Lund

~100.000 inhabitants, ~40.000 students

The Dome

The main University Building

Control at the quantum level

Stefan Kröll

Lund University

Knut och Alice Wallenbergs Stiftelse

Vetenskapsrådet

Lund Laser Centre

QuReP

Quantum Repeaters for Long Distance Fibre-Based Quantum Communication

<Q|A|P>

Outline

- Some reflections regarding the beginning of the field of quantum computing and why might quantum computers be interesting
- How to construct quantum computers
- The Lund approach to quantum computing
- Quantum memories for quantum cryptography
  - The most efficient quantum memories today, how do they work and how are they made

LUND UNIVERSITY

Outline

- **Some reflections regarding the beginning of the field of quantum computing** & why quantum computers might be interesting
- How to construct quantum computers
- The Lund approach to quantum computing
- Quantum memories for quantum cryptography
  - The most efficient quantum memories today, how do they work and how are they made

LUND UNIVERSITY

Computing, history

- There is a universal Turing machine that can simulate any other Turing machine
  - Alan Turing 1936
- If an algorithm can be performed at any class of hardware, then there is an equivalent efficient algorithm for a Turing machine
  - Church-Turing thesis (strong version)

(Quantum) computing, history

- Rolf Landauer, IBM, 1960ies
  - From an entropy point of view a computation consumes an energy $>kT*\ln(2)$ ($\sim 3*10^{-21}$ J) per bit information erased or discarded
  - A reversible computer, which after the computations just prints the answer and then reverse its operations going back to the original state, could give a much lesser entropy change and thus could be much more energy efficient

Information is physical

Rolf Landauer

(Quantum) computing, history

- Charles Bennett, IBM, 1973
  - It is in principle possible to construct a reversible Turing machine with essentially the same performance as a Turing machine

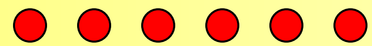
Regarding operations on quantum systems

- Generally a quantum system, Ψ, at time t_2 can be related to its state at some earlier time, t_1, by a unitary transformation U
- $\Psi(t_2)=U\Psi(t_1)$
- Clearly, if we expose the system at time t_2 to U^{-1}, the original state is obtained
- $U^{-1}\,\Psi(t_2) = U^{-1}\,U\,\Psi(t_1) = \Psi(t_1)$

Quantum computing, history

- Paul Benioff, Argonne National Lab., 1982
  - For any arbitrary Turing machine carrying out a calculation, Q, in N steps, there is a set of states, Ψ, and a hamiltonian, H, such that the time development of Ψ under H reproduces the calculation of Q by the Turing machine.
  - Benioff also shows that a quantum mechanical implementation of a Turing machine is as least as efficient as a classical Turing machine and it would in principle not need to consume any energy for its calculations

Simulation of N coupled quantum systems (R Feynman 1982)



N qubits

For large N such a quantum system is too complex to be simulated by a (classical) computer

Quantum computing, history

- David Deutsch, Oxford, 1985
  - Deutsch argues (and shows) that, as for classical computers, it should be possible to program a quantum computer to carry out arbitrary operations
  - Such quantum computers would have properties different from classical computers, e. g., quantum computers would be faster on certain calculations due to 'quantum parallelism'

In quantum computers data is represented by quantum bits (qubits)

- A qubit is a quantum mechanical systems with two states |0> and |1> that can be in any arbitrary superposition

$$\Psi = \alpha|0\rangle + \beta\,|1\rangle$$

of those states

Superposition of states makes a quantum computer (QC) powerful

Input data (4 bits)

Input data (4 qubits)

$(|0>+|1>)/\sqrt{2}$ 0

$(|0>+|1>)/\sqrt{2}$ 1

$(|0>+|1>)/\sqrt{2}$ 1

$(|0>+|1>)/\sqrt{2}$ 0

Quantum Computer

Input ≡ 0110

(|0>+|1>) (|0>+|1>) (|0>+|1>) (|0>+|1>)/4=

=(|0000>+|0001>+|0010>+|0011> . . . +|1111>)/4

LUND
UNIVERSITY

Quantum parallelism

- Consider an operation, *f*, performing the operation *f(x)* on a state *x* and putting the result in *y*. For a system $|x, y>$ we obtain for $x= (|0>+|1>)/\sqrt{2}$
- $|x,y>= [|0,f(0)>+|1,f(1)>]/\sqrt{2}$
- By performing the operation *f* on state *x*, *f*(0) and *f*(1) have been calculated in one operation.

