Differential Phase Shift Quantum Key Distribution and Beyond

Yoshihisa Yamamoto
E. L. Ginzton Laboratory, Stanford University
National Institute of Informatics (Tokyo, Japan)

- **DPS-QKD system**

  Protocol
  System components
  Experiments
  Security issue

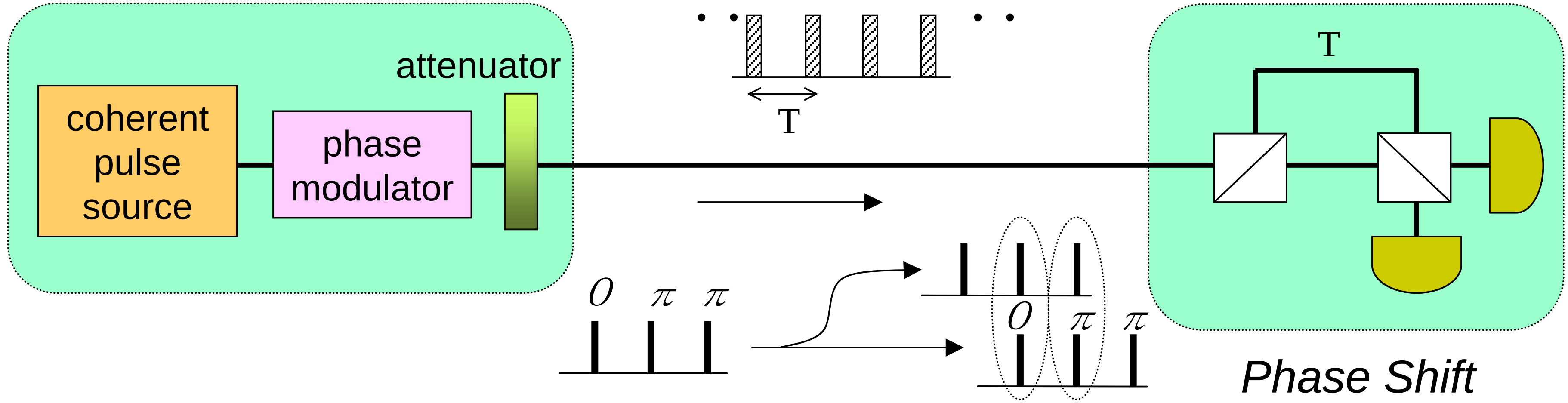
- **Future photonic quantum information systems**

  Single photon source
  Quantum repeaters
  Quantum computers

MIT/Stanford/UC Berkeley Nanotechnology Forum
(NASA Ames Research Center, Oct. 20, 2005)

Differential Phase Shift
Quantum Key Distribution (DPS-QKD)

Average photon number < 1 photon/pulse
A single photon occupies many pulses simultaneously



Alice

Time	*t1*	*t2*	*t3*	*t4*	*t5*	*t6*	*t7*
Phase Difference	0	π	0	0	0	π	0

Time	*t2*	*t4*	*t6*
Raw key	1	0	1

Bob

Time	*t2*	*t4*	*t6*
Detector	*Det2*	*Det1*	*Det2*
Phase Difference	π	0	π
Raw key	1	0	1

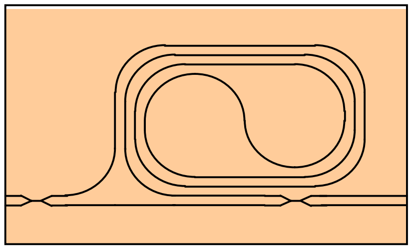
Inoue, Waks, Yamamoto, PRL, 89, 037902 (2002).

Nondeterministic wavepacket reduction by quantum measurement provides absolute security.

