Applicazioni Fotonica 3: Emissione dispositivi quantistici

Campo quantistico

$$\vec{E}_{\vec{k},\lambda}(\vec{r}) = i\left(\frac{\hbar\omega_k}{2\varepsilon_0 V}\right)^{1/2}\left[\hat{a}_{\vec{k},\lambda}\, e^{i\vec{k}\cdot\vec{r}} - \hat{a}^{+}_{\vec{k},\lambda}\, e^{-i\vec{k}\cdot\vec{r}}\right]\vec{e}_{\vec{k},\lambda}$$

Stati di Fock $\left|n_{\vec{k},\lambda}\right\rangle$ numero di fotoni definito

$$\hat{a}\left|n_{\vec{k},\lambda}\right\rangle = \sqrt{n}\left|(n-1)_{\vec{k},\lambda}\right\rangle \qquad \hat{a}^{+}\left|n_{\vec{k},\lambda}\right\rangle = \sqrt{n+1}\left|(n+1)_{\vec{k},\lambda}\right\rangle$$

Gli stati di Fock non rappresentano campi classici $\left\langle n_{\vec{k},\lambda}\left|\vec{E}_{\vec{k},\lambda}\right|n_{\vec{k},\lambda}\right\rangle = 0$

$$\left\langle n_{\vec{k},\lambda}\left\|\vec{E}_{\vec{k},\lambda}\right|^2\right|n_{\vec{k},\lambda}\right\rangle = \frac{\hbar\omega_k}{\varepsilon_0 V}(2n+1)$$ Fluttuazioni quantistiche

Stato coerente (classico)

$$\hat{a}\left|\alpha\right\rangle = \alpha\left|\alpha\right\rangle \quad \Rightarrow \quad \left\langle\alpha\right|\hat{a}^{+}\left|\alpha\right\rangle = \alpha^{*}$$

$$\vec{E}_{\vec{k},\lambda}\left(\vec{r}\right) = i\left(\frac{\hbar\omega_{k}}{2\varepsilon_{0}V}\right)^{1/2}\left[\hat{a}_{\vec{k},\lambda}e^{i\vec{k}\cdot\vec{r}} - \hat{a}^{+}_{\vec{k},\lambda}e^{-i\vec{k}\cdot\vec{r}}\right]\vec{e}_{\vec{k},\lambda}$$

$$\left\langle\alpha\right|\vec{E}_{\vec{k},\lambda}\left|\alpha\right\rangle = i\left(\frac{\hbar\omega_{k}}{2\varepsilon_{0}V}\right)^{1/2}\left[\alpha\, e^{i\vec{k}\cdot\vec{r}} - \alpha^{*}e^{-i\vec{k}\cdot\vec{r}}\right]\vec{e}_{\vec{k},\lambda}$$

(Onda piana (LASER))

Stato coerente (Onda piana, sferica, fascio Gaussiano (LASER))

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$$

$$|\alpha\rangle = \sum_{n=0}^{\infty} \alpha^n \frac{e^{-\frac{|\alpha|^2}{2}}}{\sqrt{n!}}|n\rangle$$

Roy Glauber

Nobel Prize in Physics 2005 "for his contribution to the quantum theory of optical coherence"

$$\hat{a}|\alpha\rangle = \sum_{n=0}^{\infty} \alpha^n \frac{e^{-\frac{|\alpha|^2}{2}}}{\sqrt{n!}}\hat{a}|n\rangle = \sum_{n=1}^{\infty} \alpha^n \frac{e^{-\frac{|\alpha|^2}{2}}}{\sqrt{n!}}\sqrt{n}|n-1\rangle$$

$$= \alpha \sum_{n=1}^{\infty} \alpha^{n-1} \frac{e^{-\frac{|\alpha|^2}{2}}}{\sqrt{(n-1)!}}|n-1\rangle = \alpha \sum_{n=0}^{\infty} \alpha^n \frac{e^{-\frac{|\alpha|^2}{2}}}{\sqrt{n!}}|n\rangle = \alpha|\alpha\rangle$$

Stato coerente (Onda piana, sferica, fascio Gaussiano (LASER))

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$$

$$|\alpha\rangle = \sum_{n=0}^{\infty} \alpha^n \frac{e^{-\frac{|\alpha|^2}{2}}}{\sqrt{n!}}|n\rangle$$

Roy Glauber

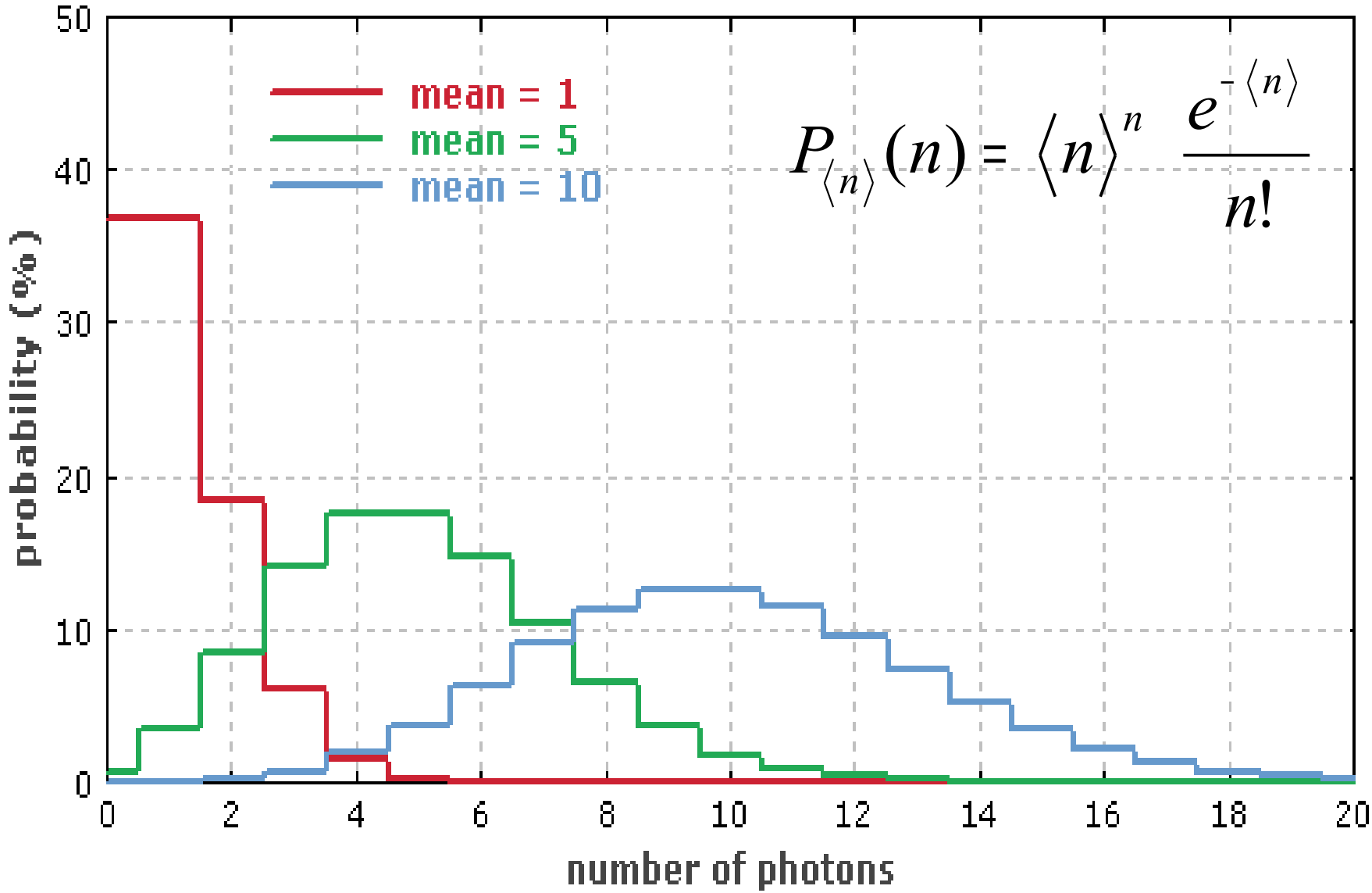
Nobel Prize in Physics 2005 "for his contribution to the quantum theory of optical coherence"

$$\langle n\rangle = \langle\alpha|\hat{a}^+\hat{a}|\alpha\rangle = |\alpha|^2 \quad \Rightarrow \quad \langle n^2\rangle - \langle n\rangle^2 = \langle n\rangle$$

$$P_\alpha(n) = |\langle n|\alpha\rangle|^2 = |\alpha|^{2n}\frac{e^{-|\alpha|^2}}{n!} = \langle n\rangle^n \frac{e^{-\langle n\rangle}}{n!}$$