Quantum parallelism

- Such a ’quantum parallelism' is not automatically useful because a measurement on system $|x,y>$ will collaps the superposition $[|0,f(0)>+|1,f(1)>]/\sqrt{2}$ to either the first or the second term
- However, in a measurement where $f(0)$ and $f(1)$ interferes, global properties of f, requiring that both values have been calculated can be obtained

Quantum parallelism

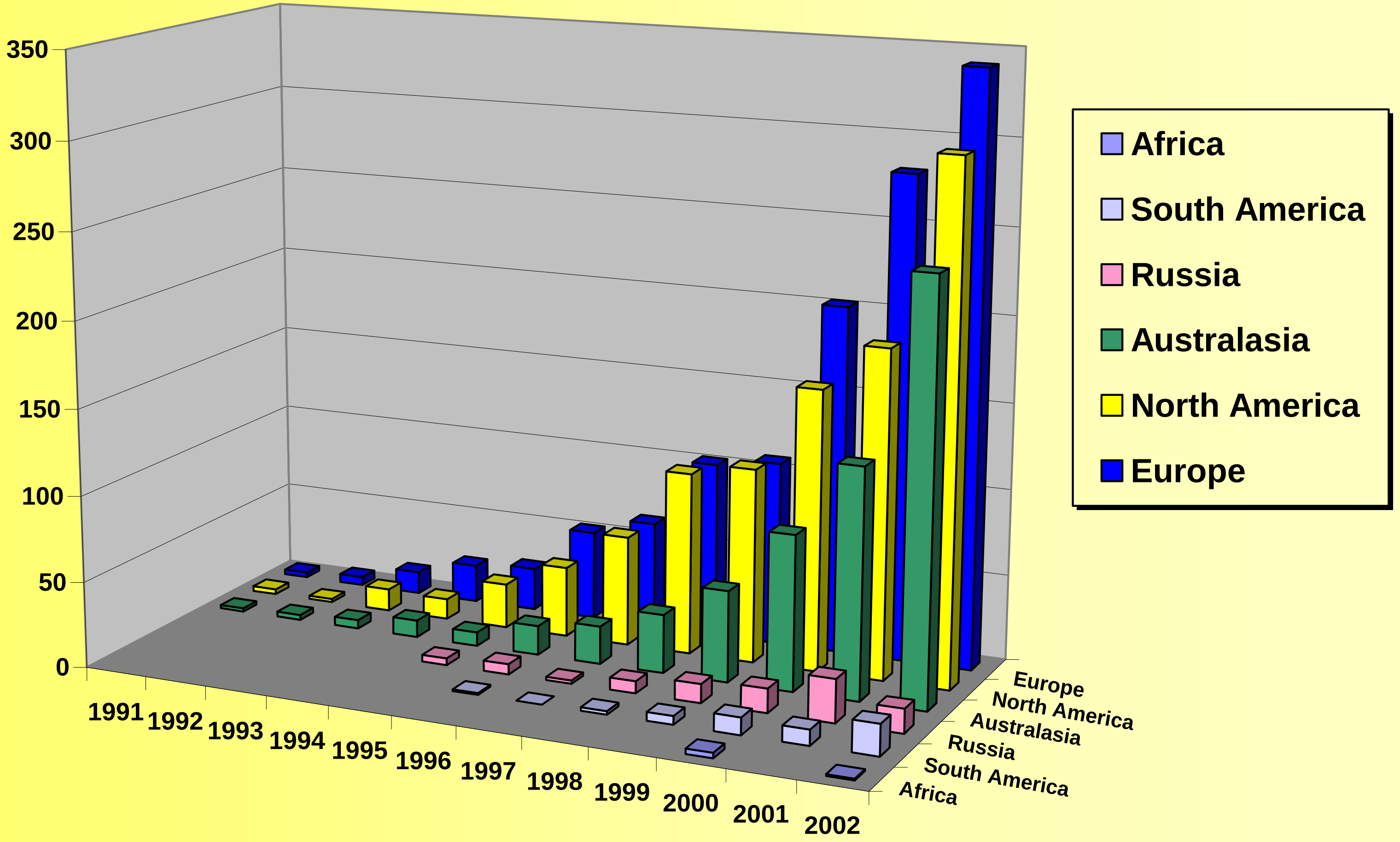
- More generally, if x *is* represented by n quantum bits it can be a superposition of 2^n values. The function f is then evaluated in 2^n points in one step.

