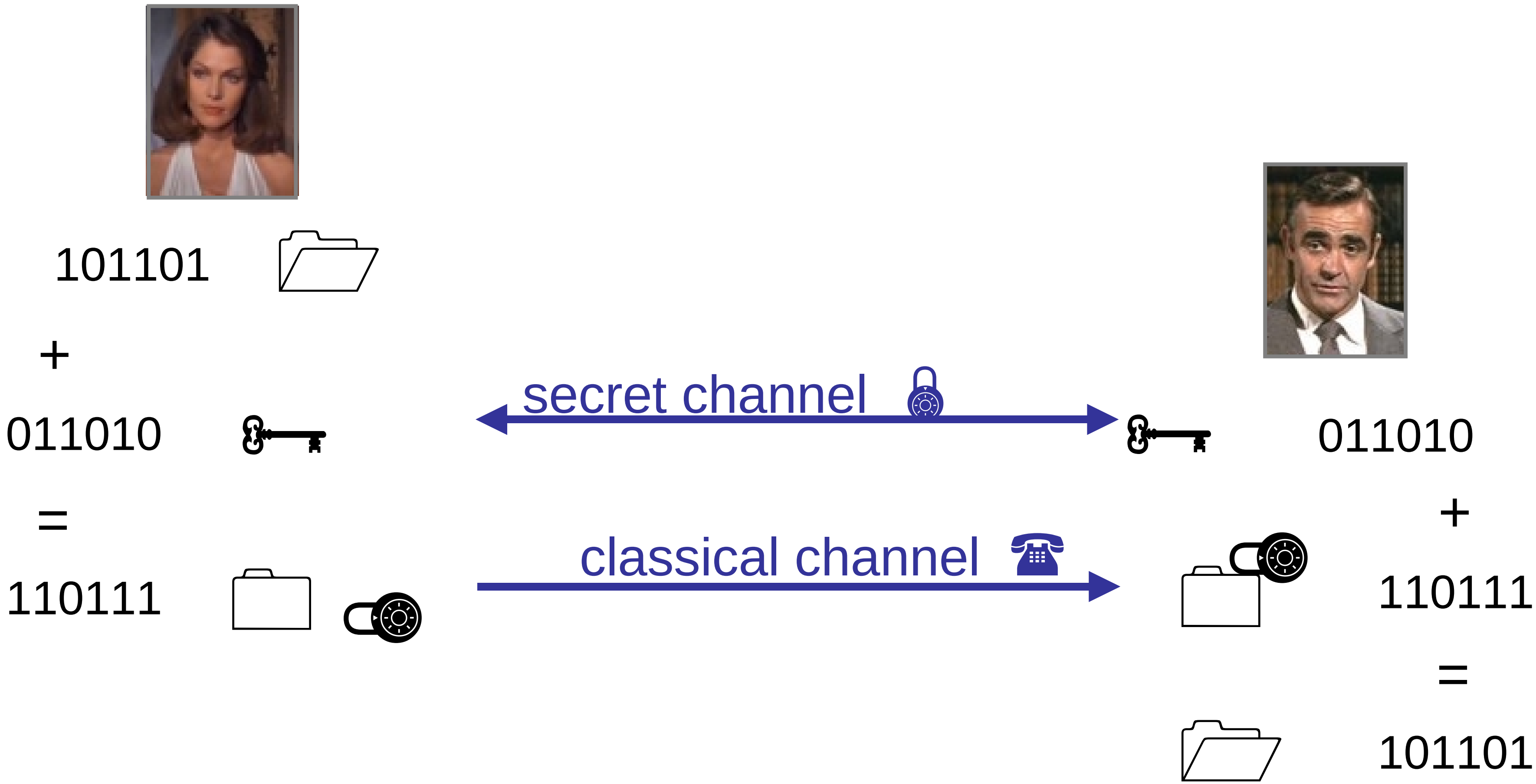
- Article by Peter Shor (1994) :

a "quantum computer" might be able to factorize the product of two prime numbers in a "polynomial" time ! *lot of reactions !*

Public key cryptosystems (1970)



Secret key cryptosystem :
one-time pad (G. Vernam, 1917)



CRYPTOGRAPHY :
FROM VERNAM'S CYPHER TO QUANTUM MECHANICS

- Shannon's demonstration (1940)

Vernam's cypher cannot be broken, provided that the list of random numbers is as long as the message, and is used only one time ("one-time pad").

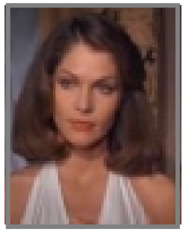
- Difficult to implement...

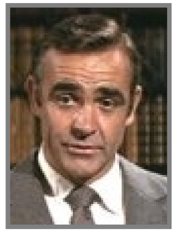
The one-time pad is used for military-type purposes. For commercial purposes one uses shorter keys but more complex processing (e.g. : "Data Encryption Standard" : 56 random bits used over a limited period in time).

- Problem of "secret key" cryptosystems :

Transmission of the key (the messenger may be corrupted...) "Classical" attacks are physically possible -> **quantum cryptography.**

Quantum Secret Key Cryptosystem :
Bennett-Brassard (1984)





101101

+

011010

=

110111

quantum channel ☯

classical channel ☎

011010

+

110111

=

101101

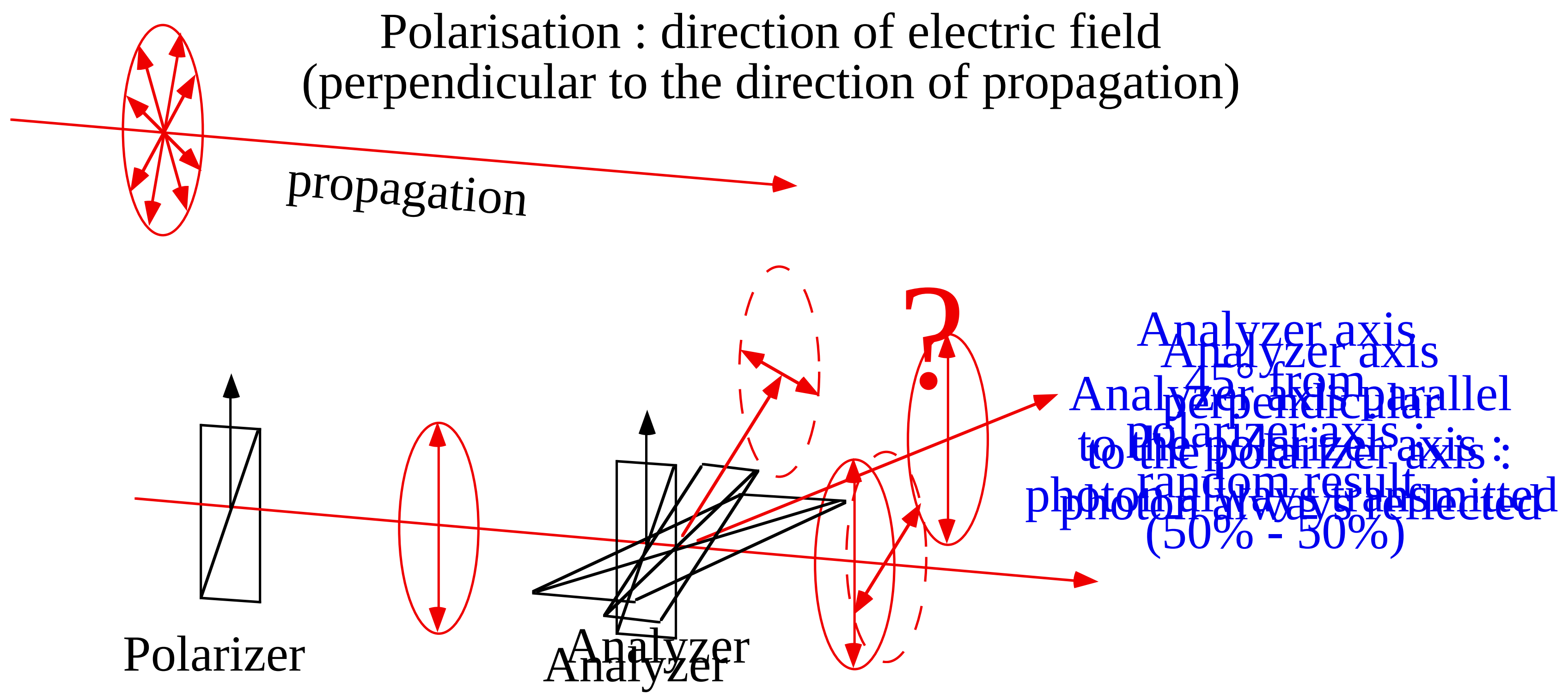
Demonstrably secure if the key is :