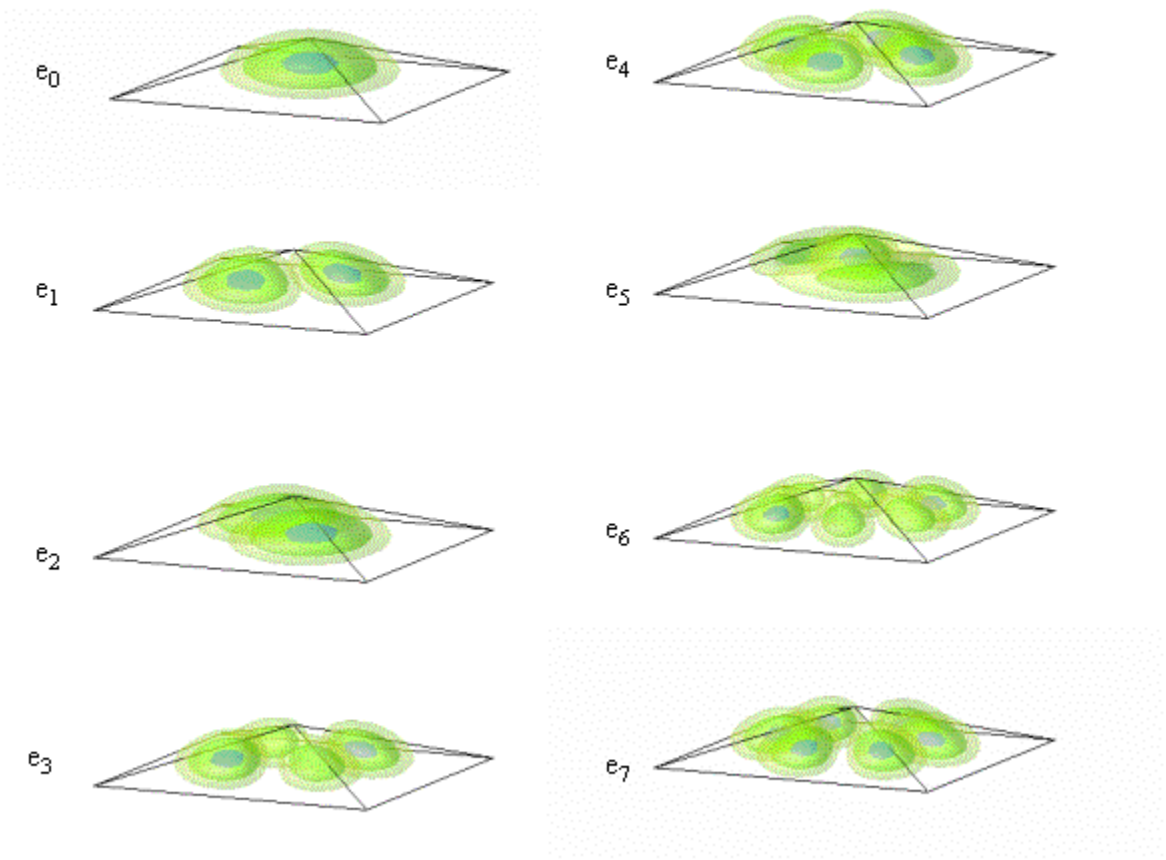
Statistica Poissoniana

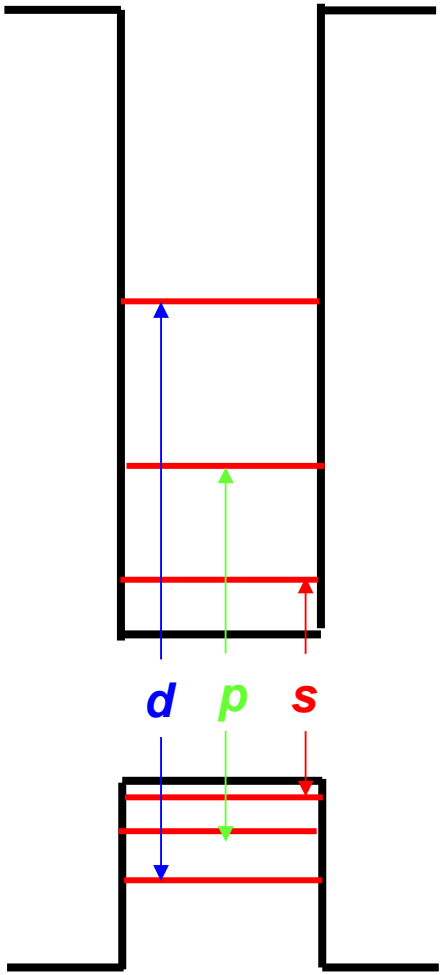
Statistica Poissoniana



QDs
Emettitori quantistici

Electron states in InAs 36h/250b dot





Ogni livello contiene 2 stati di spin. La transizione S è degenere

Spettroscopia con risoluzione spaziale

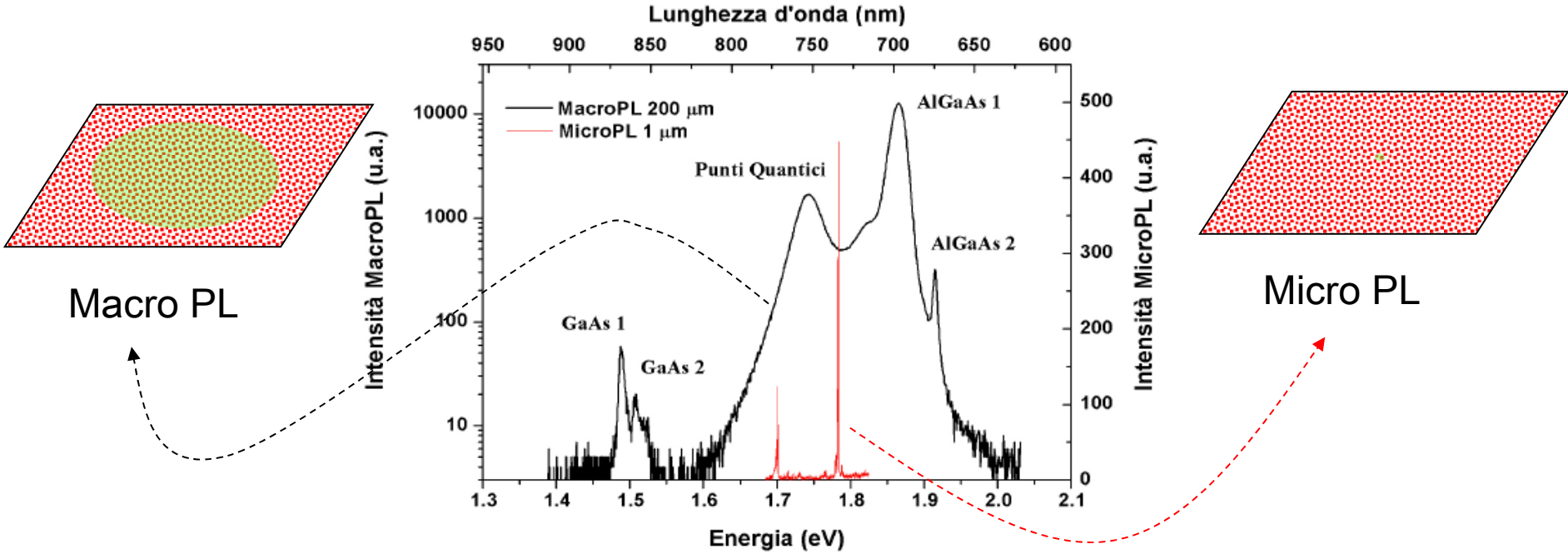


Figura 4.1: *In nero, spettro di macro fotoluminescenza (MacroPL) della radiazione proveniente dagli emettitori racchiusi in un area di circa* $200\,\mu m$ *di diametro, di un campione di punti quantici di GaAs immersi in AlGaAs. In rosso, spettro di micro fotoluminescenza (MicroPL) della radiazione emessa dai punti quantici contenuti in una regione di circa* $1\,\mu m$ *di diametro del medesimo campione. di MacroPL. Il campione è stato cresciuto con la tecnica MDE.*

Spettroscopia con risoluzione spaziale

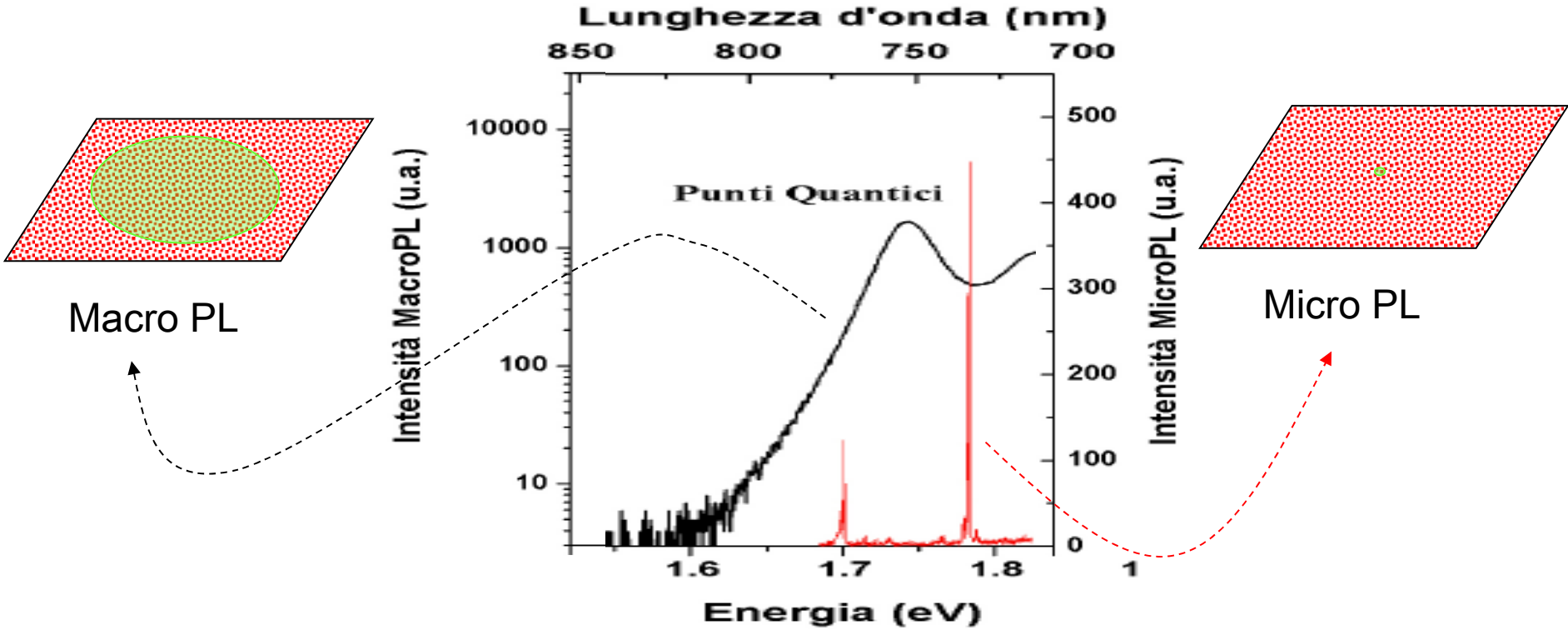
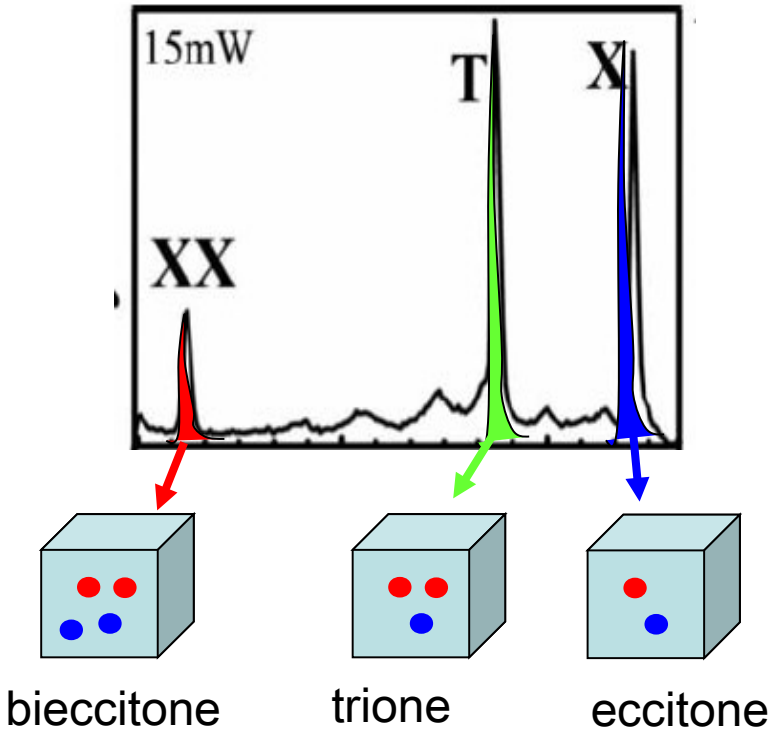