LUND UNIVERSITY

Quantum computing, history

- Peter Shor, ATT Bell laboratories, 1994
  - Quantum algorithms for prime number factorisation much more efficient than the best known algorithms for classical computers
  - Encryption, security protocols on the internet and elsewhere

Papers published in quantum information science



Quantum computing impacts the landscape of computer science

- QC algorithms do not violate the Church-Turing thesis:
  - any algorithmic process can be simulated using a Turing machine
- QC algorithms challenge the strong version of the Church-Turing thesis
  - If an algorithm can be performed at any class of hardware, then there is an equivalent efficient algorithm for a Turing machine

Outline

- Some reflections regarding the beginning of the field of quantum computing and why might quantum computers be interesting
- How to construct quantum computers
- The Lund approach to quantum computing
- Quantum memories for quantum cryptography
- The best quantum memories today, how do they work and how are they made

Why is QC interesting?

- A quantum computer would be able to solve some problems which are untractable on conventional computers, such as, certain computationally hard problems
- **QC is a structured way to learn how to control quantum systems and how to design fully controllable quantum systems**

Why is QC interesting?

- **A quantum computer can solve some problems which are untractable with conventional computers, such as, certain computationally hard problems**
- QC is a structured way to learn how to control quantum systems and how to design fully controllable quantum systems

Computationally hard problems

- The number of steps required to solve the problem using the best known algorithms on classical computers increase exponentially with the size of the problem
- For some of these problems there are, however, quantum algorithms where the number of steps only increase polynomially

Computationally hard problems

- Consider a computationally hard problem with an input represented by n=25 bits that takes 1 hour to solve on a classical computer (computation time goes as 2^n)
- It will take 1000 years to solve an n=50 qubit input problem
- While it on a quantum computer (computation time goes as n^2) the time would go from 1 hour to 4 hours.

Fourier transforms

- Fast Fourier transform on a function represented by $N=2^n$ numbers
- Classically this requires $N\log_2(N)=n2^n$ steps
- On QC $[\log_2(N)]^2= n^2$ steps
- This looks fantastic!
- However, we do not have full information, readout will collapse the state

Multiple qubits

- N qubits span a computational basis $|x_1,x_2,x_3 \ldots ,x_N>$
- The quantum state is specified by 2^N amplitudes
- Lets say N ≈ 500 would it be difficult to store these amplitudes?
- The number of amplitudes is larger than the estimated number of atoms in the universe

Power of quantum computers

- The quantum corollary to Moore’s law could essentially be something like ”a single qubit will be added to quantum computers every 18 months”

Outline

- Some reflections regarding the beginning of the field of quantum computing and why might quantum computers be interesting
- How to construct quantum computers
- The Lund approach to quantum computing
- Quantum memories for quantum cryptography
  - The most efficient quantum memories today, how do they work and how are they made

Requirements for quantum computing

(Di Vincenzo criteria)

- Coherent two-state systems acting as qubits
- Possibility to manipulate the qubits individually (single qubit operations)
- Coupling between any two qubits (two-bit gates)
- Possibility for reliable read-out of the individual qubits
- Scalability

Why is it difficult to construct a quantum computer

- The quantum bits must remain in superposition states all through the calculations – Thus the quantum bits must not interact with the environment
- Quantum logics requires that bits can control each other – Thus the quantum bits must interact with each other

Will there be quantum computers?

Quantum error correction

- There are efficient error correction algorithms for correcting errors in quantum computer operation when the error per operation is $< 10^{-4}$ ($<10^{-2}$)
- If quantum operations can be performed with a fractional error of less than 10^{-4} we can keep an arbitrary large quantum system coherent for an arbitrary long time!

Outline

- Some reflections regarding the beginning of the field of quantum computing and why might quantum computers be interesting
- How to construct quantum computers
- The Lund approach to quantum computing
- Quantum memories for quantum cryptography
  - The most efficient quantum memories today, how do they work and how are they made

Requirements for quantum computing

- **Coherent two-level systems acting as qubits**
- Possibility to manipulate the qubits individually (single qubit operations)
- Coupling between any two qubits (two-bit gates)
- Possibility for reliable read-out of the individual qubits
- Scalability

1. Coherent

Compared to what?