- random
- as long as the message
- used only once (Shannon)
- **unknown by Eve : Quantum laws !**

QUANTUM CRYPTOGRAPHY : PRINCIPLE

Goal : sending a "secret key" by using the laws of physics to warrant the complete security of the transmission

Method : light pulses, ideally "photons" (light quanta with energy E = h ν)

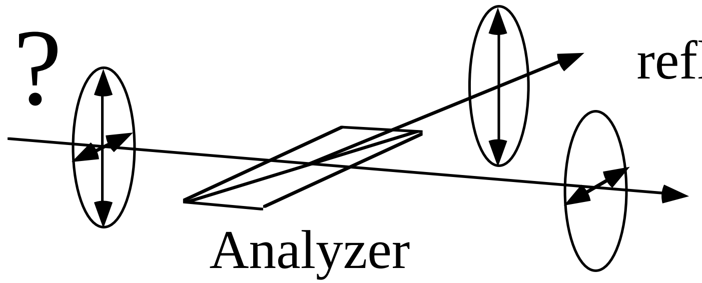


QUANTUM CRYPTOGRAPHY : PRINCIPLE

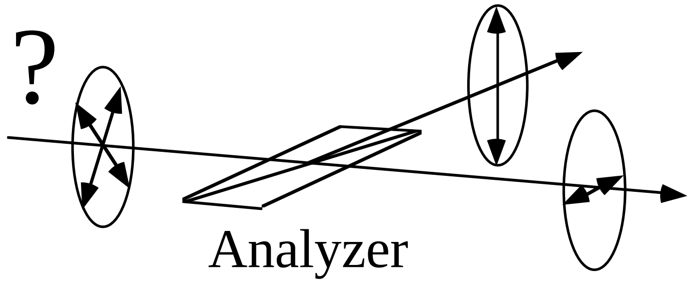
Crucial point :

- in all cases there are two analyzer outputs : "transmitted" or "reflected"

- detecting the photon in one output gives the direction of the polarizer axis **if this axis is paraller or perpendicular to the analyzer axis**



- when the polarizer is oriented in another direction with respect the analyzer, the result is random (50 % - 50 % for 45° relative angle)



detecting the photon **does not give any information** about the initial polarisation, and moreover **destroys the initial information**

QUANTUM CRYPTOGRAPHY : PRINCIPLE
(C. Bennett and G. Brassard, 1984)

1 - Alice sends random "bits" (0 ou 1) encoded in two 2 different "basis"

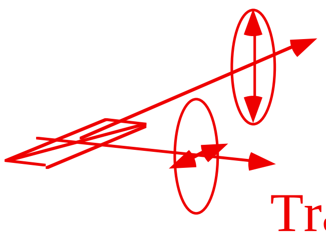
0° : bit "0", basis "+"

90°: bit "1", basis "+"

135° : bit "0", basis "×"

45° : bit "1", basis "×"

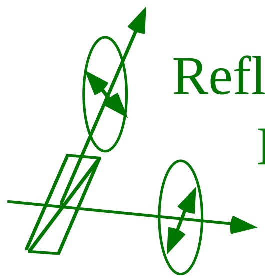
2 - Bob randomly chooses either the "+" or the "×" basis and records the transmitted and reflected photons (giving "1" et "0" if basis ok)



Reflected (0°) ->"0"

Basis "+"

Transmitted (90°) ->"1"



Reflected (135°) ->"0"

Basis "×"

Transmitted (45°) ->"1"

3 - Bob announces openly his choice of basis (but not the result !) and Alice answers "ok" or "no". Bits with different basis are discarded.

4 - The remaining bits give the secret key

QUANTUM CRYPTOGRAPHY : PRINCIPLE
(C. Bennett and G. Brassard, 1984)

Alice Basis	Alice Bit	Eve ! Basis	Eve ! Bit	Bob Basis	Bob Bit	
+	1	×	0	+	1 / 0	ok-> 1 / error !
+	0	+	0	×	0	no
×	1	+	1	×	1	ok-> 1
×	0	×	0	+	1	no
×	1	+	0	+	0	no
+	0	+	0	+	0	ok-> 0
+	1	+	0	×	0	no
×	0	+	1	×	0 / 1	ok-> 0 / error !
×	1	×	0	+	1	no
×	0	+	0	+	0	no

QUANTUM CRYPTOGRAPHY : PRINCIPLE
(C. Bennett et G. Brassard, 1984)

*** Result of the transmission protocol:**

- "raw key" exchanged between Alice and Bob
- Alice and Bob measure the error rate by comparing a part of the raw key:

  -> evaluation of the amount of information (maybe) available to Eve.

*** Error correction and privacy amplification** (classical algorithms) :

- the errors are corrected (this reduces the size of the key)

(ex : block parity tests + bissection)

- Eve's residual knowledge is eliminated (this reduces the size of the key)

(ex : hashing functions)

- The size of the remaining key is non-zero if the error rate was $< 15\%$

6 - Alice and Bob have a totally secure and errorless secret key.

Questions...

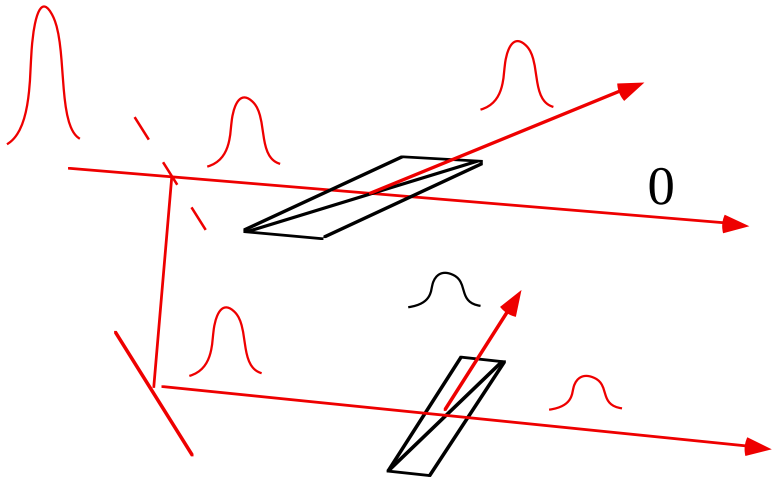
What is quantum in quantum cryptography ?

How to implement that idea in practice ?

QUANTUM CRYPTOGRAPHY : PRINCIPLE

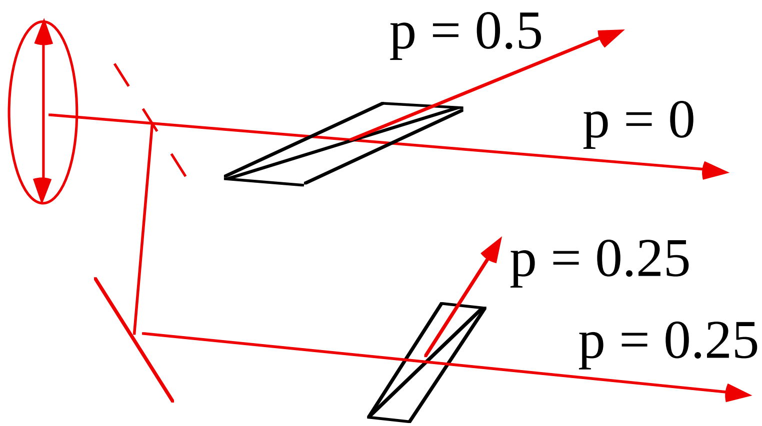
Light pulse
- the polarisation of a light pulse can be measured easily (use a beamsplitter with R = T = 50%)

p(good result) = 1



Single photon
- a single photon is detected only once, and the initial polarization cannot be obtained with certainty

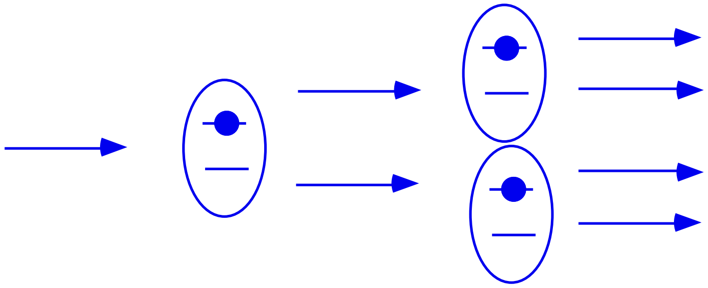
p(good result) = 0.5



SINGLE PHOTON VS LIGHT PULSE

Question : Is it possible to "clone" the polarization state of a photon ?

$| 1: u > \longrightarrow \; | 1: \; u > \otimes | 2: u > \otimes | 3: \; u > \otimes .... \otimes | N: u >$



etc...