Figura 4.1: *In nero, spettro di macro fotoluminescenza (MacroPL) della radiazione proveniente dagli emettitori racchiusi in un area di circa* $200\,\mu m$ *di diametro, di un campione di punti quantici di GaAs immersi in AlGaAs. In rosso, spettro di micro fotoluminescenza (MicroPL) della radiazione emessa dai punti quantici contenuti in una regione di circa* $1\,\mu m$ *di diametro del medesimo campione. di MacroPL. Il campione è stato cresciuto con la tecnica MDE.*

PHYSICAL REVIEW B 78, 125321 (2008)

Exciton fine structure in strain-free GaAs/ $Al_{0.3}Ga_{0.7}As$ quantum dots: Extrinsic effects

M. Abbarchi,[1] C. A. Mastrandrea,[1] T. Kuroda,[2] T. Mano,[2] K. Sakoda,[2] N. Koguchi,[3] S. Sanguinetti,[3] A. Vinattieri,[1] and M. Gurioli[1]



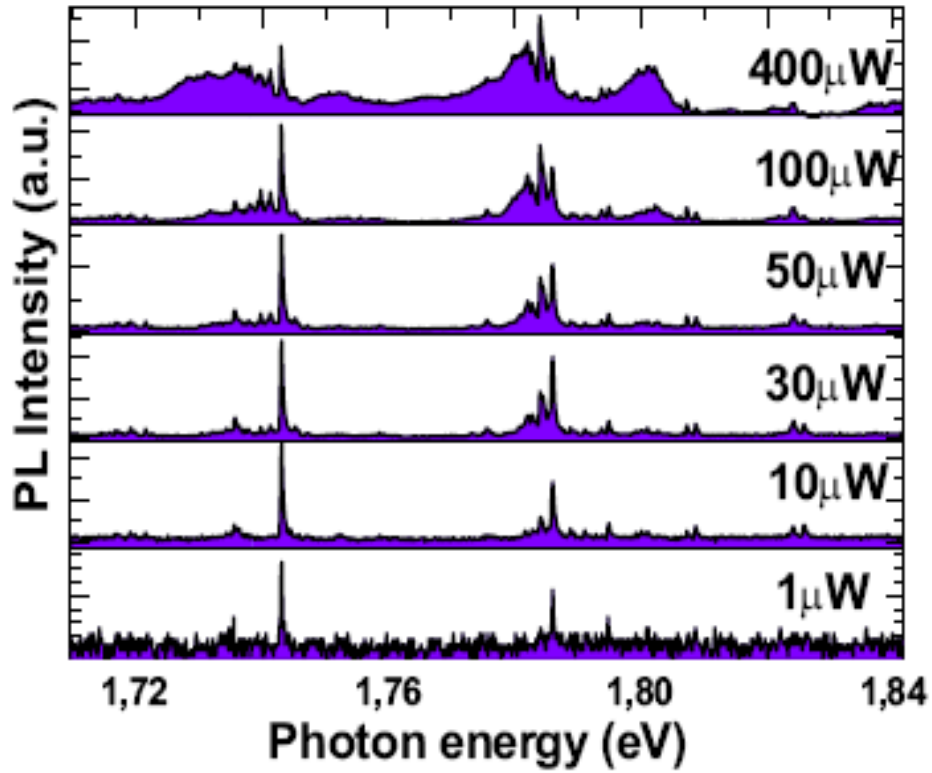
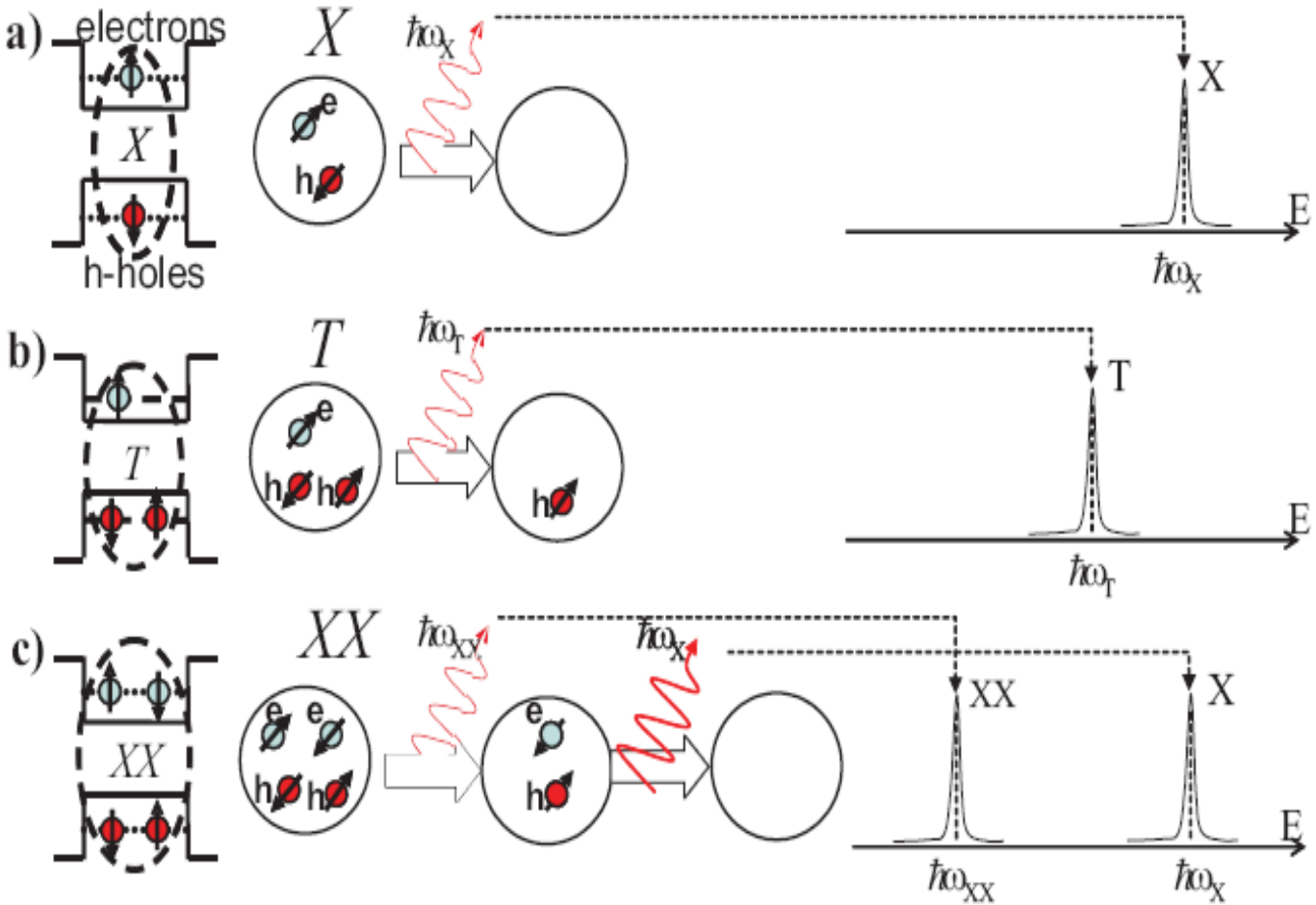


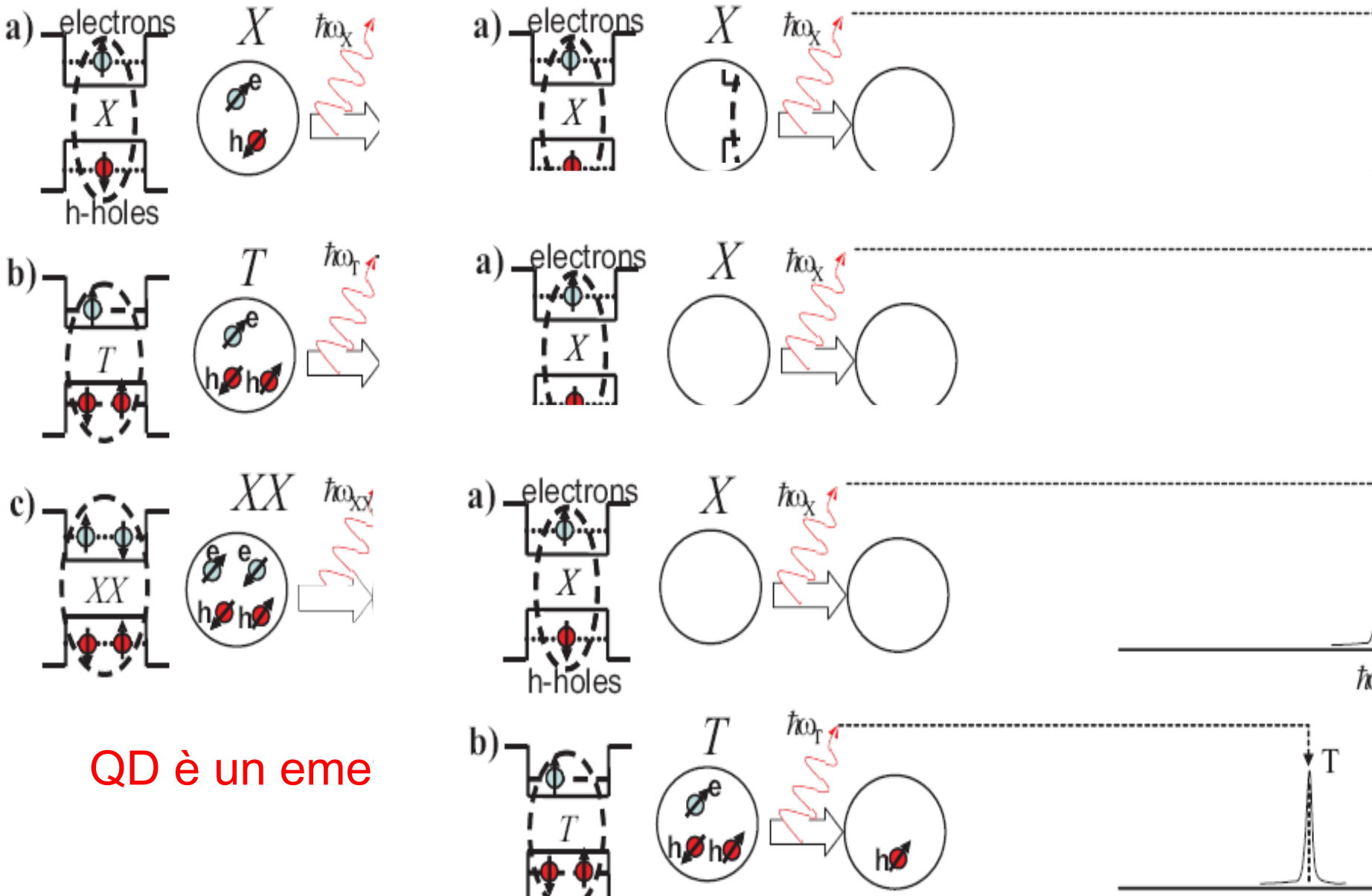
Fig. 1 μPL spectra at different excitation power.