Choosing a good system

$$N_{operation} = \frac{T_{coherence}}{T_{singleoperation}}$$

Strong interaction

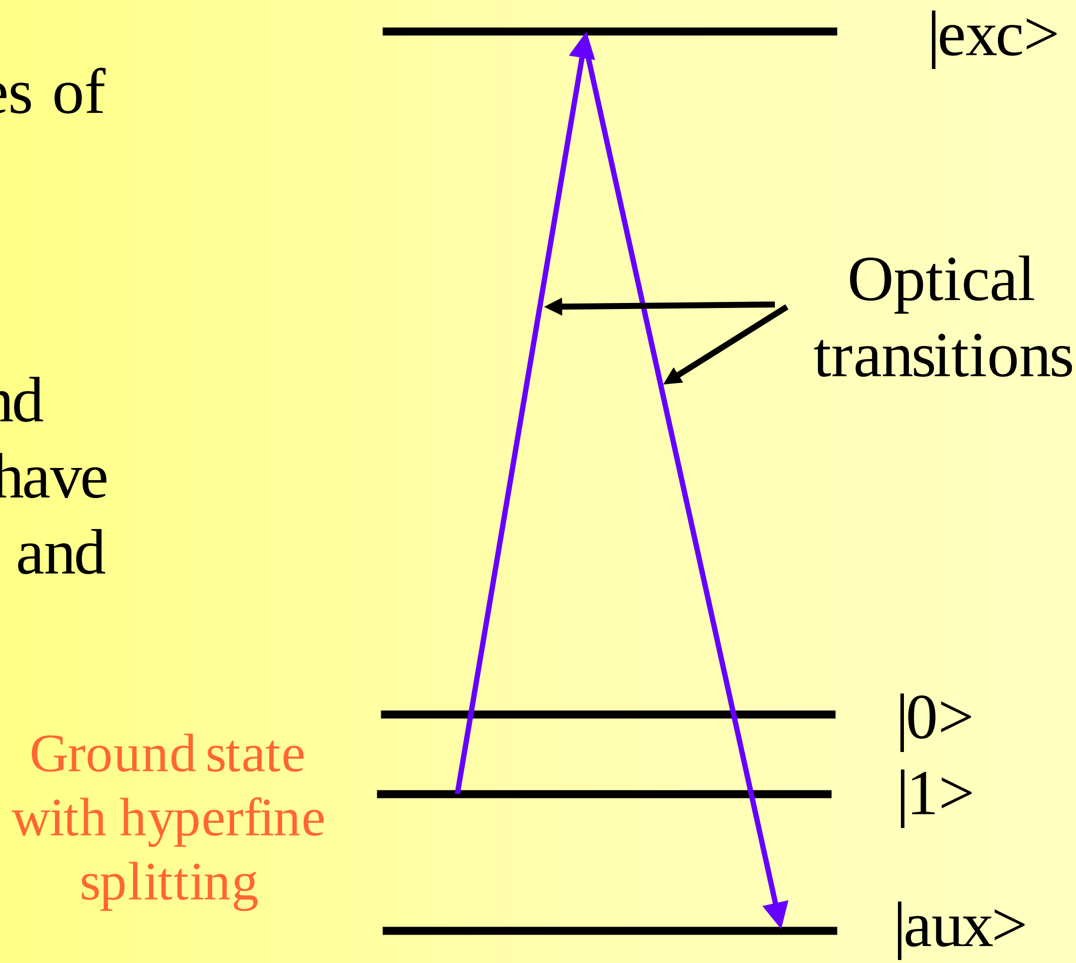
The rare-earth-ions hyperfine states are used as qubit states

LUND UNIVERSITY

- Long coherence times of the optical transitions (up to several ms)

- At 4 Kelvin the ground state hyperfine levels have ms-s coherence times and very long lifetimes (~ hours)