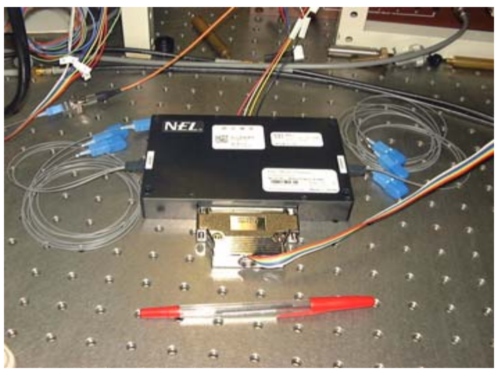
Mach-Zehnder Interferometer by PLC

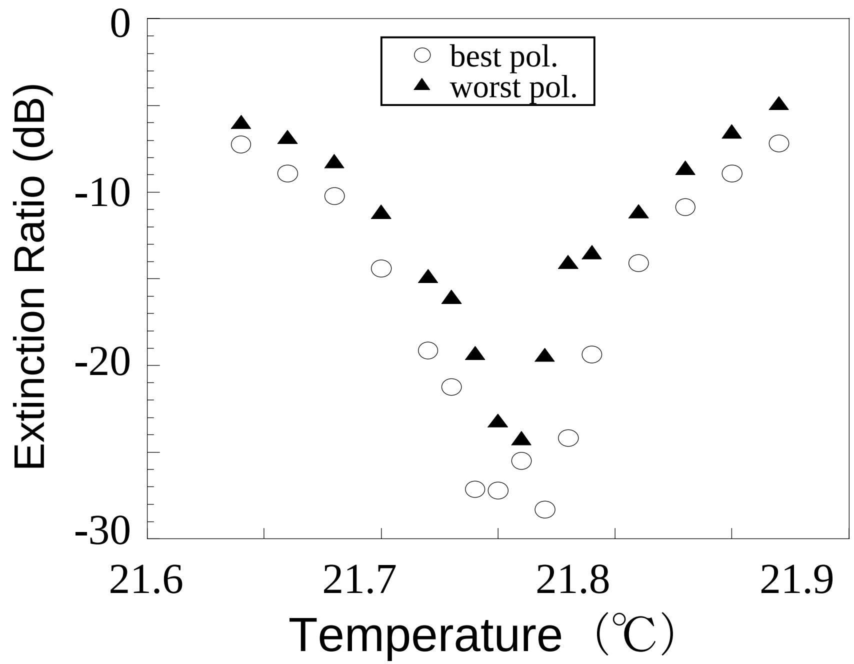
Stable Optical Delay Line

Optical Path Difference 20 cm



Loss ２dB （fiber-fiber）





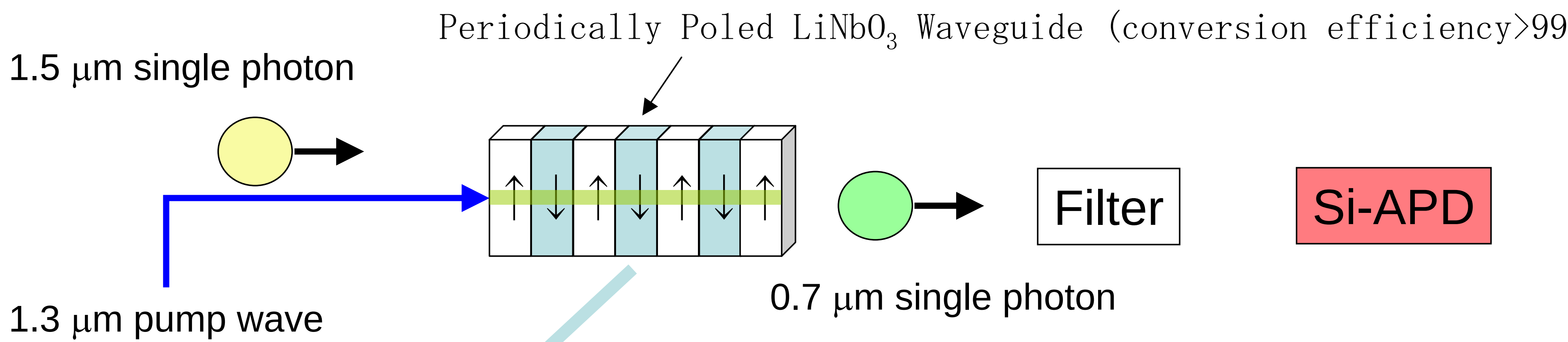
Extinction Ratio > 20 dB

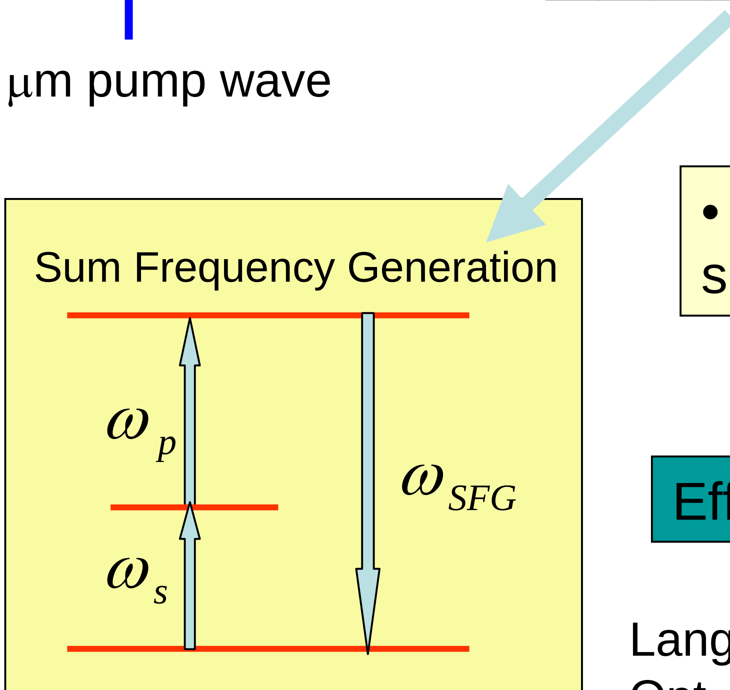
Honjo, Inoue, Takahashi, Opt. Lett., 29, 2797 (2004).

Single Photon Counting InGaAs APD vs Si APD

	InGaAs	Si
Wavelength [nm]	1300-1600	500-900
Quantum Efficiency	～10 %	～70 %
Dark Count [Hz]	2×10^4 (typ)	50 (typ)
After Pulse Effect	Large → Gated mode operation (slow repetition)	Small → non-gated mode operation (fast repetition)

Frequency Up-conversion for 1.5μm Single Photon Detection



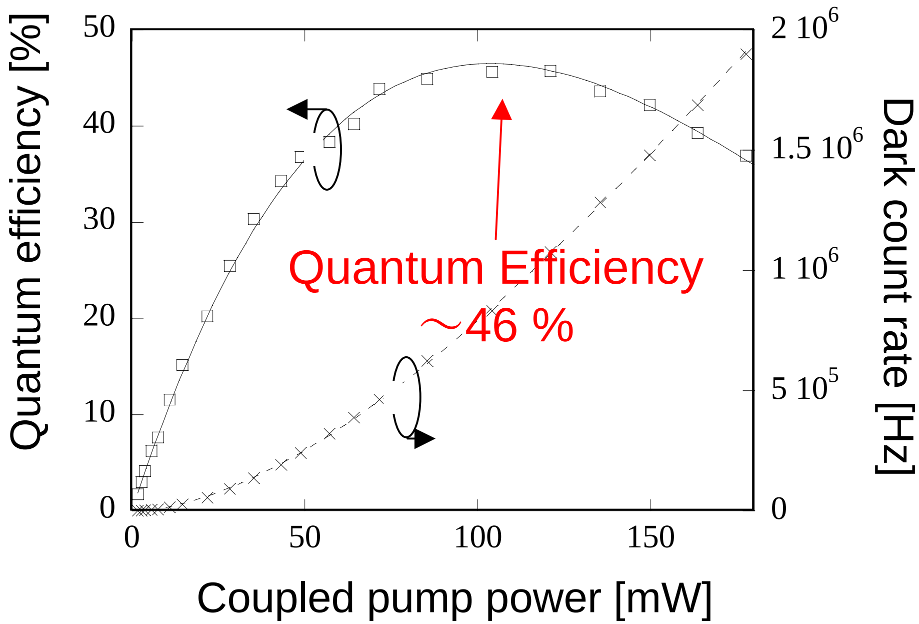


- 1.5 μm single photon is converted to 0.7 μm single photon and is detected by Si-APD.

Efficient and fast single photon detector at 1.5 μm

Langrock, Diamanti, Roussev, Yamamoto, Fejer, Takesue, Opt. Lett., 30, 1725 (2005).