Interazione Coulombiana rompe la degenerazione



Interazione Coulombiana cambia l'energia della transizione ottica della shell S a seconda del numero di cariche spettatrici

Ogni transizione emette 1 fotone alla volta



QD è un eme

Come si verifica che uno stato è stato di Fock?

La funzione di correlazione del primo ordine $g^{(1)}(\triangle\mathbf{x},\tau)$ rappresenta la correlazione del campo E in due diversi punti $(\mathbf{x},t)$ e $(\mathbf{x}+\Delta\mathbf{x},t+\tau)$:

$$g^{(1)}(\mathbf{x},\triangle\mathbf{x},t,\tau)=\frac{\langle E^{*}(\mathbf{x},t)\,E(\mathbf{x}+\triangle\mathbf{x},t+\tau)\rangle}{\sqrt{\langle|E(\mathbf{x},t)|^{2}\rangle\langle|E(\mathbf{x}+\triangle\mathbf{x},t+\tau)|^{2}\rangle}}\,, \qquad (1.1)$$

in cui le parentesi $\langle . \rangle$ indicano la media statistica sul tempo e sullo spazio finiti su cui avviene la misura. Analogamente, è possibile definire una funzioni di correlazione del secondo ordine che correla l' intensità istantanea $I(t)=|E|^{2}(t)$ invece che il campo:

$$g^{(2)}(\mathbf{x},\Delta\mathbf{x},t,\tau)=\frac{\langle I(\mathbf{x},t)\,I(\mathbf{x}+\triangle\mathbf{x},t+\tau)\rangle}{\langle I(\mathbf{x},t)\rangle^{2}}\,. \qquad (1.2)$$

Funzione di correlazione temporale

$$g^{(2)}(x_o,t,\tau) = \frac{\langle I(x_o,t)I(x_o,t+\tau)\rangle}{\langle I(x_o,t)\rangle^2}$$

$$\Rightarrow \quad g^{(2)}(\tau) = \frac{\langle I(t)I(t+\tau)\rangle}{\langle I(t)\rangle^2} \quad \Rightarrow \quad g^{(2)}(0) = \frac{\langle \hat{n}(\hat{n}-1)\rangle}{\langle \hat{n}\rangle^2}$$

Campo classico

$$g^{(2)}(0) \geq g^{(2)}(\tau)$$

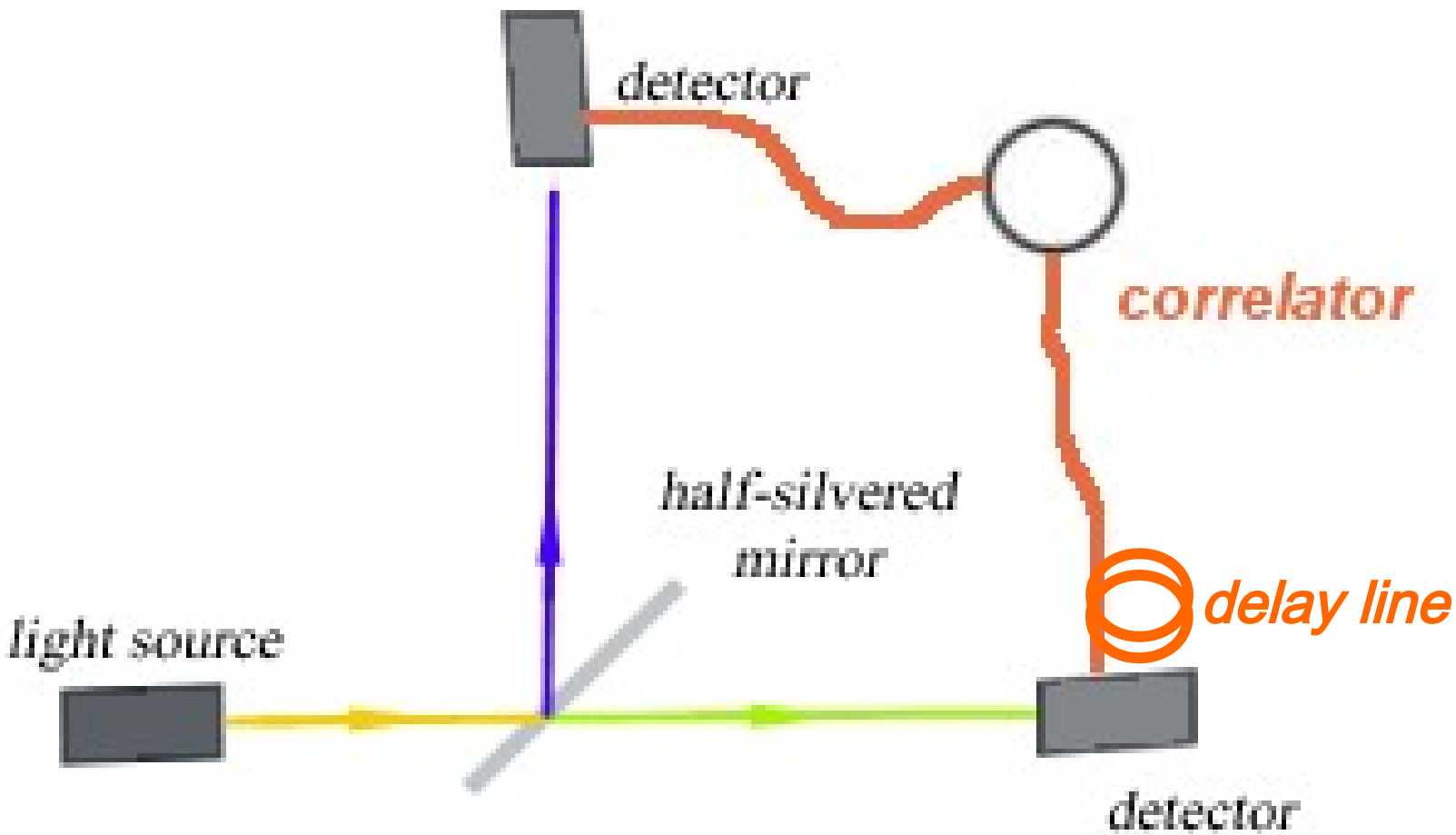
$$\infty \geq g^{(2)}(0) \geq 1$$

Stato di Fock

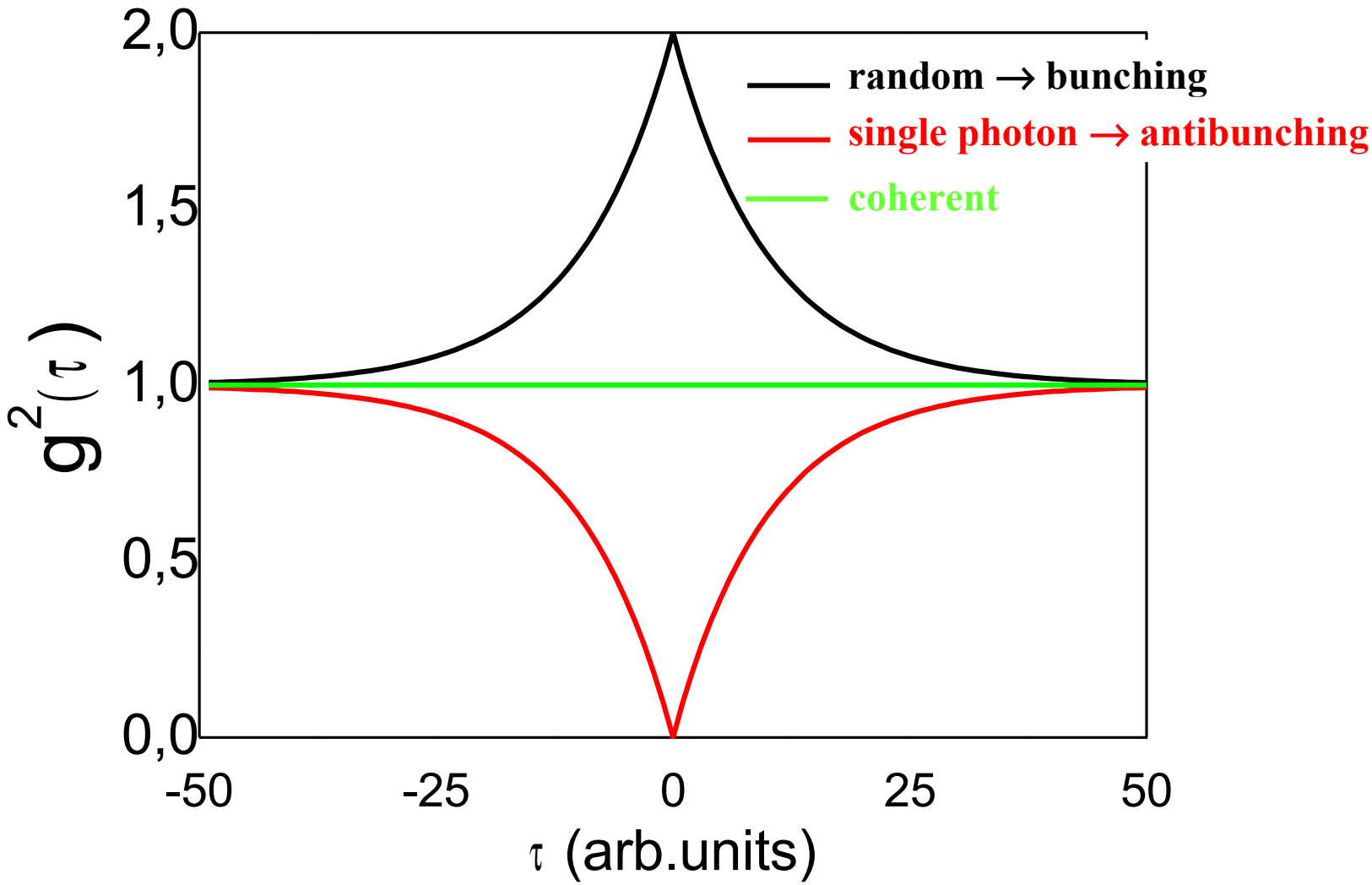
$$g^{(2)}(0) = \frac{n-1}{n}$$

$$n = 1 \Rightarrow g^{(2)}(0) = 0$$

Hanbury Brown & Twiss $$g^{(2)}(\tau) = \frac{\langle I(t) I(t+\tau) \rangle}{\langle I(t) \rangle^2}$$