Answer : No !

Two arguments : - formal demonstration ...

- "physically forbidden" consequences

"CLONING" A QUANTUM STATE ?

Linearity of quantum mechanics :

$$|\varphi_n\rangle_1 \; |\psi\rangle_2 \quad \Rightarrow \quad |\varphi_n\rangle_1 \; |\varphi_n\rangle_2$$

$$|\varphi_m\rangle_1 \; |\psi\rangle_2 \quad \Rightarrow \quad |\varphi_m\rangle_1 \; |\varphi_m\rangle_2$$

$$\left(\frac{|\varphi_n\rangle_1 + |\varphi_m\rangle_1}{\sqrt{2}} \right) |\psi\rangle_2 \quad \Rightarrow \quad \frac{|\varphi_n\rangle_1 \; |\varphi_n\rangle_2 \; + \; |\varphi_m\rangle_1 \; |\varphi_m\rangle_2}{\sqrt{2}}$$

but one would like :

$$\left(\frac{|\varphi_n\rangle_1 + |\varphi_m\rangle_1}{\sqrt{2}} \right) \; |\psi\rangle_2 \quad \Rightarrow \quad \left(\frac{|\varphi_n\rangle_1 + |\varphi_m\rangle_1}{\sqrt{2}} \right) \left(\frac{|\varphi_n\rangle_2 + |\varphi_m\rangle_2}{\sqrt{2}} \right)$$

Contradiction !

* Cloning is possible if { $|\varphi_n>$, $|\varphi_m>$ } are orthogonal
(then direct measurement is also possible)

* Cloning is impossible for a set of non-orthogonal states: **ok for cryptography**

WHAT IS QUANTUM
IN QUANTUM CRYPTOGRAPHY ?

- It it impossible to copy an arbitrary quantum state chosen among a set of non-orthogonal states : **"no-cloning theorem"**

  (demonstration : strongly related to the Heisenberg relations)

- Beyond its consequences for the security of quantum cryptography, cloning would have other unacceptable consequences :

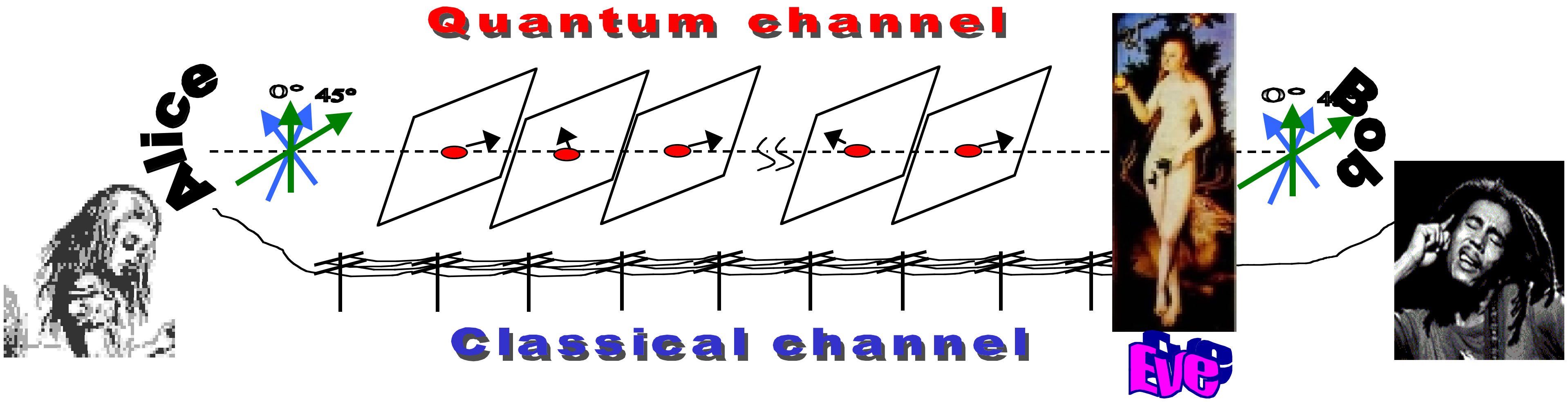
    - violation of Heisenberg's relations ...

    - conflict between Quantum Mechanics and Special Relativity ...

- The security of quantum cryptography is deeply rooted in quantum laws !

Photon Counting Quantum Key Distribution

QIPC



Quantum Key Distribution (QKD) protocol :

* Alice encodes bits onto non-orthogonal states of a stream of single photons

* Bob detects the photons, and then Alice and Bob agree on the measurement basis.

* Any attempt by Eve to measure or copy information the quantum channel will induce perturbations (errors) that can be evaluated by Alice and Bob

-> As long as the error rate is not too big, Eve's knowledge can be reduced to zero by privacy amplification.

EXPERIMENTAL QUANTUM CRYPTOGRAPHY

Hugo Zbinden, "Introduction to quantum computation and information", World Scientific, p. 120 (1998)

Wavelength (detector)	800nm (Si)	1300nm (InGaAs)	1300 nm (InGaAs)	1300 nm (InGaAs)	1500nm (InGaAs)
Temperature ηdet Pdark (w :1ns) Att (dB/km)	Peltier 50% 10^{-8} 2.0	LN2 20% $3\ 10^{-6}$ 0.35	LN2 30% $10\ 10^{-6}$ 0.35	Peltier 10% $20\ 10^{-6}$ 0.35	Peltier 2% $10\ 10^{-6}$ 0.2
QBER (2 km) R (2km)	0.00006% 79 kHz	0.02% 82 kHz	0.04% 123 kHz	0.25% 27 kHz	0.56% 9 kHz
QBER (25km) R (25km)	0.2% 25 Hz	0.12% 13 kHz	0.25% 20 kHz	1.5% 6.7 kHz	1.6% 3.2 kHz
QBER (50km) R (50km)		0.93% 1.8 kHz	1.9% 2.7 kHz	11% 0.9 kHz	5% 1 kHz
D[QBER=15%] R(D km)	29 km 0.3 Hz	84 km 110 Hz	76 km 330 Hz	54 km 670 Hz	74 km 333 Hz

10 MHz clock, attenuated light pulses $P(n\geq 1) = 0.1$

id Quantique

A quantum leap for cryptography

QUANTUM KEY DISTRIBUTION (QKD)

Key distribution is a central problem in cryptography. Currently, public key cryptography is commonly used to solve it. However, these algorithms are vulnerable to increasing computer power. In addition, their security has never been formally proven.
Quantum cryptography exploits a fundamental principle of quantum physics - observation causes perturbation - to distribute cryptographic keys with absolute security. id Quantique is introducing the first quantum key distribution system, which exchanges keys over standard optical fibers.

Main features

- First commercial quantum key distribution system
- Key distribution distance: up to 60 km
- Key distribution rate: up to 1000 bits/s
- Compact and reliable

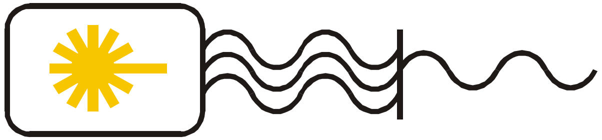
id Quantique

10, rue Cingria 1205 Genève Switzerland

http://www.idquantique.com

QKD with Attenuated Light Sources

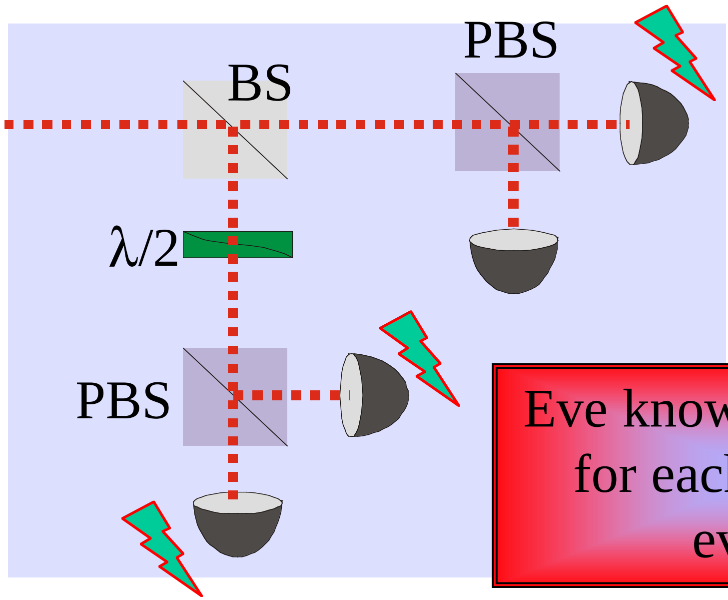
Usual QKD : Pulsed Attenuated Laser



☹ Poissonian Statistics with $p(1) << 1$:

$$\mathbf{p(2) = p(1)^2 / 2}$$
$$\mathbf{p(3) = p(1)^3 / 6}$$

Alice
4-states
BB 84
(polarization encoding)



☹ The line is totally unsecure unless one has $p(1)^2/16 < \eta$!