- π-pulse takes < 1 μs

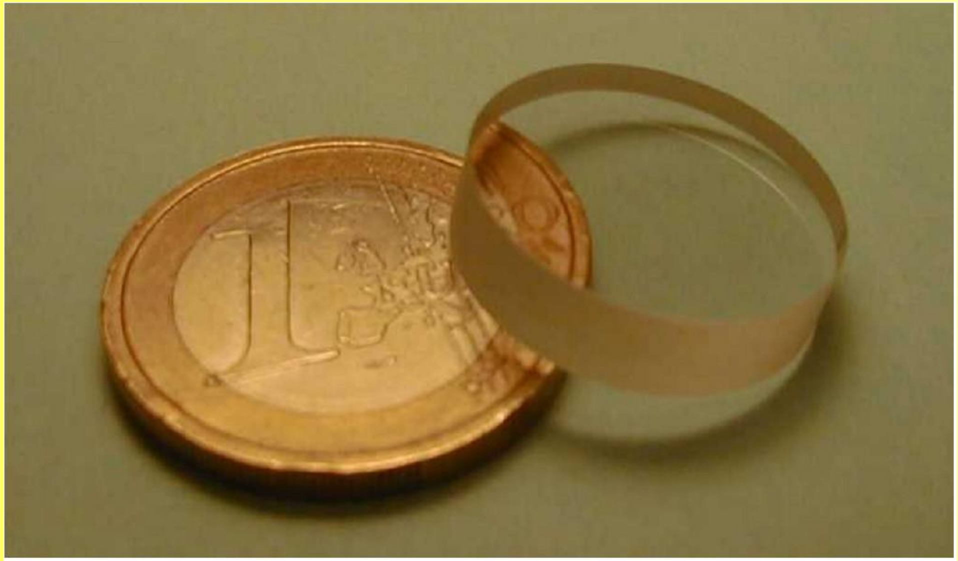


LUND UNIVERSITY

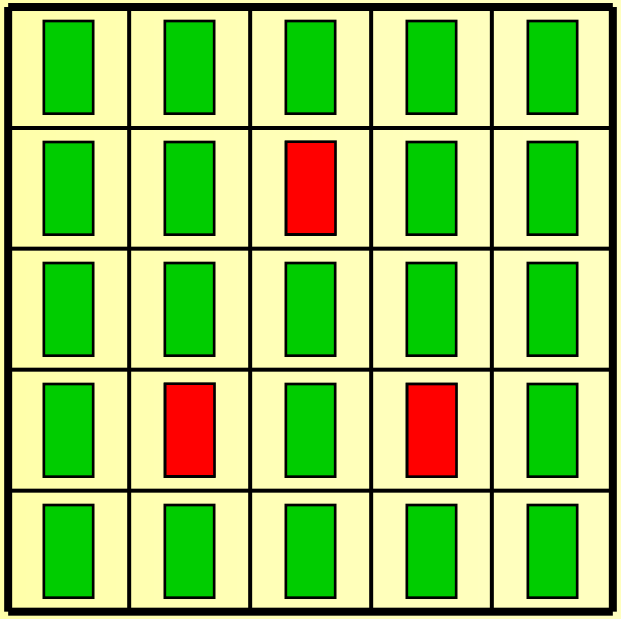
Requirements for quantum computing

- Coherent two-level systems acting as qubits
- **Possibility to manipulate the qubits individually (one-bit gates)**
- Coupling between any two qubits (two-bit gates)
- Possibility for reliable read-out of the individual qubits
- Scalability