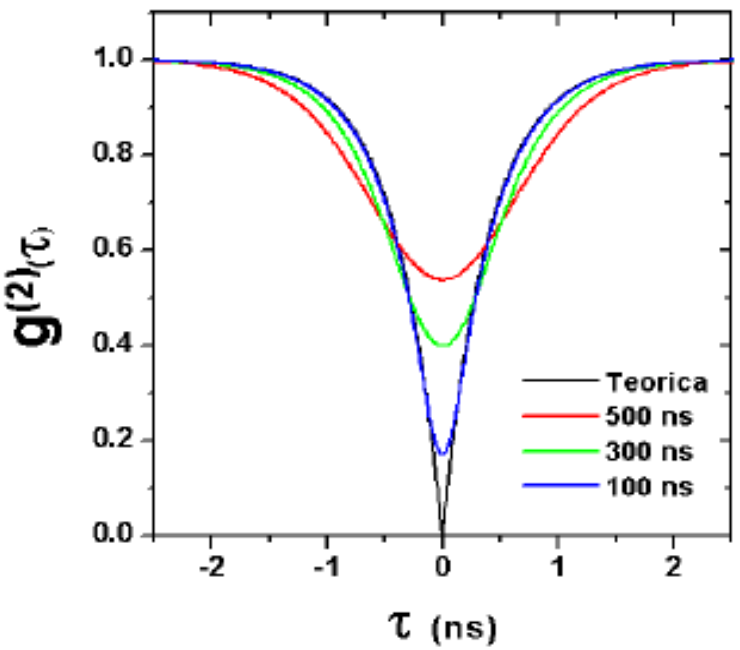
Hanbury Brown & Twiss $g^{(2)}(\tau) = \dfrac{\langle I(t) I(t+\tau) \rangle}{\langle I(t) \rangle^2}$

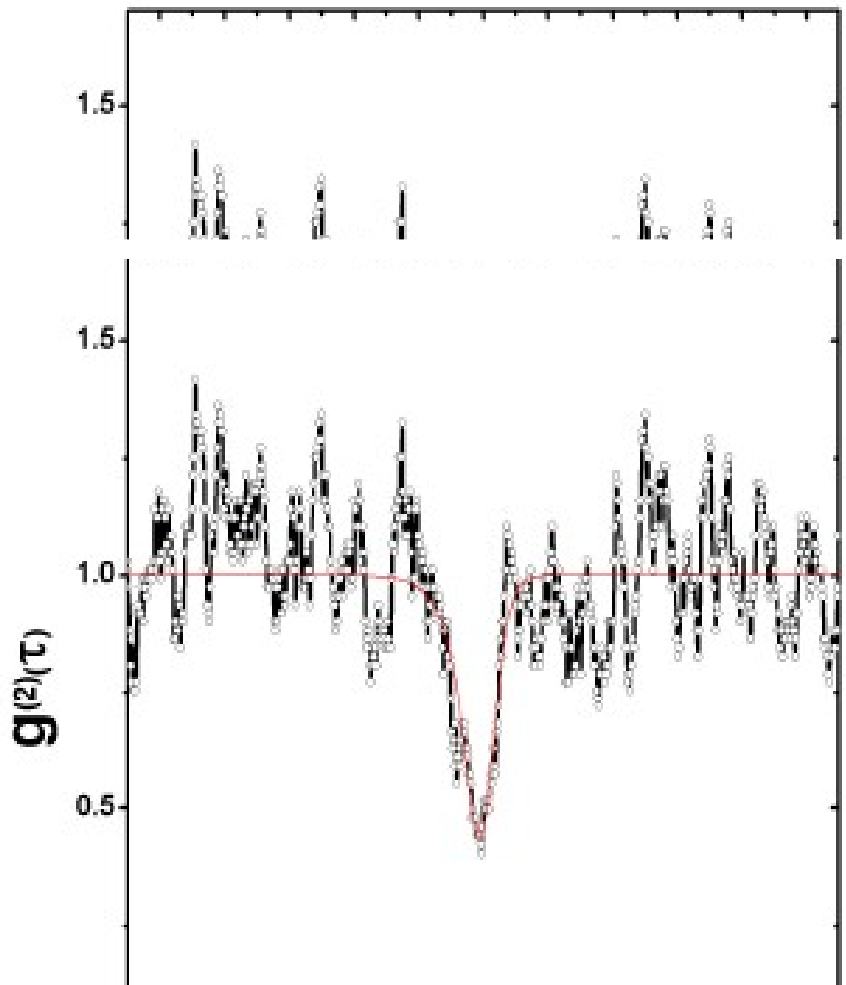


Applied Physics Express 1 (2008) 042001

Photon Correlation in GaAs Self-Assembled Quantum Dots

Takashi Kuroda[1,2*], Marco Abbarchi[1,3], Takaaki Mano[1], Kenji Watanabe[1], Masakazu Yamagiwa[1], Keiji Kuroda[1], Kazuaki Sakoda[1], Giyuu Kido[1], Nobuyuki Koguchi[1], Carmine Mastrandrea[3], Lucia Cavigli[3], Massimo Gurioli[3], Yoshihiro Ogawa[4], and Fujio Minami[4]

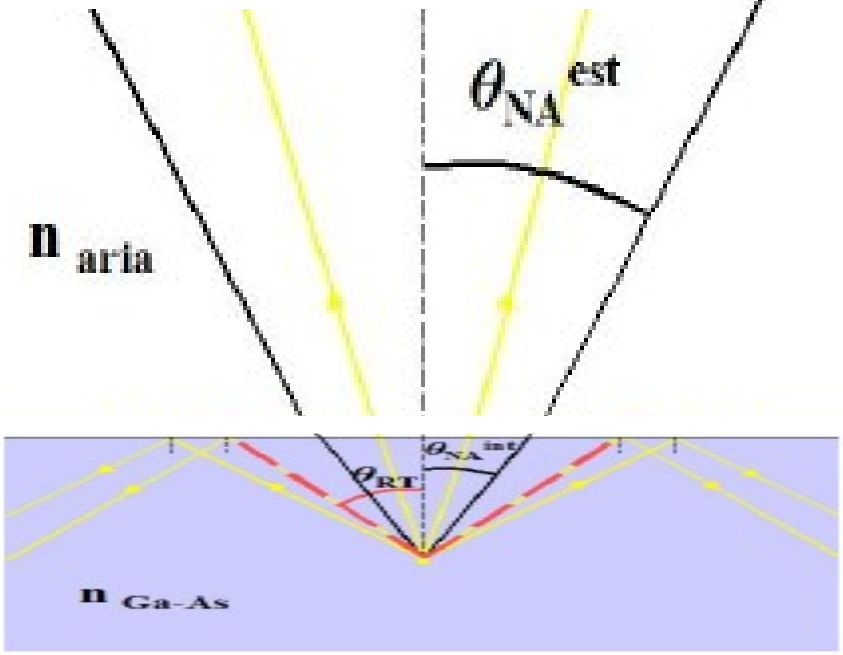




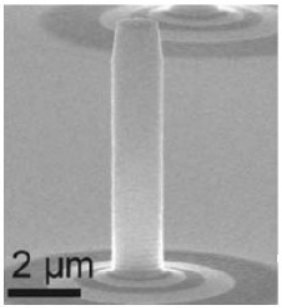
Efficienza di estrazione

OBIETTIVO

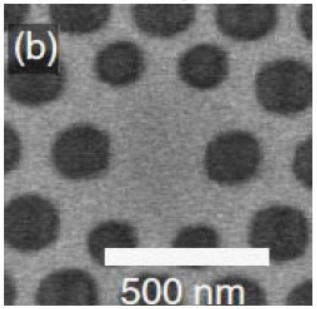
$$\frac{\Omega_{RT}}{4\pi} = \frac{1 - cos\theta_{RT}}{2} \simeq 2\% \ .$$



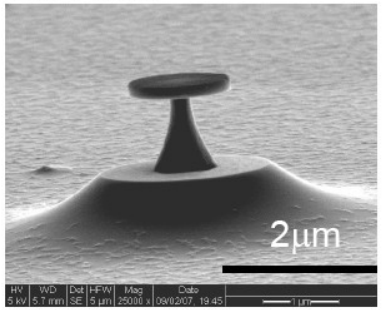
Micropillar



Photonic Crystal



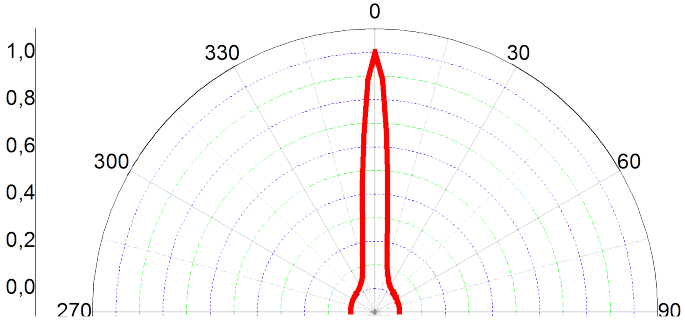
Microdisk



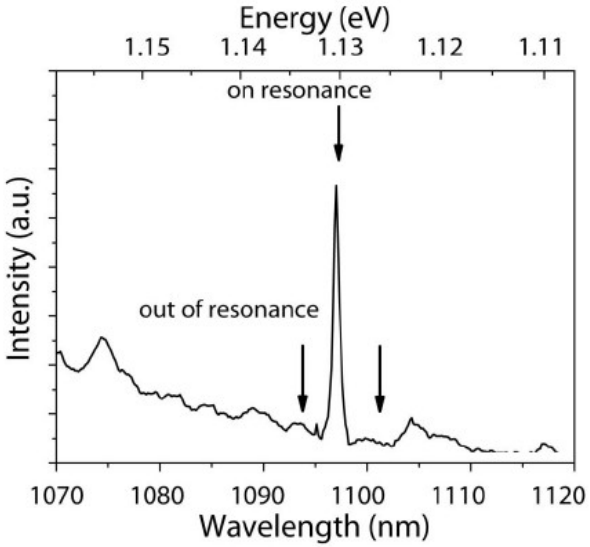
Vantaggi MC

Microcavità

1. Controllo direzionalità di emissione, aumento efficienza di estrazione



2. Effett
rate di ϵ



a) b)

QDs
Emettitori quantistici
Applicazioni in QIT

Criptografia:

Private Key Cryptography

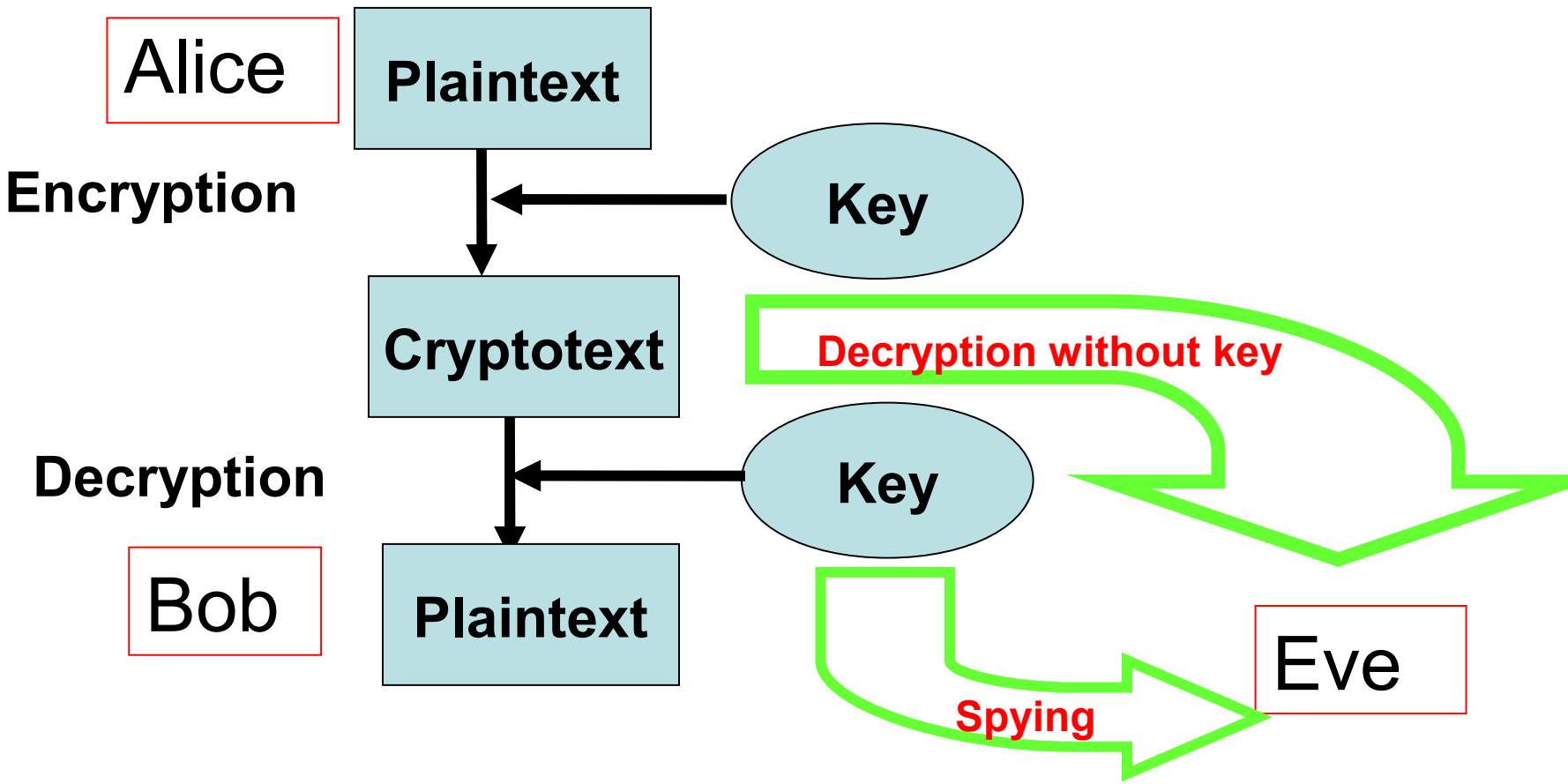
Alice (Bush)

Bob (Cheney)

Eve (Bin Laden)

- Private key cryptography can be provably secure
  - Alice has secret encoding key e, Bob has decoding key d

Cryptography



Old Style Cryptography

- Shift of alphabet
  - e.g. Caesar cipher A=D, B=E, C=F

Caesar → Fdbvdt

- Many more sophisticated systems developed from 1500s to mid-20th century
  - Substitution and transposition of letters
  - Some essentially unbreakable by manual means
- Made obsolete by computers circa 1940

Criptografia moderna (classica)

- **Fattorizzazione in numeri primi**

Easy Problem

Given two large primes p and q compute

$$n = p \times q$$

Hard Problem

Given n compute p and q.

Protocollo RSA

(Rivest, Shamir and Adleman, 1978)

p e q numeri primi (stesso ordine)

$n=pq$ KEY MODULE

$f=(p-1)(q-1)$

e PUBLIC KEY ESPONENT

d PRIVATE KEY ESPONENT

scegliere e: $1<e<f$

calcolare d: $de=1 \pmod{f}$

$(de)=kf+1$ (k naturale)

(n,e) PUBLIC KEY

(n,d) PRIVATE KEY

m MESSAGE $(0<m<n)$

c CODE MESSAGE

Encryption

$$m^e=c \pmod{n}$$

Decryption

$$c^d=m \pmod{n}$$

Prova

$c^d=m^{de} \pmod{n}$ (formula binomiale)

$m^{de}=m^{kf+1}=m(m^f)^k=m \pmod{n}$ (teorema di Eulero)

Esempio RSA

p=53 e q=61
n=3233 KEY MODULE
f=3120
e=17 PUBLIC KEY ESPONENT
d=2753 PRIVATE KEY ESPONENT

scegliere e=17
calcolare d: de=1 (mod(f))
(17*2753)=15*3120+1

(3233,17) PUBLIC KEY
(3233,2753) PRIVATE KEY
m=123 MESSAGE

Encryption

$123^{17}=c \pmod{3233}$ c=855 CODE MESSAGE

Decryption

$855^{2753}=m \pmod{3233}$ → m=123

SICUREZZA:
1. difficoltà trovare f
2. protezione private key

Esempi di criptomessaggi con RSA

Caso 1 comunicazione segreta e firmata

- *Alice, Bob et al creano le proprie chiavi e l'elenco delle chiavi pubbliche è noto*
- *Alice cifra il suo messaggio con la chiave pubblica di Bob*
- *Bob decripta il messaggio con la sua chiave privata (solo Bob può leggerlo)*

Caso 2 comunicazione segreta e firmata

2. *Alice cifra il suo messaggio con la sua chiave privata*
3. *Alice cifra il messaggio criptato con la chiave pubblica di Bob*
4. *Bob decripta il messaggio con la sua chiave privata (solo Bob può leggerlo), ottenendo il messaggio criptato di Alice*
5. *Bob decripta il messaggio con la chiave pubblica di Alice (è certo che il messaggio sia di Alice).*

RSA viene commercializzato, vedi http://www.rsa.com/

RSA
The Security Division of EMC

Vantaggio RSA

1. La fattorizzazione in numeri primi è un problema numerico difficile ($O(\exp(N)^k)$). Record 2005 200 digits (mesi macchina di 80 AMD Opteron)

Problemi RSA

1. Con Quantum Computer la fattorizzazione in numeri primi diventa risolvibile (Shor's algorithm $O(\log(N)^3)$)

2. La chiave privata può essere copiata

Quantum Cryptography

E' una delle tecnologie della Quantum Information la cui base è usare un Quantum Bit invece di un Classical Bit

Classical Bit $\boxed{0}$ $\boxed{1}$

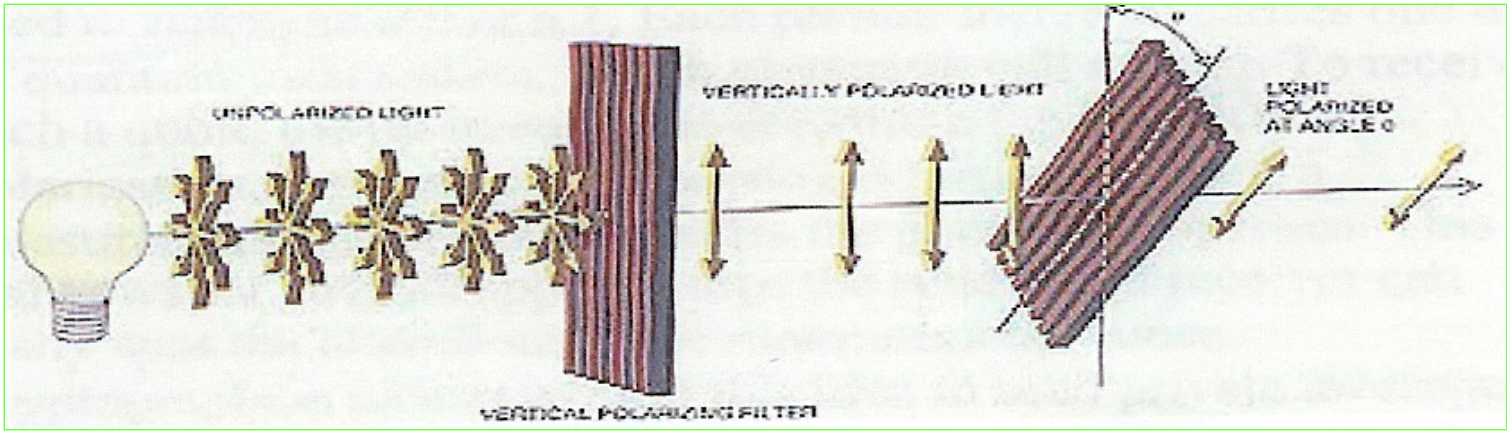
$|c\rangle = |\alpha\rangle$ con $\alpha=0$ oppure $\alpha=1$

Quantum Bit $\boxed{\alpha,\beta}$

$|q\rangle = \alpha|0\rangle+\beta|1\rangle$ con ($\alpha\in\mathbb{C},\beta\in\mathbb{C}$) e $|\alpha|^2+|\beta|^2=1$)

Photonic qu(antum)bit

- La polarizzazione può essere definita su una base arbitraria e i due stati sono 0 o 1.
- Ogni fotone trasporta un qubit di informazione
- I qubit del fotono sono facilmente inizializzabili in una base arbitraria



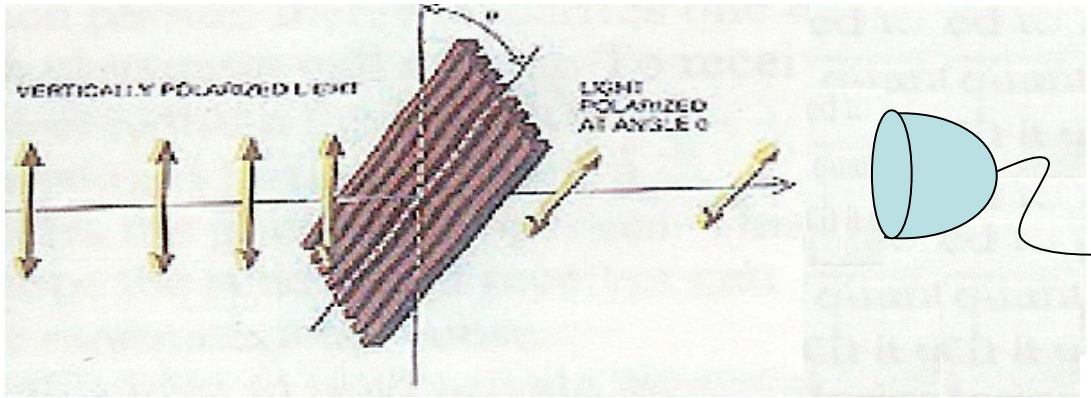
Write $|\nearrow\rangle = \cos\phi\,|\uparrow\rangle + \sin\phi\,|\rightarrow\rangle$