20 dB loss : $p(1) < 0.4$

30 dB loss : $p(1) < 0.13$

Eve knows everything for each 3-photon event !

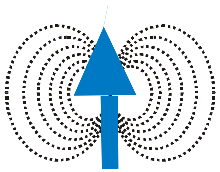
Bob is easily cheated !

☹ $pccc = p(1)^3/16 = \eta\ p(1)$

Single Photon Sources

Elimination of multiple photon events : Single photon source

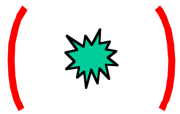
Pulsed Single Emitter



☺ Subpoissonian Statistics:

$$p(2) = c_N(0)\,\frac{p(1)^2}{2}$$

☺ $\boldsymbol{c_N(0) << 1}$



Single atom or ion in a cavity

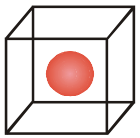
Molecule, nanocrystallites

☹ Photobleaching, blinking

Quantum Dot

☺ Narrow Spectrum

☹ T = 4K

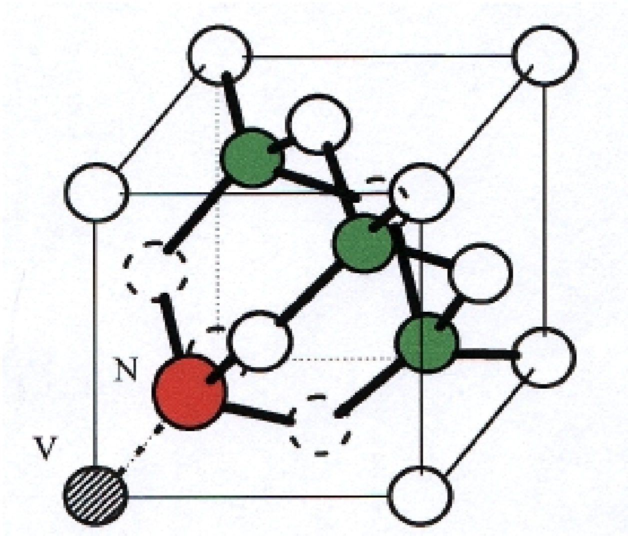


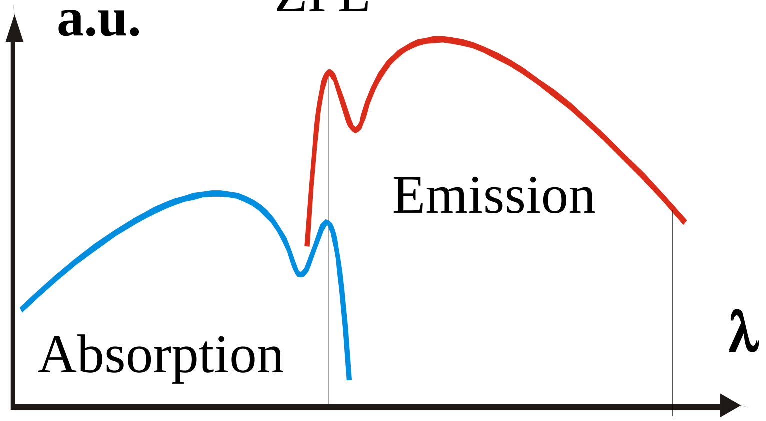
Color Centers

☺ Stable at Room Temperature

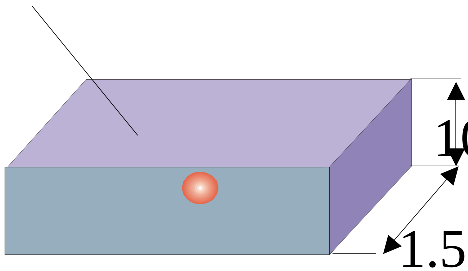
☺ Easy to Produce

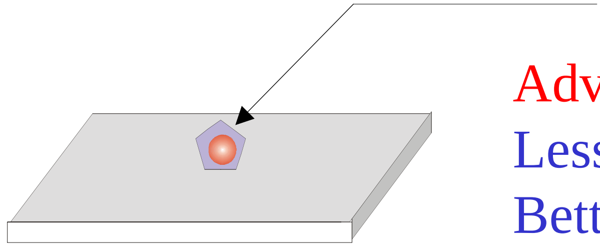
NV-Centers in diamond





Bulk or Nanocrystals





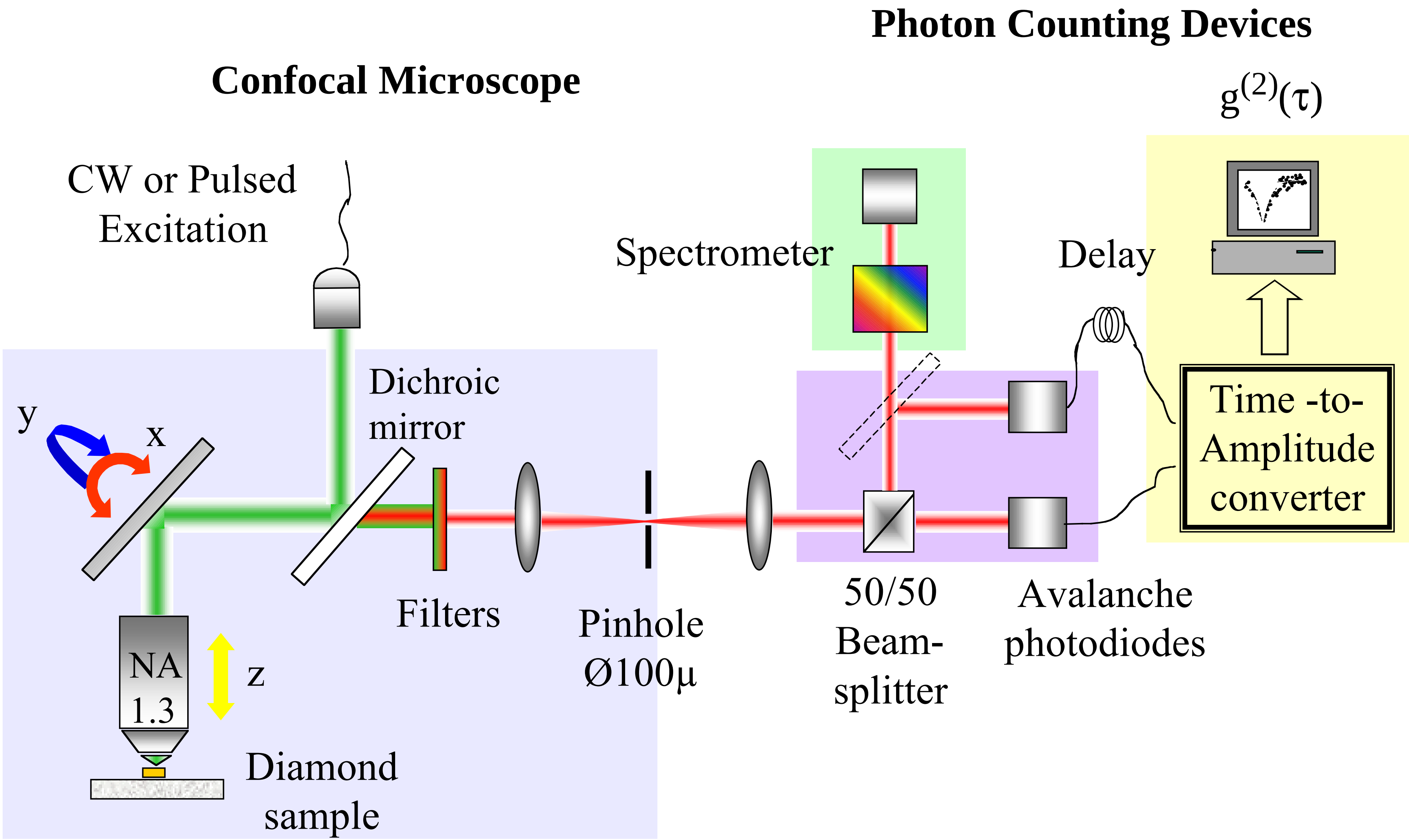
Advantages :