Experimental Results

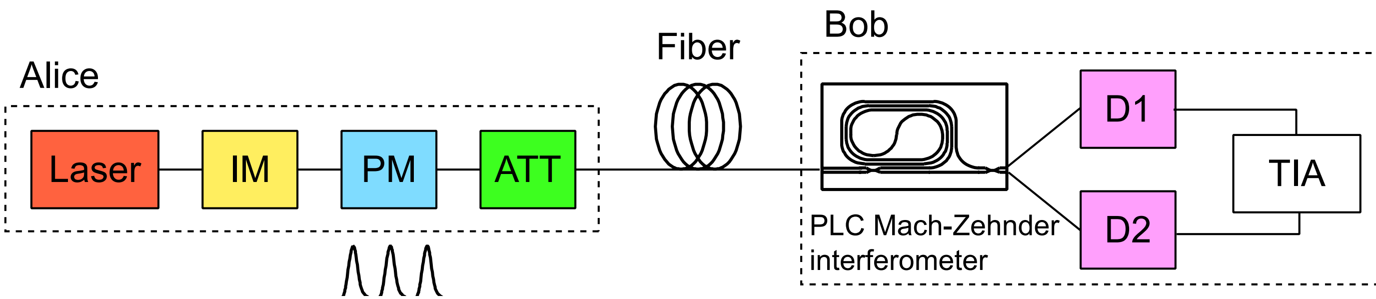


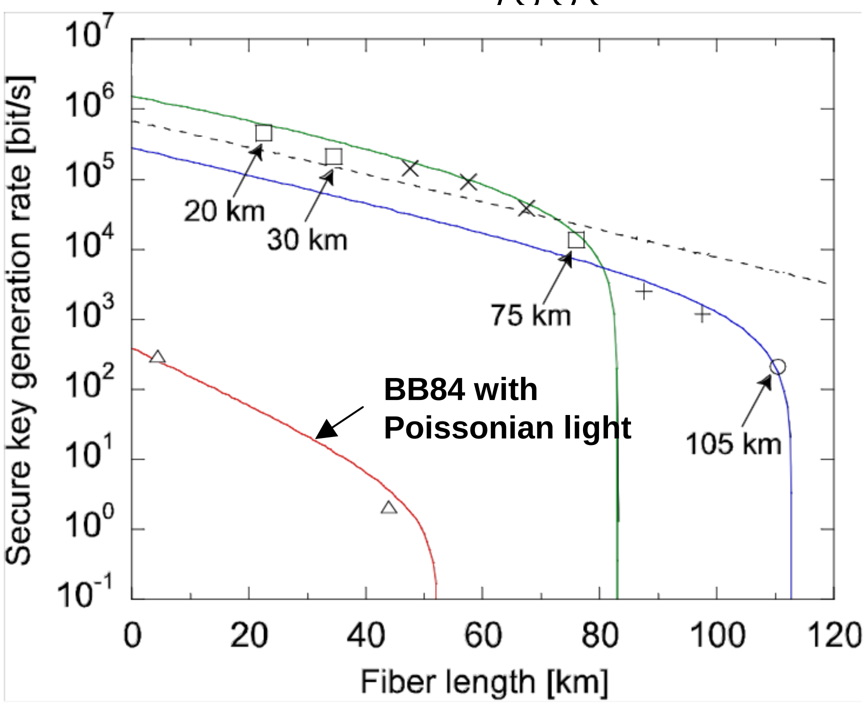
	InGaAs APD	Up-conversion	
Wavelength [nm]	1300-1600	1550 (Bandwidth 0.4 nm)	
Quantum Efficiency [%]	～10 %	46% (peak)	9%
Dark count [Hz]	20 k (typ)	800 k	13 k
Speed	Gated mode (slow)	Non-gated mode (fast)	

GHz Differential Phase Shift QKD Experiment

Security is based on nonlocal phase correlation and non-deterministic state reduction of single photons.

H. Takesue et al. ,quant-ph/0507110 (2005)





If Raman scattering is suppressed in PPLN waveguides,

Single photon BB84-QKD

$\Rightarrow 100\ bit/s$ over $L = 270km$

DPS-QKD

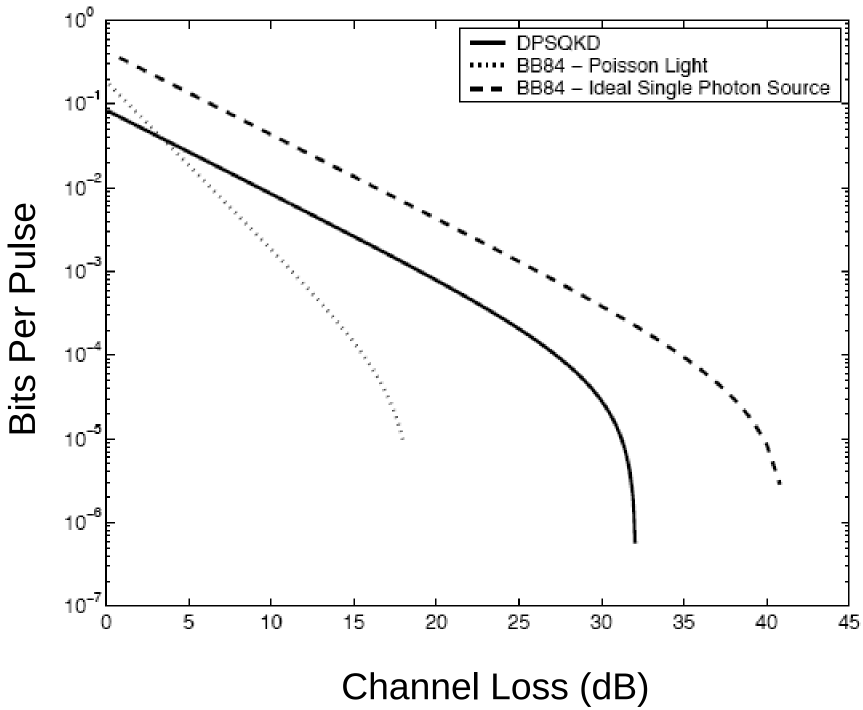
$\Rightarrow 100 bit/s$ over $L = 200km$