Photonic qu(antum)bit

Read

$|\uparrow\rangle = \cos\phi\,|\nearrow\rangle + \sin\phi\,|\nwarrow\rangle$

- 1 con prob. $(\cos\phi)^2$
- 0 con prob. $(\sin\phi)^2$



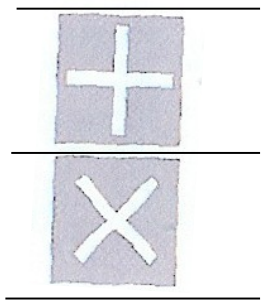
- 1 ⇒ $|\nearrow\rangle$
- 0 ⇒ $|\nwarrow\rangle$

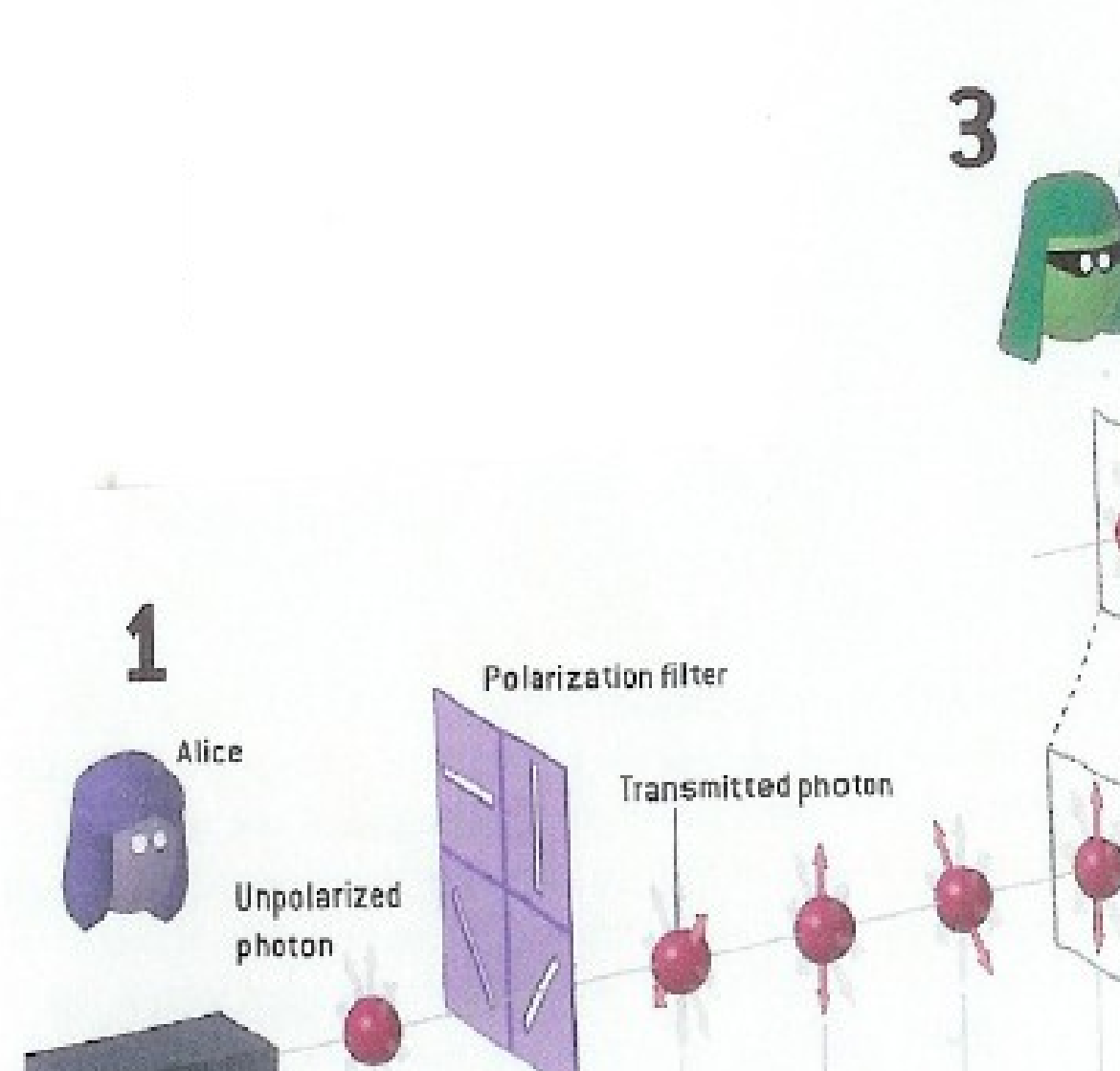
La lettura proietta lo stato sulla base scelta e dà solo un'informazione parziale che può essere completa solo se la base scelta coincide con quella di scrittura del qubit

Photonic qu(antum)bit in QKD

Si usano solo 4 qubits (0,1) nelle basi (0°,90°) e (-45°,45°)

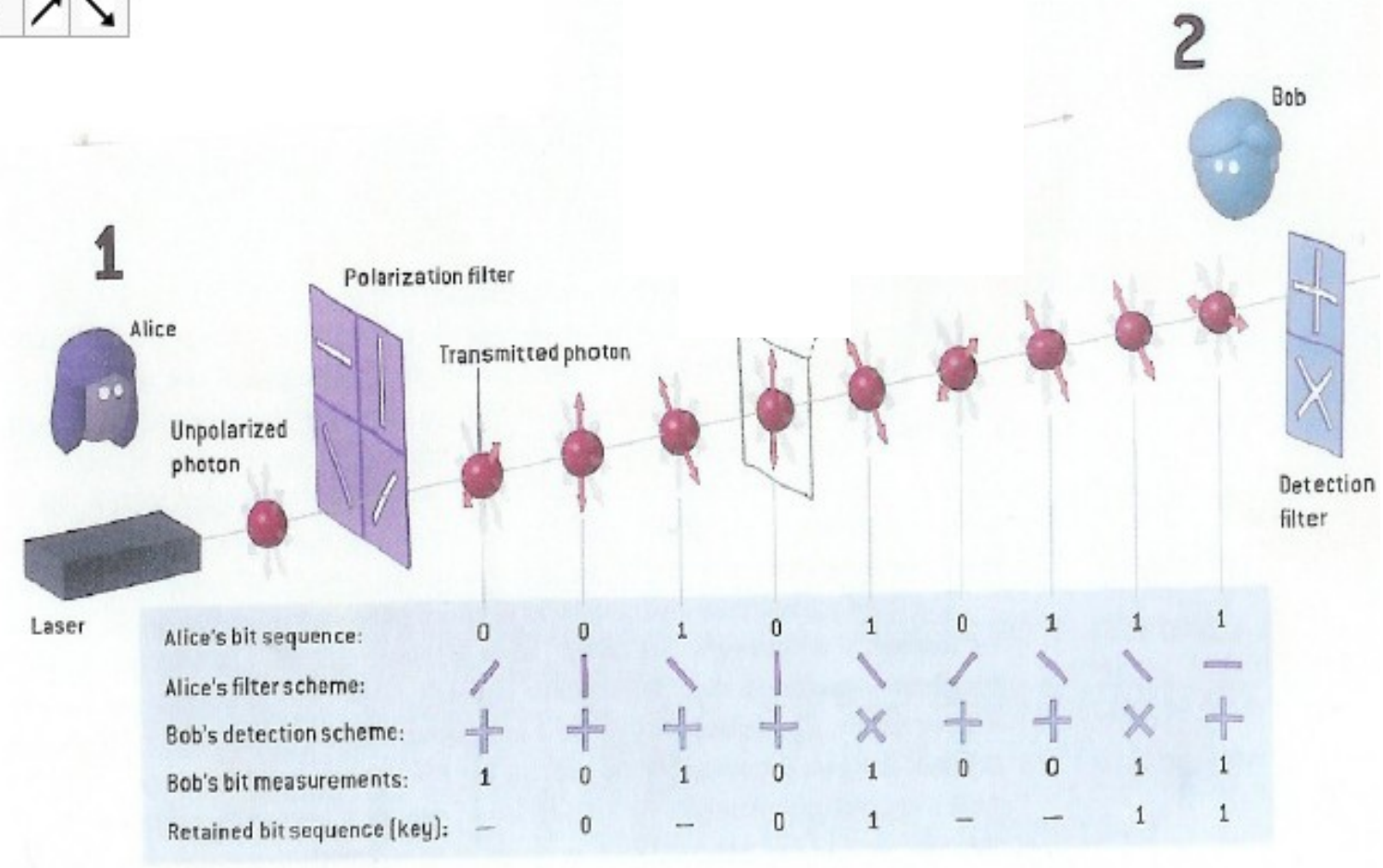
Basi di lettura





Qubit communication

Basis	0	1
+	↑	→
×	↗	↘



BB84 Protocol

1) Alice spedisce 4N random qubits {0°,90°,-45°,45° } a Bob
2) Bob misura ogni qubit in una base o {0°,90° } o {- 45°,45° } scelta a caso
3) Alice e Bob confrontano le loro 4N basi. In media 2N volte saranno uguali e solo questi casi sono considerati.
4) Alice e Bob verificano le misure su circa N bit scelti a caso fra i 2N bits considerati.
5) Se gli errori compatibili con la segretezza
6) I rimanenti N bits sono la chiave segreta