Less background

Better collection

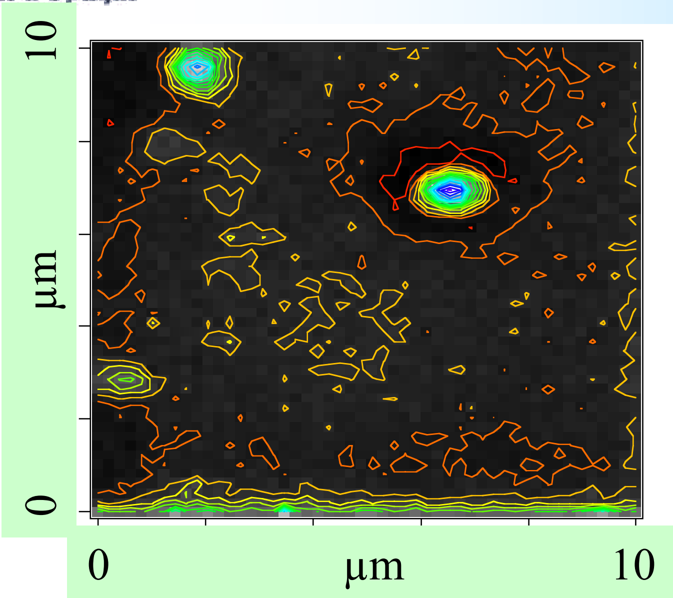
Easier to handle

Experimental Setup



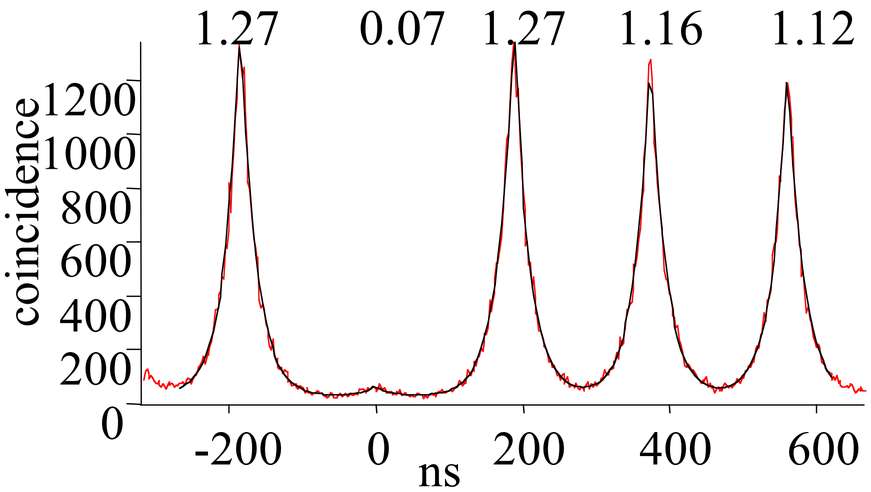
Pulsed excitation of the NV center

QIPC / S4P



Scan of the sample (10 x 10 µm)

The background light is reduced by photobleaching of the dielectric mirror (only the NV center survives !)