Crystal structure

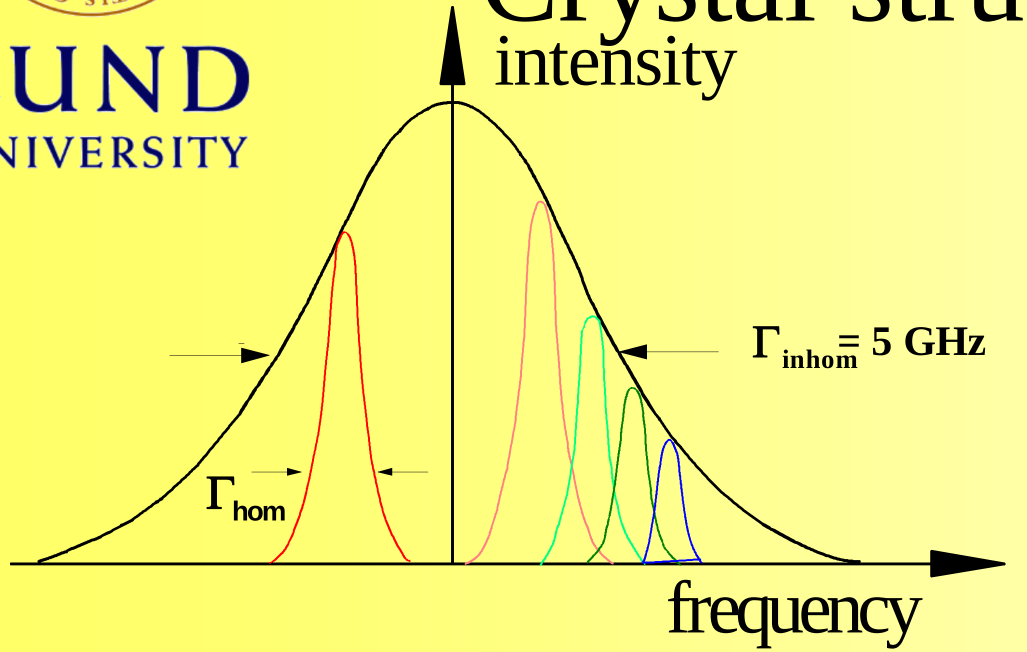


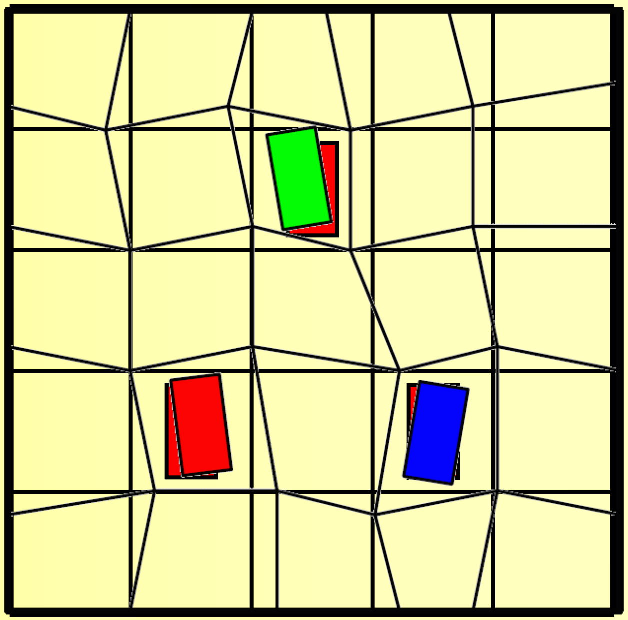
Conceptual picture of crystal



$Pr^{3+}:Y_2SiO_5$

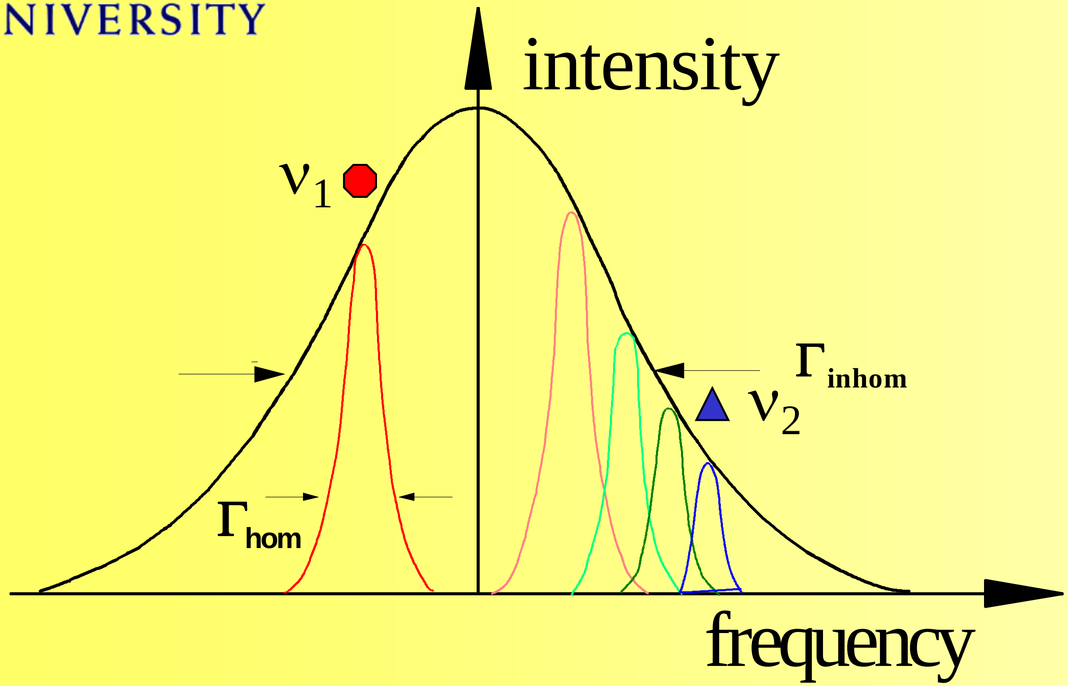
Crystal structure





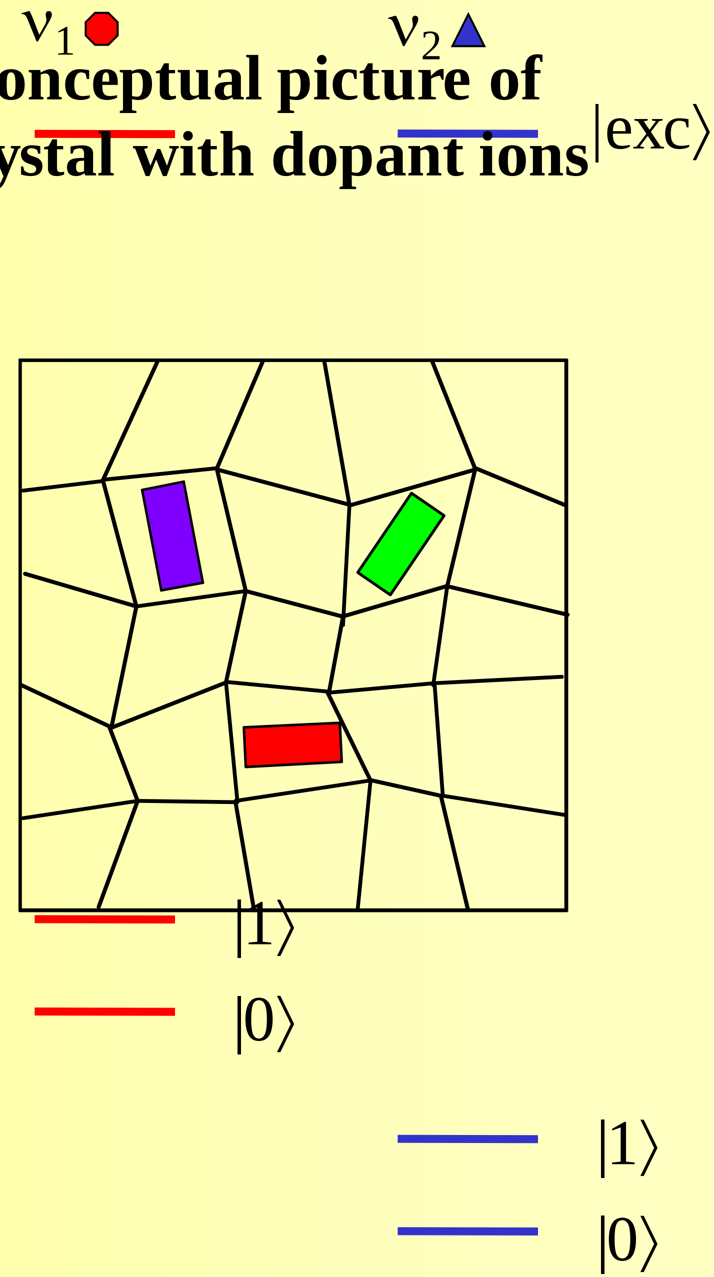
$Pr^{3+}:Y_2SiO_5$

Absorption line from dopant ions in a rare earth doped inorganic crystal



- Narrow homogeneous line-widths (1-10 kHz)