BBM92-QKD

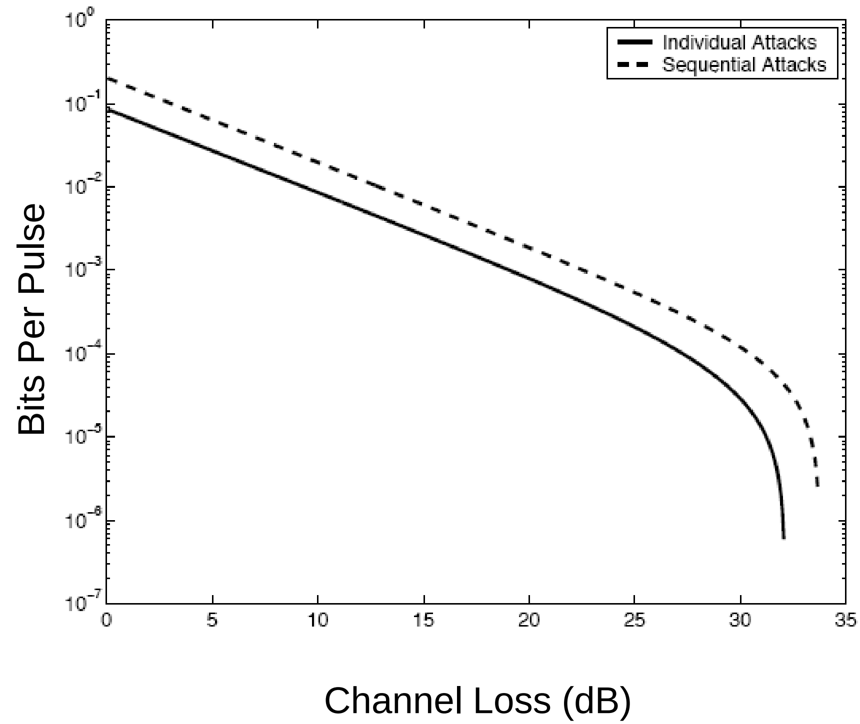
$\Rightarrow 1\ bit/s$ over $L = 380km$

Security Issue — General individual attack —

E. Waks et al. ,quant-ph/0508112 (2005)

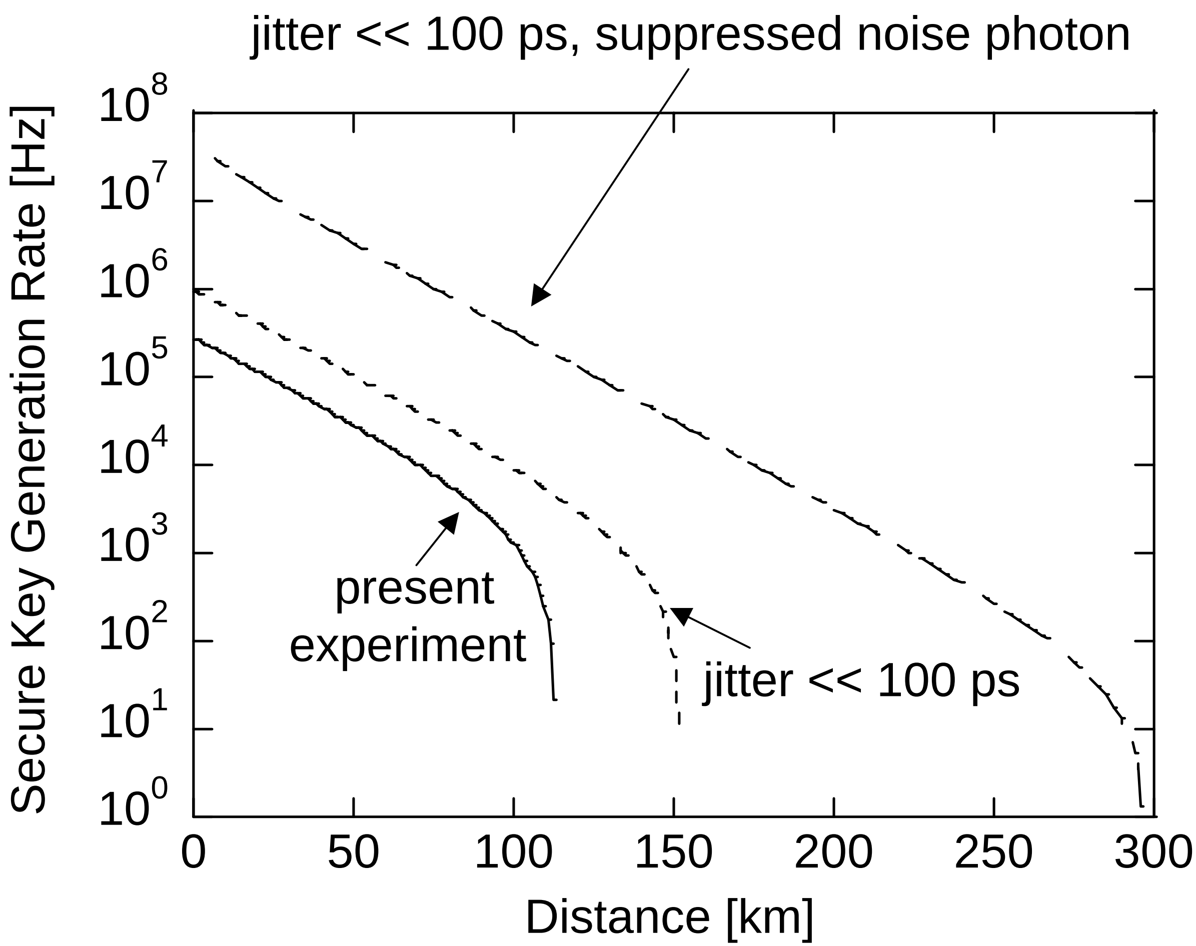


Communication rate vs. channel loss for DPSQKD and BB84.



Comparison of individual attacks to sequential attacks in DPSQKD.

DPS-QKD with Negligible APD Jitter and Suppressed Noise Photons



300 km QKD system is possible

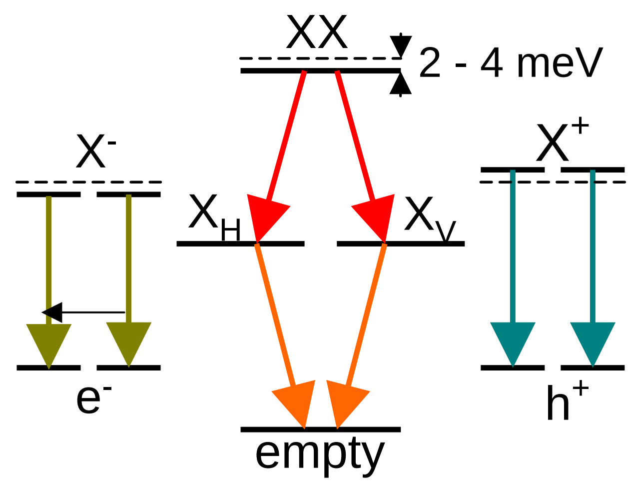
Future Prospect

— Semiconductor Cavity QED System for quantum communication and quantum computation —

QD Spectroscopy: "Artificial Atoms"

- Sharp spectral lines at low temperature $(\lesssim 10\mathrm{GHz})$
- Multiparticle effects $(<50\mathrm{K})$
- Dephasing processes (~1nsec) (phonon,electrostatic)

level diagram:

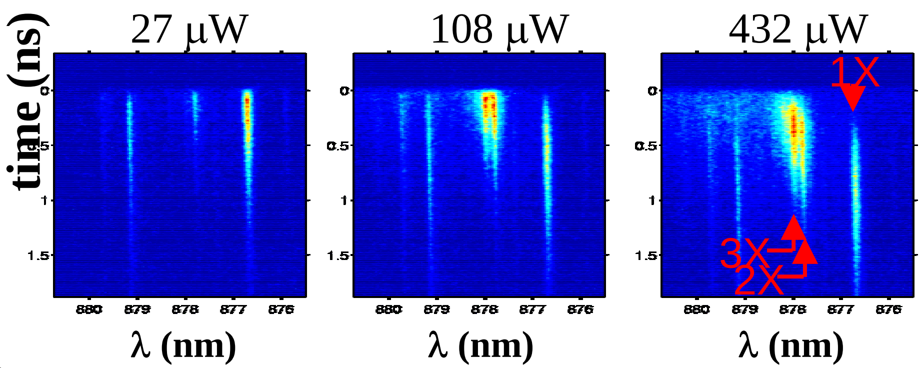


Above band excitation

On resonant excitation at 2e-2h

Suppression of X^- and X^+ lines

Cascade Photon Emission



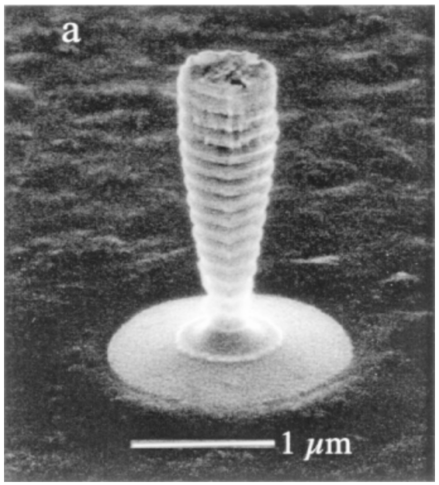
→ Deterministic single photon generation
C. Santori et al., Phys. Rev. Lett. 86, 1502 (2001)

→ Deterministic entangled photon-pair generation
O. Benson et al., Phys. Rev. Lett. 84, 2513 (2000)

$$\frac{1}{\sqrt{2}}\left(|H\rangle_1 |H\rangle_2 - |V\rangle_1 |V\rangle_2\right)$$

Single QD Microcavities

A. Imamoglu (UCSB, Zurich)
J.M.Gerard (CEA Grenoble)
A. Forchel (Würzburg)
A. Scherer (Cal. Tech)
⋮



ECR (I)

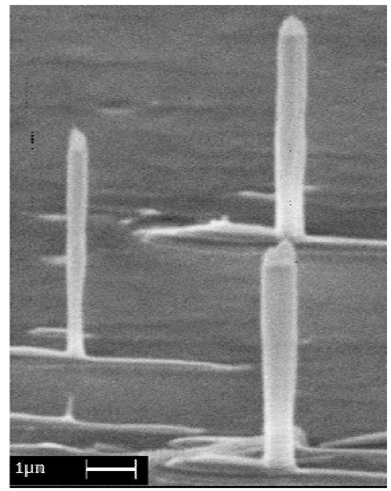
$$Q \approx 300$$

G. Solomon et al.,
Phys. Rev. Lett.
86, 3903 (2001)

ECR (II)

$$Q \approx 800$$

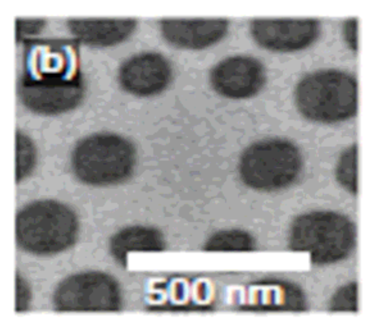
M. Pelton et al.,
Phys. Rev. Lett.
89, 233602 (2002)



CAIBE

$$Q \approx 1200$$

J. Vuckovic et al.,
Appl. Phys. Lett.
82, 3596 (2003)



Photonic Crystal

$$Q \approx 5000$$

D. Englund et al.,
Phys. Rev. Lett.
95, 013904 (2005)

Why indistinguishable single photons and entangled photons from quantum dots/impurities?

- Quantum key distributions free from

  photon splitting attack in BB84 protocol

  uncorrelated photon-pair induced error in Ekert91/BBM92 protocol

  ⇩

  10-100 psec single photons at high repetition frequency

- Quantum repeater based on

  entanglement formation, purification and swapping

  quantum memory (photonic qubit—electronic qubit—nuclear qubit)

  ⇩

  10-100 psec single photon pulse capturing and storage

- Quantum computation based on

  electron spins/nuclear spins in photonic crystal cavity network

  entanglement formation and non-local two-qubit operation

  with single photon or coherent state network

  ⇩

  10-100 psec gate operation time

Why electron spin processor must be integrated with nuclear spin memory in one system?

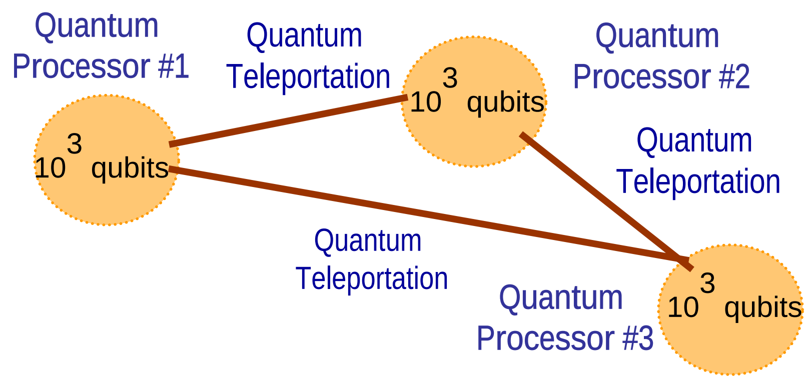
- Long distance quantum communications

GHz QKD without quantum repeaters creates a secure key at ~1 bit/s over 400 Km. Quantum repeaters for terrestrial system (~1,000 Km) and inter-continental system (~10,000 Km) require an operation time of ~1 sec and ~10 sec to complete nested entanglement purification/swapping protocol.

A nuclear spin (T2 >> 1 sec) is a unique choice to store a qubit of information.