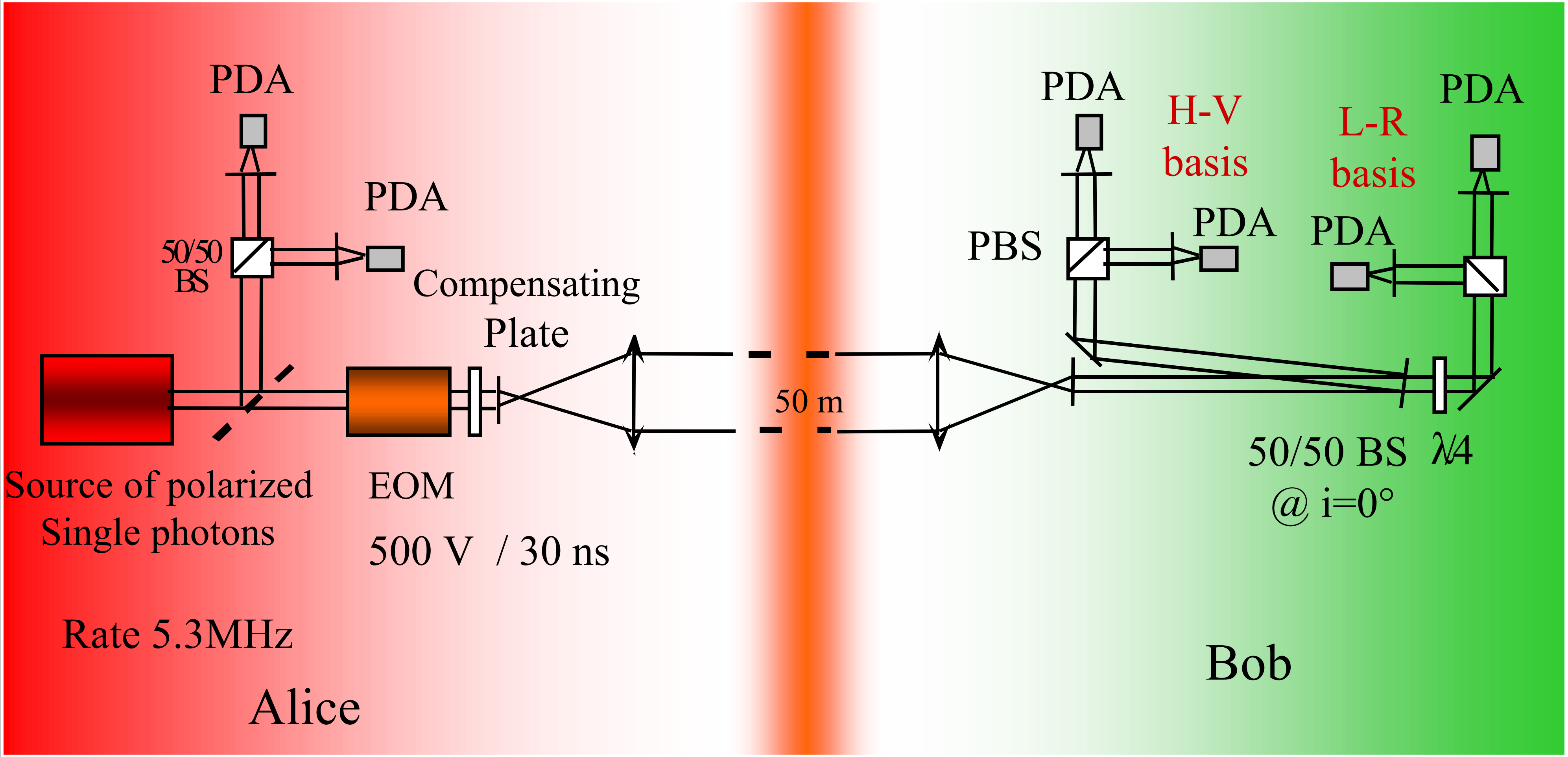
Excitation rate 5.3 Mhz

Useful single photon emission rate : 116 kcps

Global emission efficiency : 2.2 %

$$C_N(0) = 0.07 = 1/14.2$$

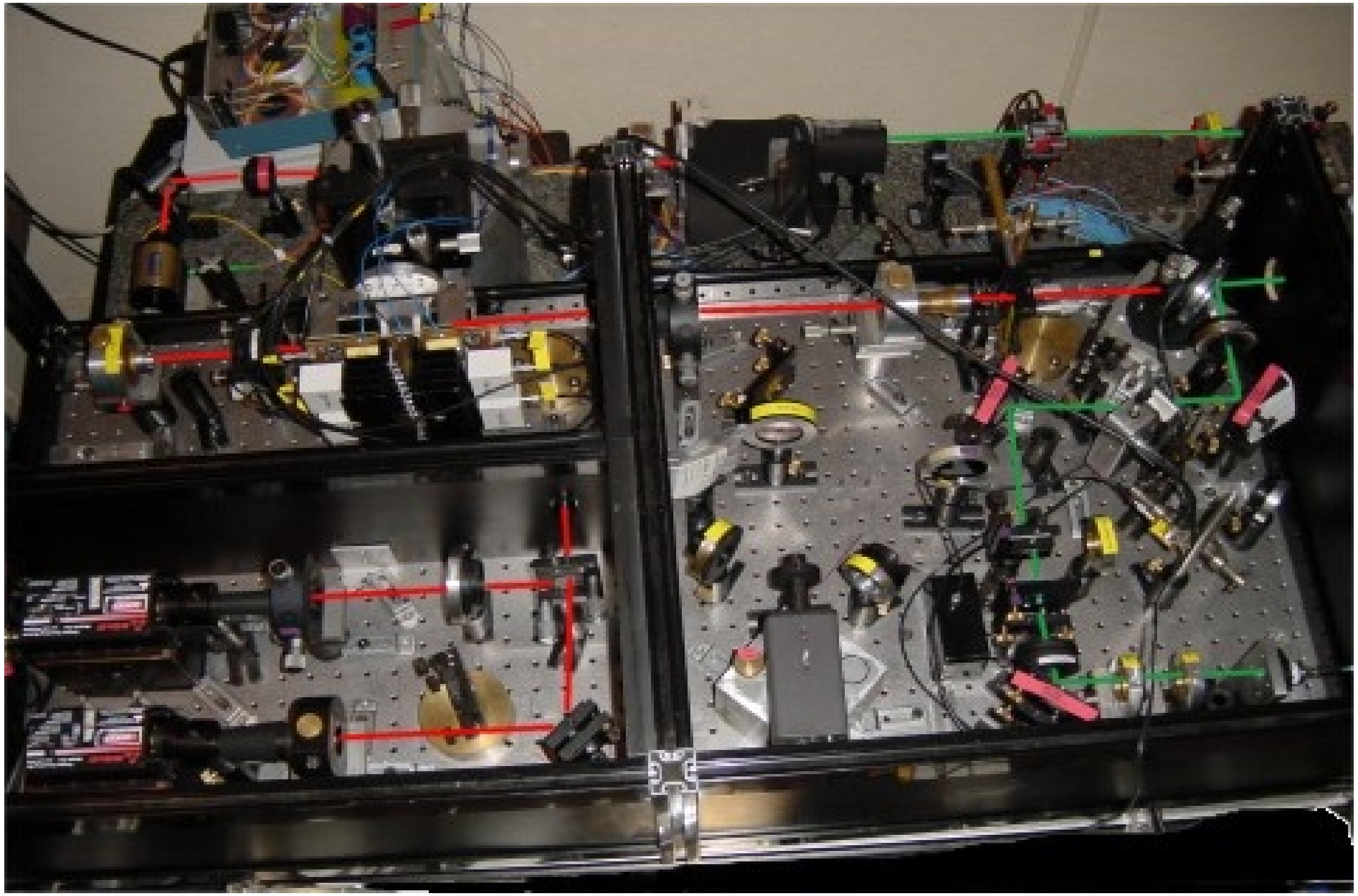
Quantum cryptography demonstrator
A. Beveratos et al, PRL **89**, 187901 (2002)



Institut d'Optique

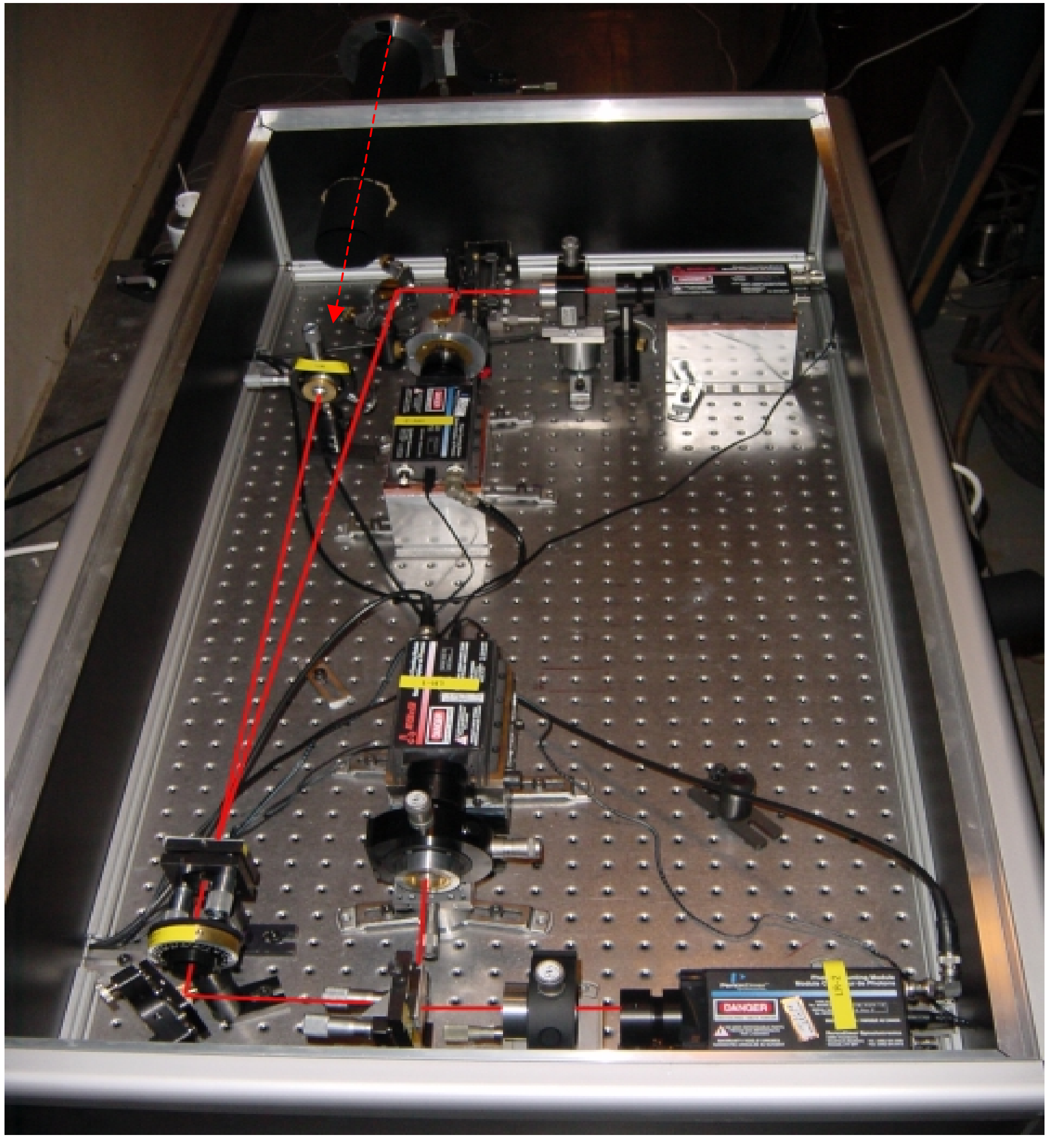
Alice

QIPC / S4P



Bob

QIPC / S4P



Alice & Bob (50 m away)

QIPC / S4P

Quantum Key Distribution : Results (part of the transmitted key)

QIPC / S4P

Alice

1011011110101000111010000001011100010
111110111010000011110001010101111111000

Bob

1011011100101000111011000001011100110
111111011101000011111010101111111111000

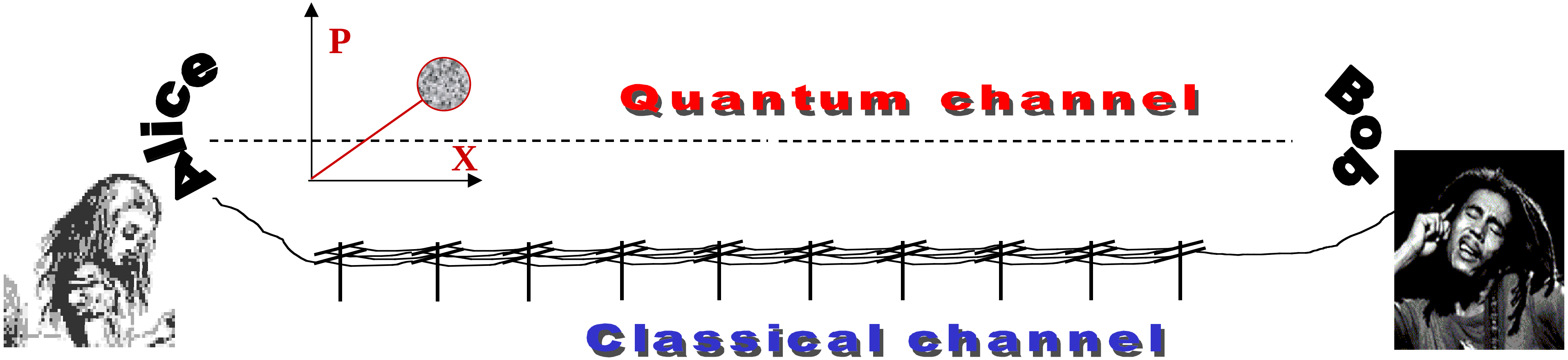
8000 secret bits /s after error correction and privacy amplification (software « QUCRYPT », Louis Salvail)

see : http://www.cki.au.dk/experiment/qrypto/doc/

Evaluations of maximum tolerable transmission losses based on security analysis by N. Lütkenhaus, PRA 61, 052304 (2000)