- Large inhomogeneous line-widths (1-200 GHz)

Conceptual picture of crystal with dopant ions

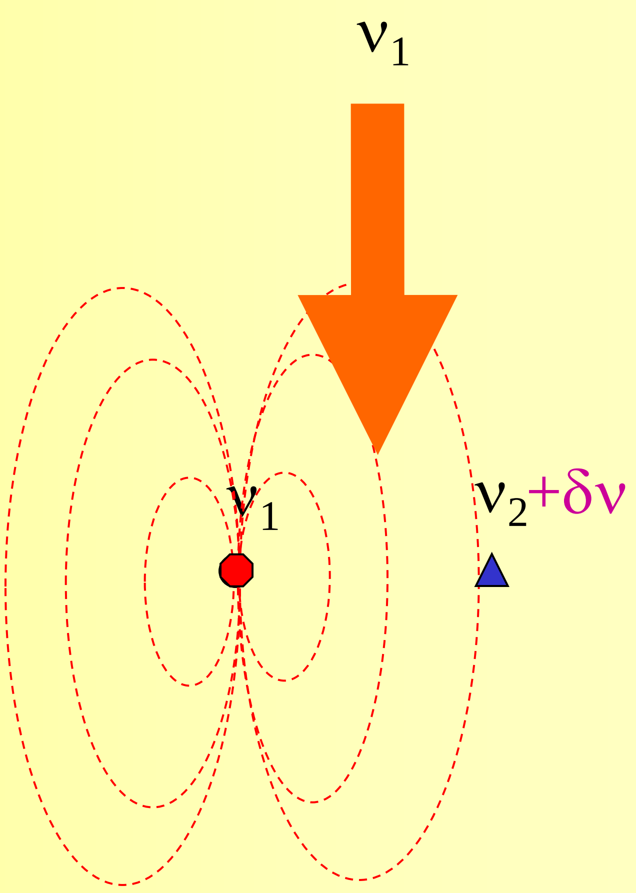


Requirements for quantum computing

- Coherent two-level systems acting as qubits
- Possibility to manipulate the qubits individually (one-bit gates)
- **Coupling between any two qubits (two-bit gates)**
- Possibility for reliable read-out of the individual qubits
- Scalability