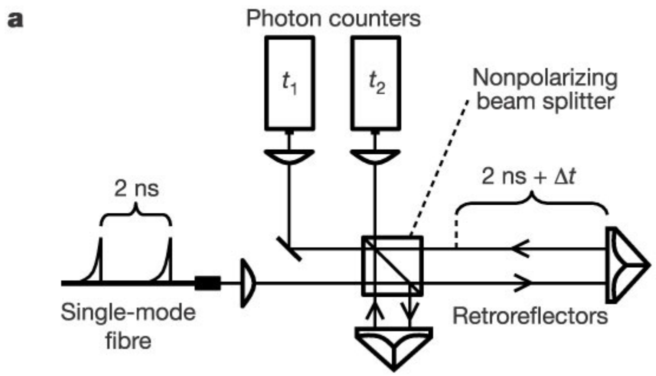
- Large-scale quantum computers

Communication bottle-neck is a severe problem for performing two-qubit operations between distant registers. Nuclear spin memory, electron spin processor and photonic qubit network should be integrated into one system.

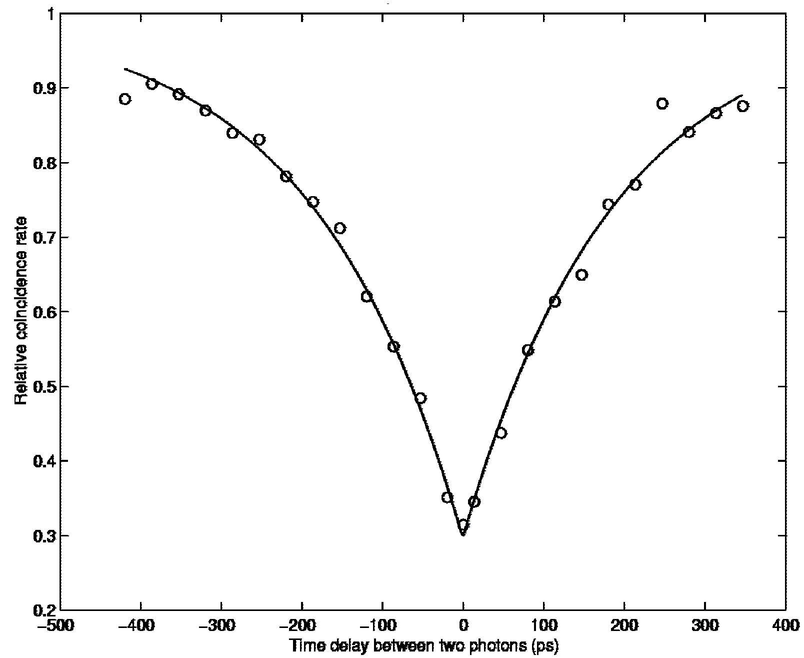


Collision of Two Single Photons

C. Santori et al., Nature 419, 594 (2002)



Hong-Ou-Mandel dip

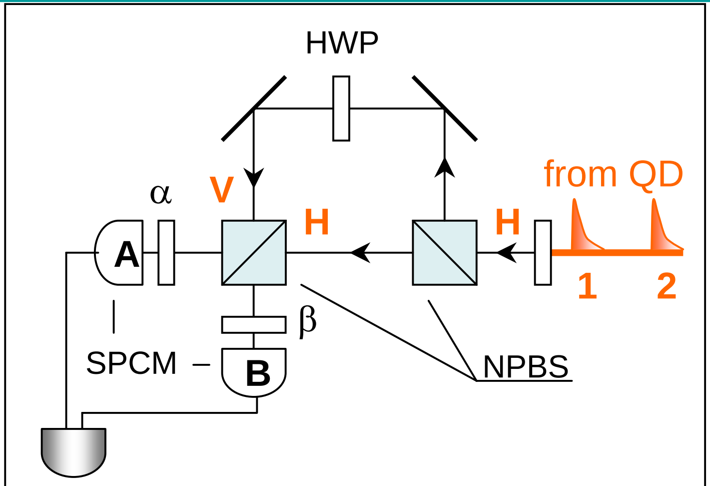


- Negligible jitter (2e-2h → 1e-1h relaxation time ~10 psec) compared to pulse duration
- No phase jump (decoherence time ~1 nsec) in pulse duration

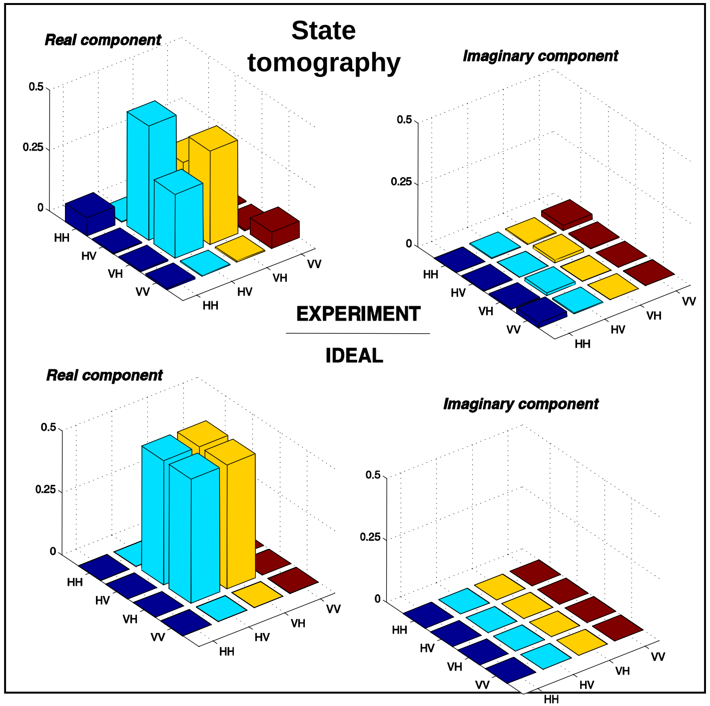
Table 1 **Summary of quantum-dot parameters**

	$g^{(2)}$	g	τ_s (ps)	τ_c (ps)	τ_m (ps)	$V(0)$
Dot 1	0.053	0.039	89	48	80	0.72
Dot 2	0.067	0.027	166	223	187	0.81
Dot 3	0.071	0.025	351	105	378	0.74

Violation of Bell's inequality



Coincidence circuit = ***post-selection***



D. Fattal *et al.*, PRL 92, 037903 (2004)

- Input : $|H\rangle_1 |H\rangle_2$
- Output : $\frac{1}{2}(|H\rangle_A |V\rangle_B - |V\rangle_A |H\rangle_B)$

Analyzer angles used in experiment:

α = 0/90° α' = 45/135°

β = 22.5/112.5° β' = 67.5/157.5°

S_{CHSH} = 2.377 ± 0.18 > 2

❑ Scheme relies on quantum interference between two **independent** single photons from a QD.