Measurable advantage for this single photon source

Coherent States Quantum Key Distribution



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

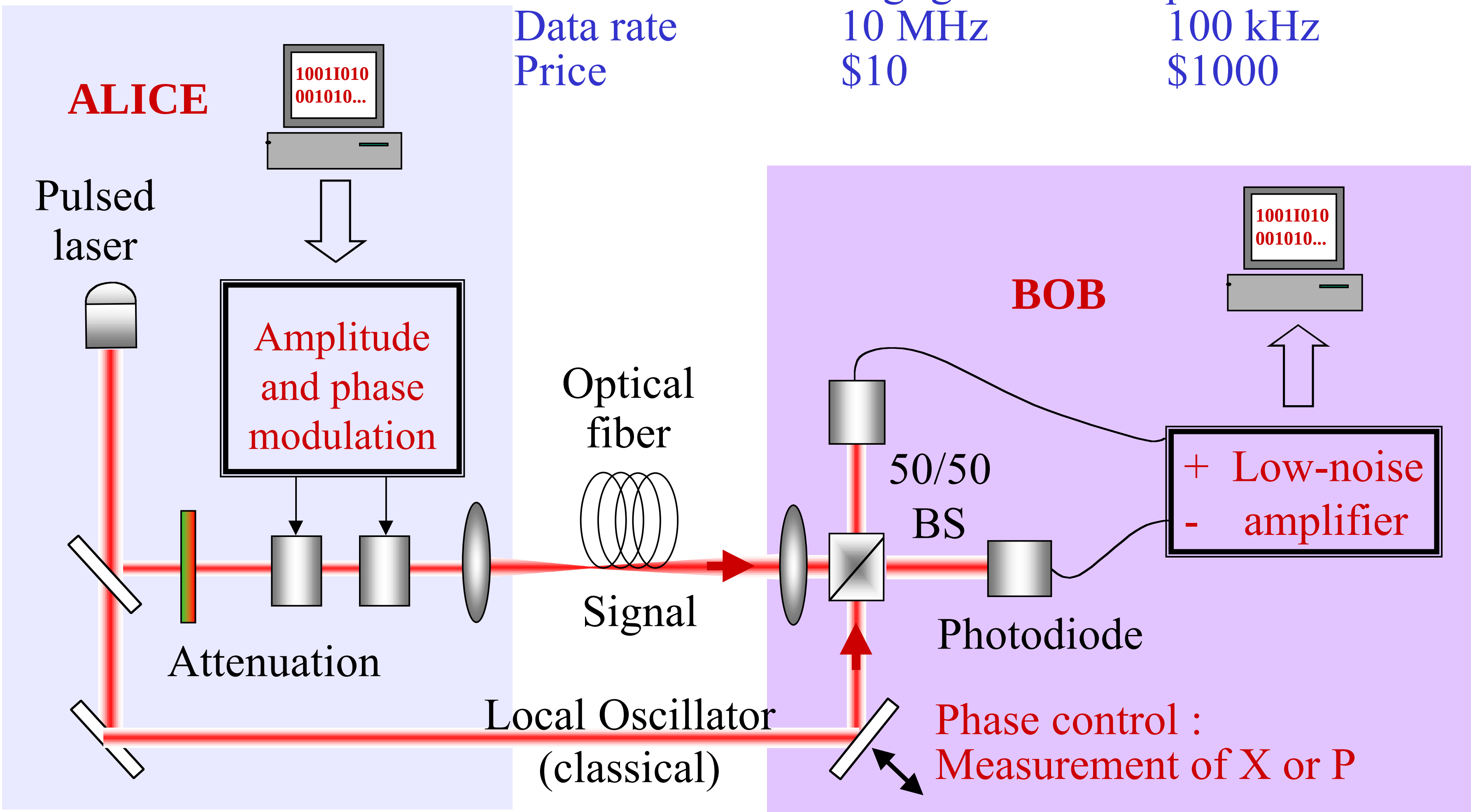
-> **not restricted to single photon polarization !**

-> New QKD protocol where :

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

Homodyne detection

	Homodyne	Counting (APD)
Efficiency	> 90%	10-50 %
Dark rate	negligible	problem
Data rate	10 MHz	100 kHz
Price	$10	$1000



QKD protocol using coherent states with gaussian amplitude and phase modulation

QIPC

Efficient transmission of information using continuous variables ?

-> Shannon's formula (1948) : the mutual information I_{AB} (unit : bit / symbol) for a gaussian channel with additive noise is given by

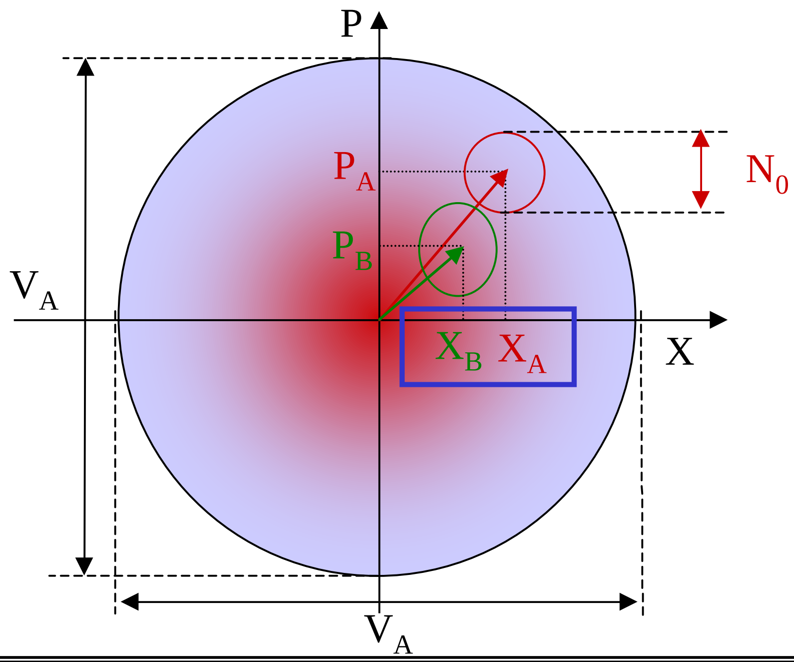
$$I_{AB} = 1/2 \log_2 [\ 1 + V(\text{signal}) / V(\text{noise})\ ]$$

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

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

(c) Bob measures either X_B or P_B

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



Data Transmission between Alice and Bob

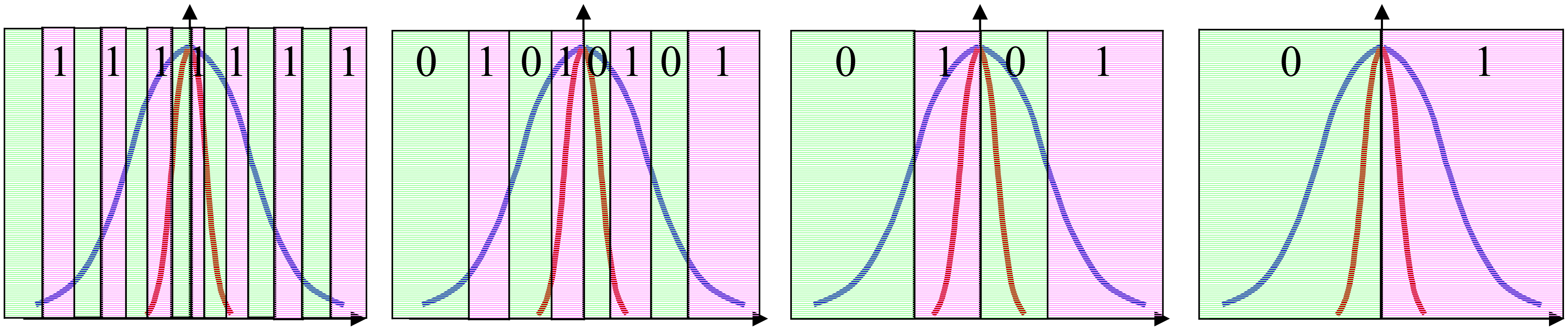
QIPC

At the end of the quantum exchange Alice and Bob share correlated strings of continuous data, from which they have to extract correlated bits.

Shannon's formula gives the maximum number of extractable bits, but this is an asymptotic value that requires adequate data processing ->

Optimized extraction method : **"sliced reconciliation"** :

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



first bit   second bit   third bit   fourth bit

Gives up to 95% of Shannon's value !