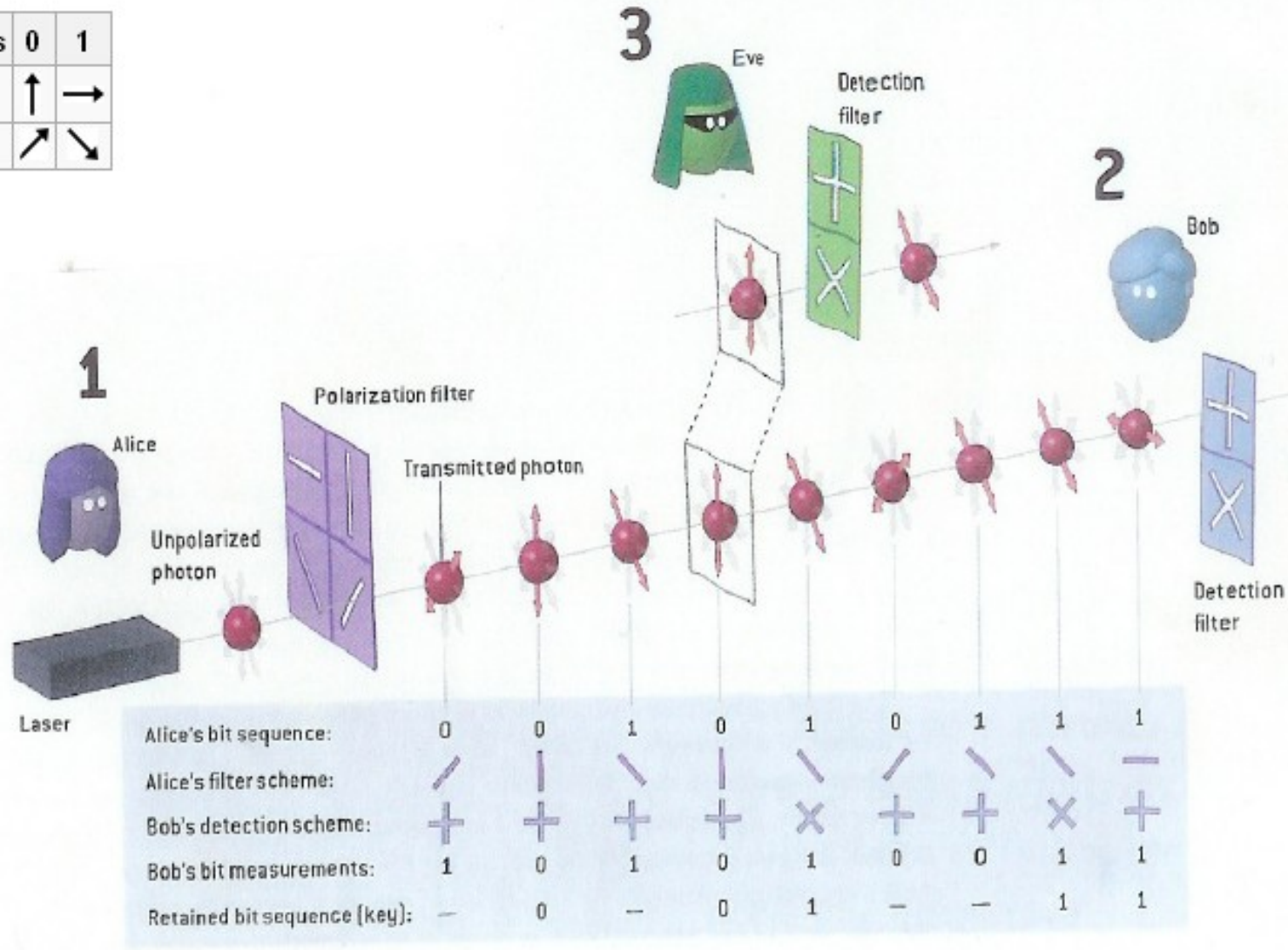
Charles Bennett and Gilles Brassard in 1984.

Sicurezza della QKD

- **La lettura di un qubits necessariamente dà un'informazione parziale**
- **Nessuno stato quantistico può essere clonato perfettamente.**
- **Se QKD è trasportata da una serie di fotoni singoli, ogni fotone viene necessariamente alterato se viene letto.**
- **Questo rende impossibile l'intercettazione segreta del messaggio.**

Qubit communication

Basis	0	1
+	↑	→
×	↗	↘



Quantum cryptography is only used to produce and distribute a key, not to transmit any message data.

It is a quantum key communication, for instance in a revised RSA protocol n,e,d would be transmitted by a quantum channel, while m would be transmitted in a classic channel

New Journal of Physics
The open-access journal for physics

Athens/Institutional login
IOP login:
Create account | Alerts |
IOP Journals Home IOP Journals List EJs Extra This Journal Search Authors Referees Librarians User Opt
This volume | This month | Abstract | Content finder

New J. Phys. 8 (2006) 193
doi:10.1088/1367-2630/8/9/193
PII: S1367-2630(06)27213-6

Long-distance quantum key distribution in optical fibre

P A Hiskett[1], D Rosenberg[1,4], C G Peterson[1], R J Hughes[1], S Nam[2], A E Lita[2], A J Miller[3] and J E Nordholt[1]

QKD su 202 km ma non con single photon source

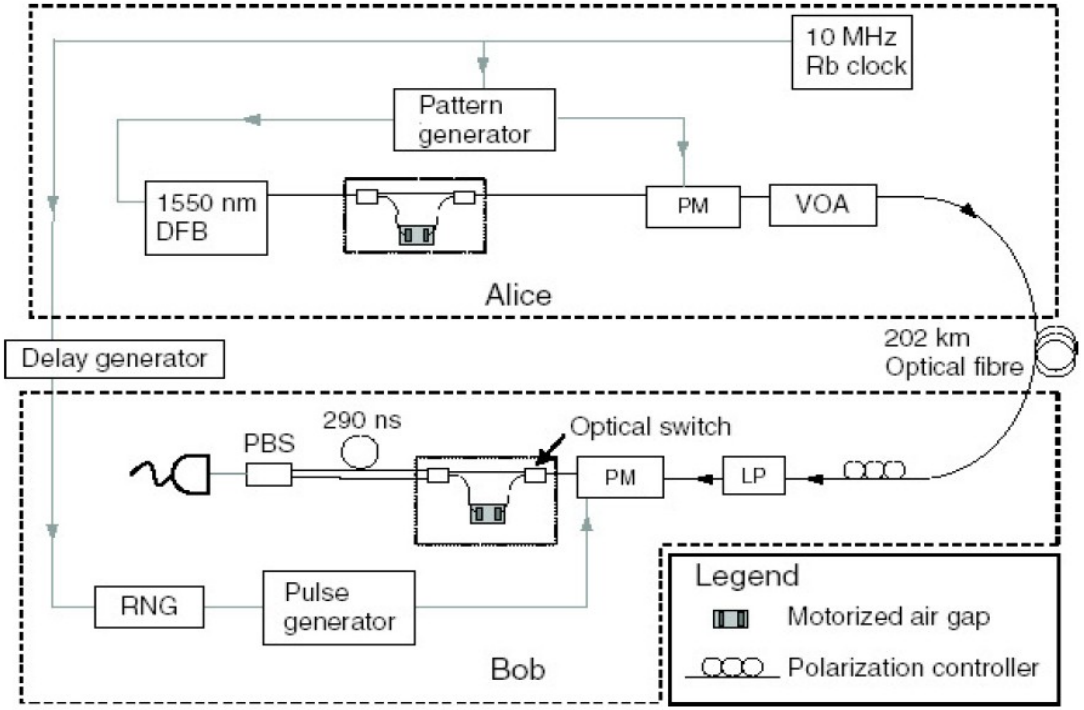
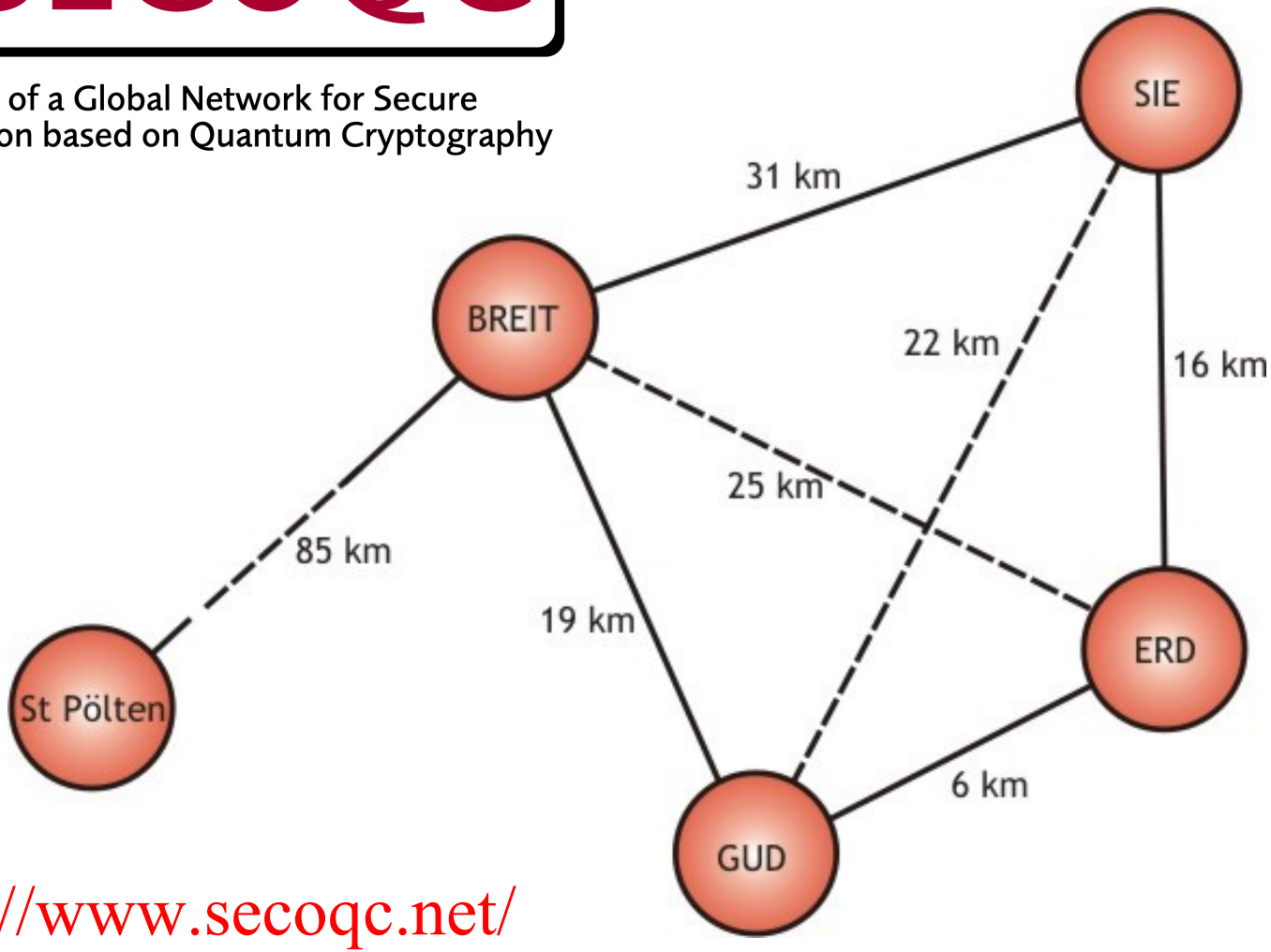


Figure 1. Simplified schematic of phase-coding QKD system. LP = linear polarizer; VOA = variable optical attenuator; PBS = polarizing beam splitter; DFB = distributed feedback laser; RNG = random number generator; PM = phase modulator.

Primo computer network protetto da QC (2008)

SECOQC

Development of a Global Network for Secure Communication based on Quantum Cryptography



http://www.secoqc.net/