❑ Entanglement is induced by the measurement: **NO optical non-linearity** required.

❑ Ideal efficiency is ½.

❑ Only **single** pairs are created.

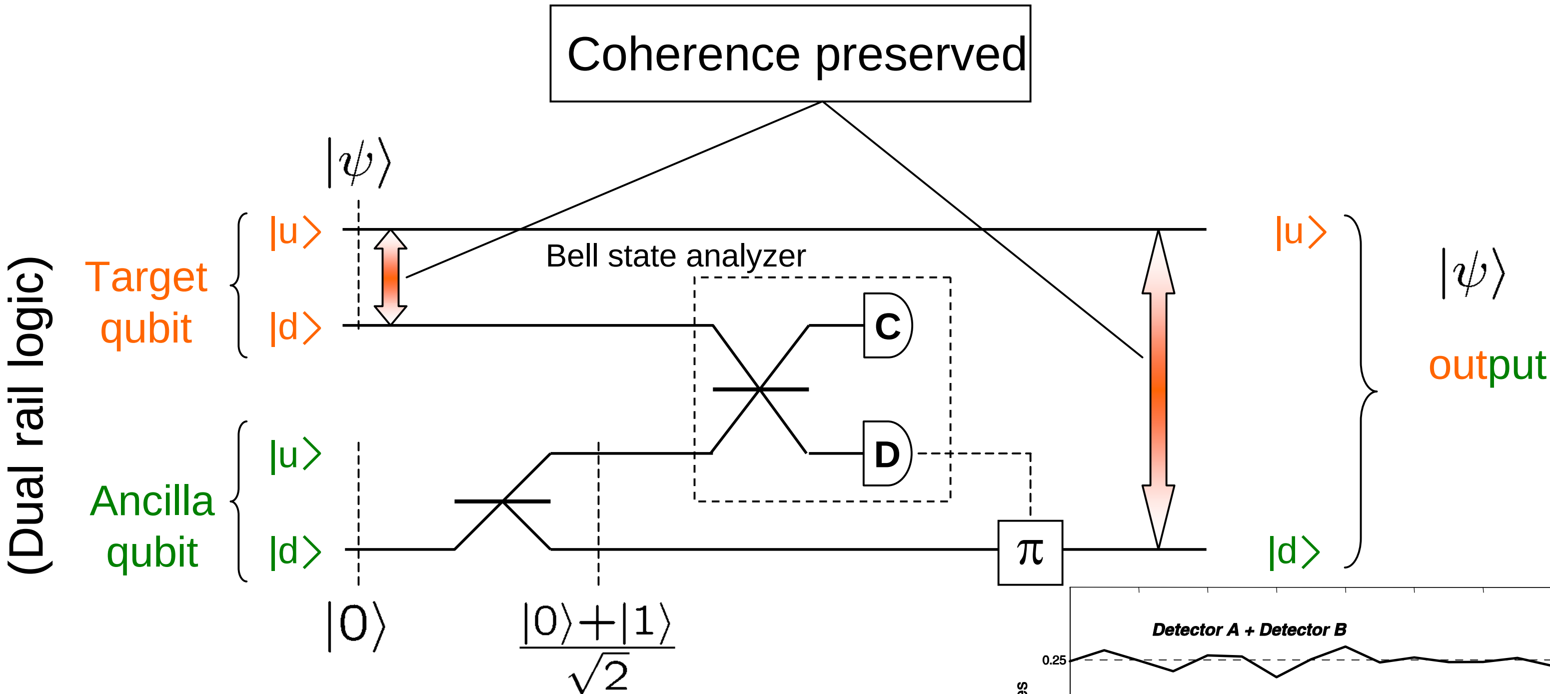
❑ Application to ***BBM92* QKD**.

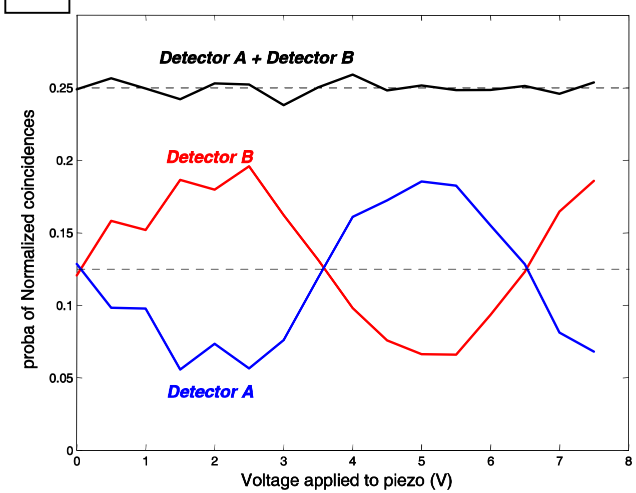
❑ Opens the way to efficient generation of **multi-particle entanglement** and **linear-optics quantum computing**…

Mixed state due to $g^{(2)}(0) \neq 0$ and $V(0)<1$.

Single Mode "Teleportation"

D. Fattal *et al.*, PRL 92, 037904 (2004)

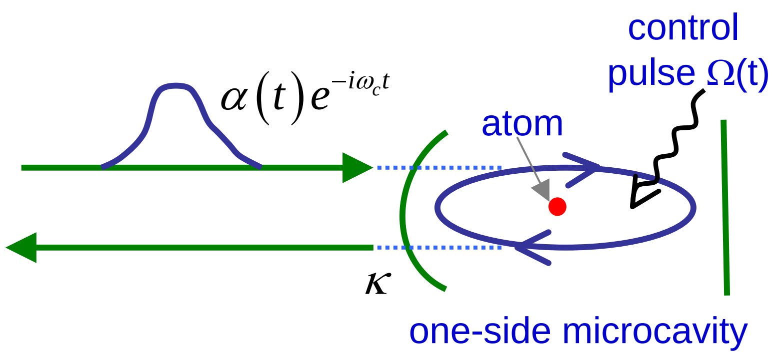




- No entangled state needed for input
- Proba of success = 1/2
- Building block of Linear-optics QC