Coherent state QKD : predictions

Institut d'Optique

QIPC

Secret key transmission : predicted results

Ideal SK rate : based on the error rate only, assumes perfect sofware efficiency (= ideal data extraction, reconciliation, and privacy amplification)

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

in shot-noise units

bits/pulse

Corresponding to a pulse rate 800 kHz

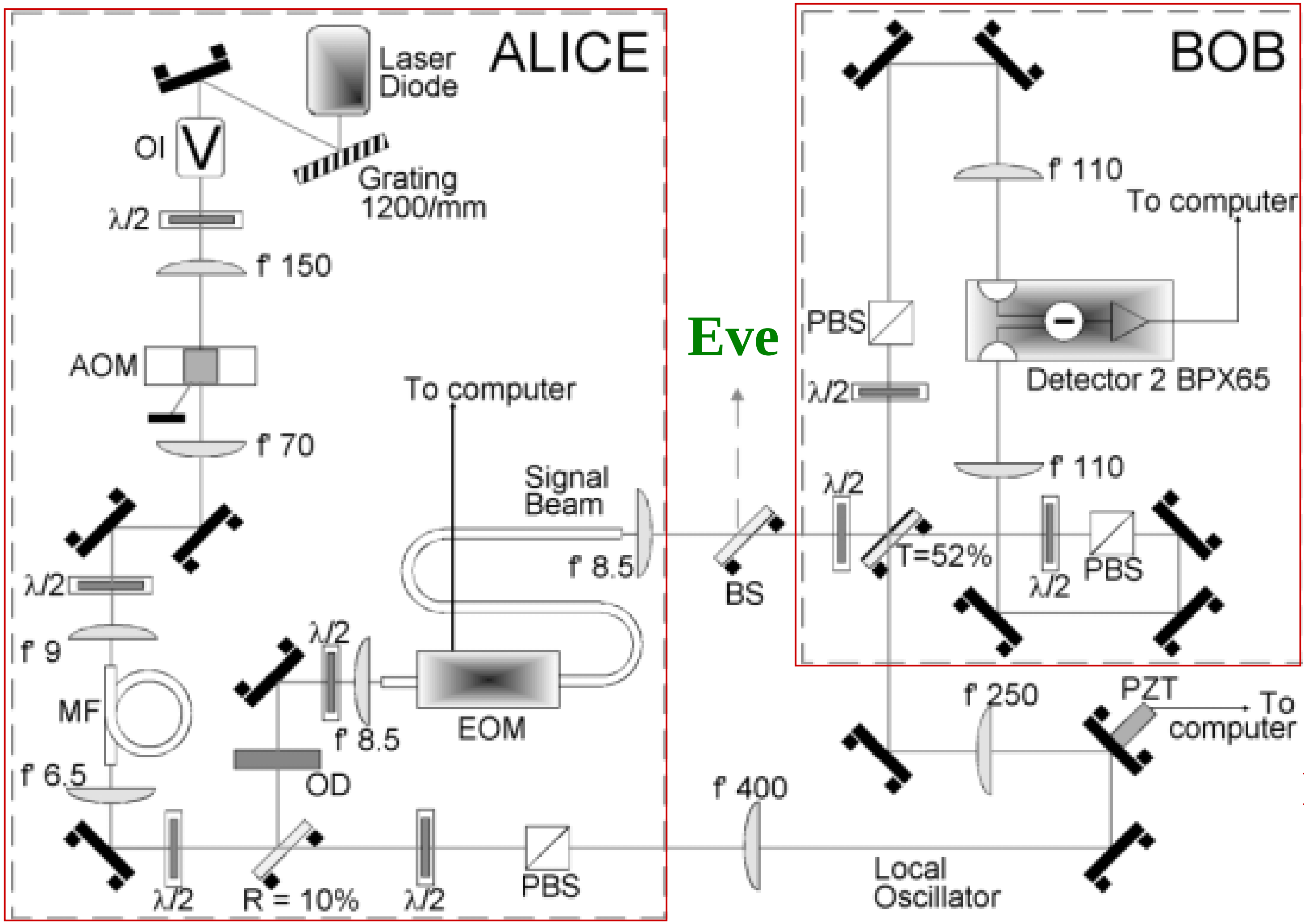
Experimental demonstration of QKD with modulated coherent states

Institut d'Optique

QIPC

120 ns pulses from a laser diode (780 nm)

AOM rep. rate 800 kHz



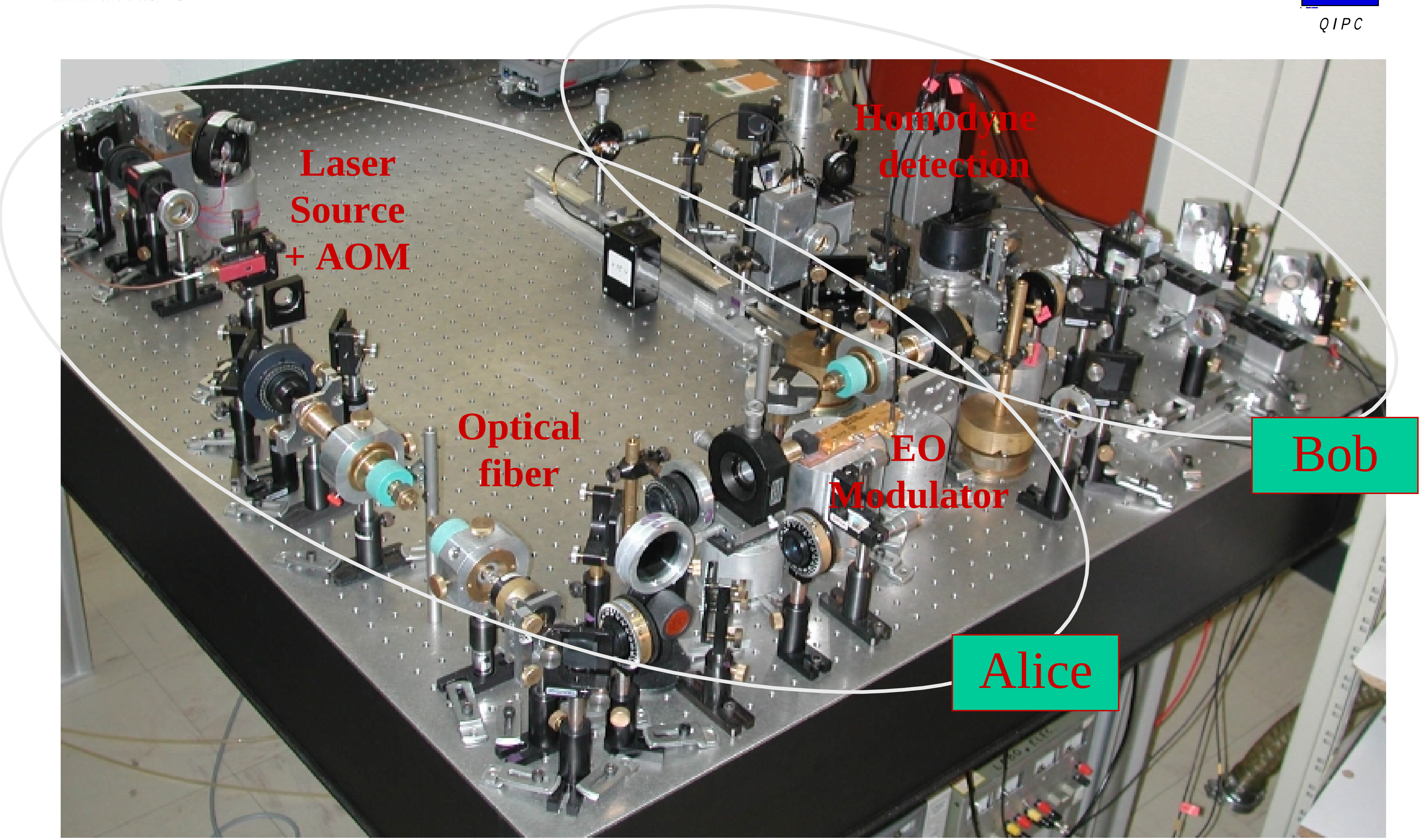
Pulsed homodyne detection

Signal pulses: 100 phot.

LO pulses: $3\ 10^8$ phot.

$N_{el} = 0.26\ N_0$

Experimental set-up



QIPC

Coherent state QKD : results

Secret key transmission : final results (after privacy amplification)

« Realistic » hypothesis : Eve cannot exploit the noise of the homodyne detection

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

in shot-noise units

bits/pulse

Corresponding to a pulse rate 800 kHz

Conclusion

Institut d'Optique

CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

QIPC

Single photon quantum cryptography : PRL **89,** 187901 (2002)

* Photostable at room temperature, very small $g^{(2)}(0) = 0.07$
* Collection efficiency 2.2% (may be improved …)
* Distance 50m with an error rate 4.6%
* Secure bit transmission rate (no loss) : 5 to 8 kbit/sec
* Quantitative advantage with respect to weak pulses

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

* At short distance / low loss very high bit rate are accessible (1.7 Mbit/sec observed without optimization, may be improved at least 10 times)
* Secure bit transmission rate @ 3.1 dB loss : 75 kbit/sec
* Competitive against faint pulses ? Test @ 1550 nm required