E. Knill, R. Laflamme and G.J. Milburn, Nature 409, 46 (2001)

Nonadiabatic Coherent Trapping and Emission of Arbitrary Single Photon Pulses



$$|\psi(t)\rangle = e(t)|e,0\rangle + r(t)|r,0\rangle + g(t)|g,1\rangle$$

atomic state

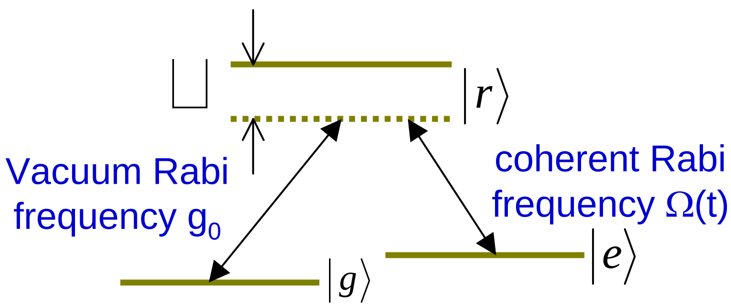
cavity state

rotating wave approximation, standard in-out coupling formalism

$$\frac{dg(t)}{dt} = -ig_0\, r(t) - \frac{\kappa}{2} g(t) + \sqrt{\kappa}\,\alpha(t)$$

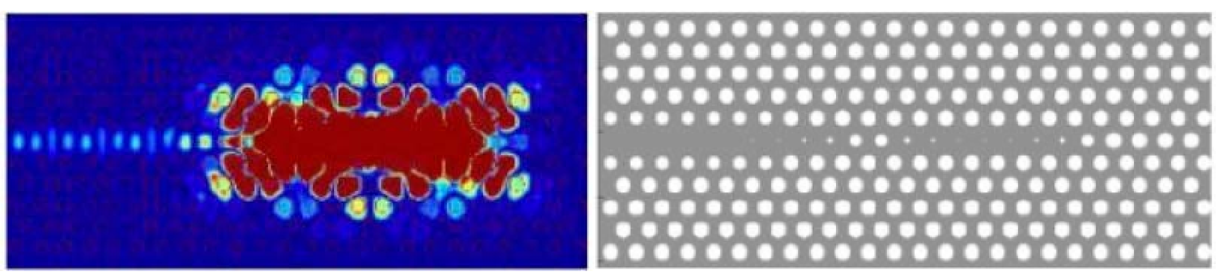
$$\frac{dr(t)}{dt} = -i\Delta r(t) - ig_0\, g(t) - i\frac{\Omega(t)^*}{2} e(t)$$

$$\frac{de(t)}{dt} = -i\frac{\Omega(t)}{2} r(t)$$



If $\alpha(t)$ is known, find $\Omega(t)$ so that

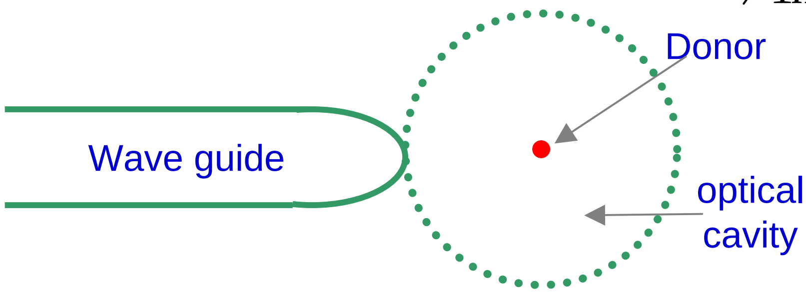
$$|\psi_{in}\rangle = |g,0\rangle \rightarrow |\psi_f\rangle = |e,0\rangle$$ ······· **Complete trapping**

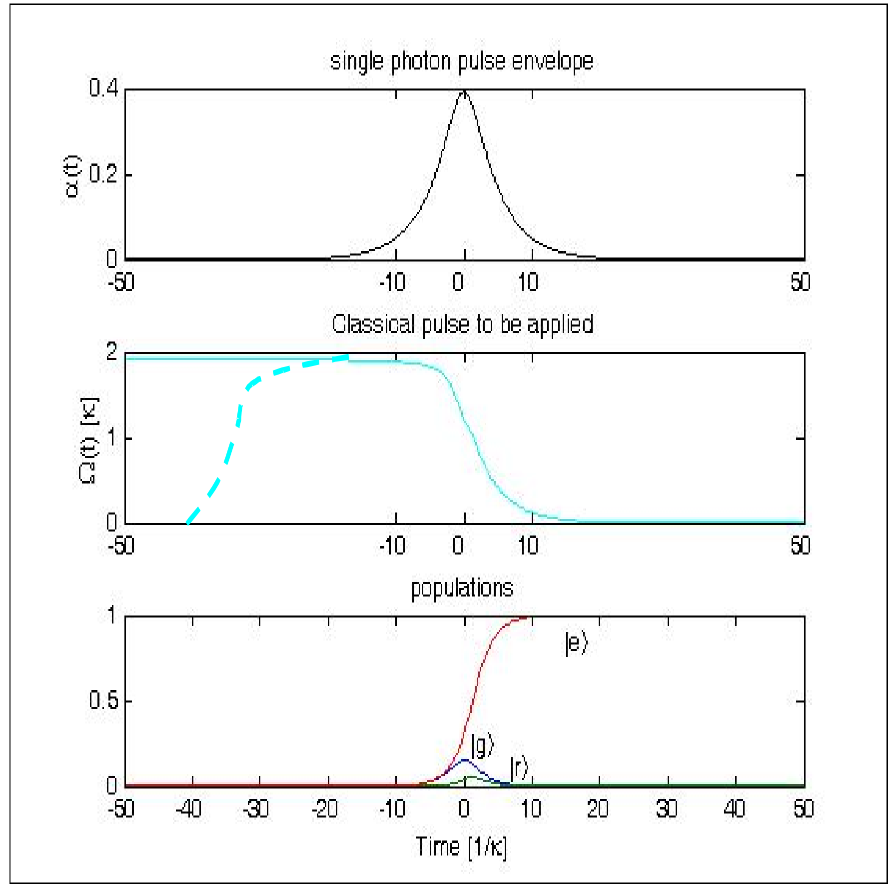


Applications to Quantum Information Systems

An experimental system: donor impurity in photonic crystal cavity

$$\gamma\left(\text{spontaneous decay rate}\right) \sim 1/_{1\text{ns}},\quad \kappa \sim 1/_{10\text{ps}},\quad g_0 \sim 1/_{10\text{ps}}$$





1. Deterministic single photon generation

$$\left(\left|\psi_{in}\right\rangle = \left|e,0\right\rangle\right)$$

pulse duration $\lesssim$10 ps,
quantum efficiency $\gtrsim$99%,
QM overlap $\gtrsim$98%,
no jitter, complete control of pulse amplitude

2. Single photon detector with coherent state probe after trapping

quantum efficiency $\gtrsim$99%,
no dark count,
dead time $\lesssim$100 ps