Dipole-dipole interaction

1. Two ions absorbing at different frequencies are located close to each other in the crystal lattice. In a non-centrosymmetric site the ions will have a permanent electric dipole moment
2. The ions have a different dipole moment in their excited state. One of the ions is excited on its optical transition
3. This change in dipole moment is sensed by the other ion causing its absorption frequency to change.



Dipole-dipole interaction strength in rare-earth crystals

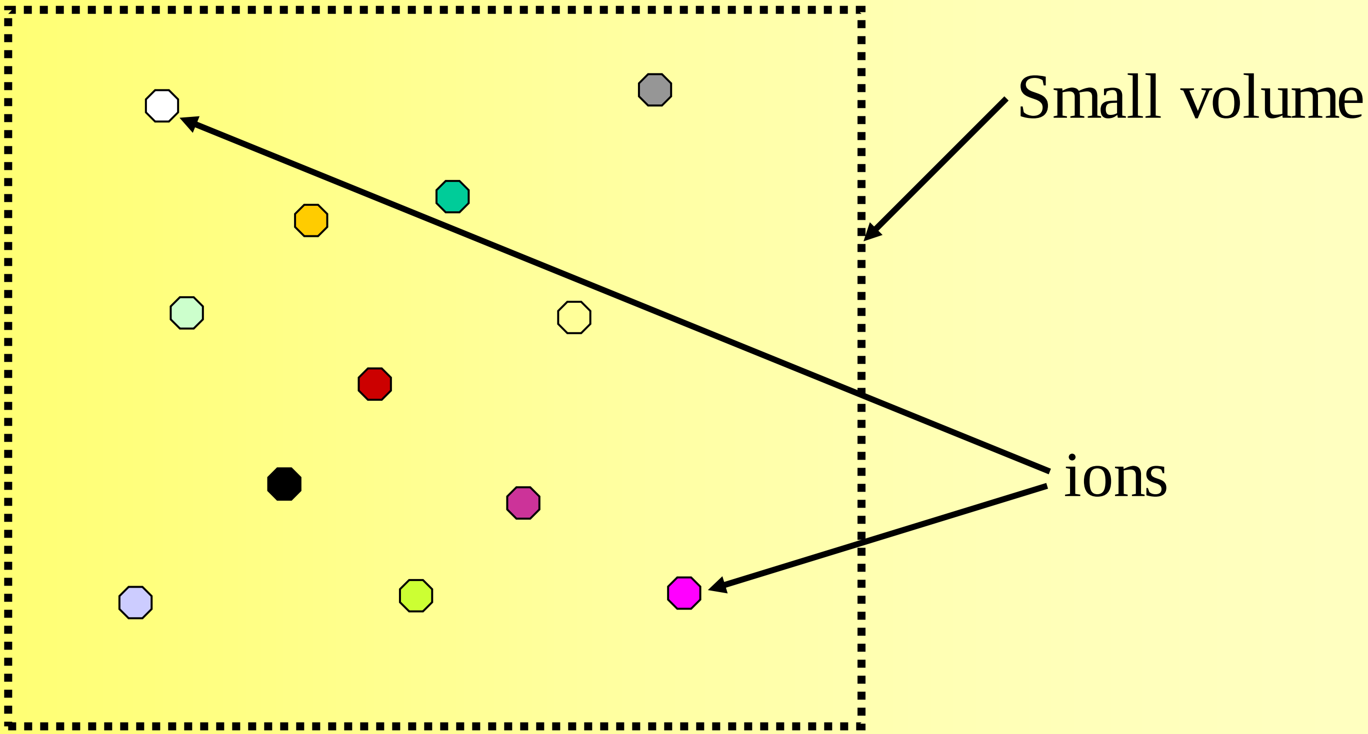
- Approximate numbers

Ion distance	frequency shift
100 nm	1 line width
10 nm	1000 line widths
1 nm	1000000 line widths

Requirements for quantum computing

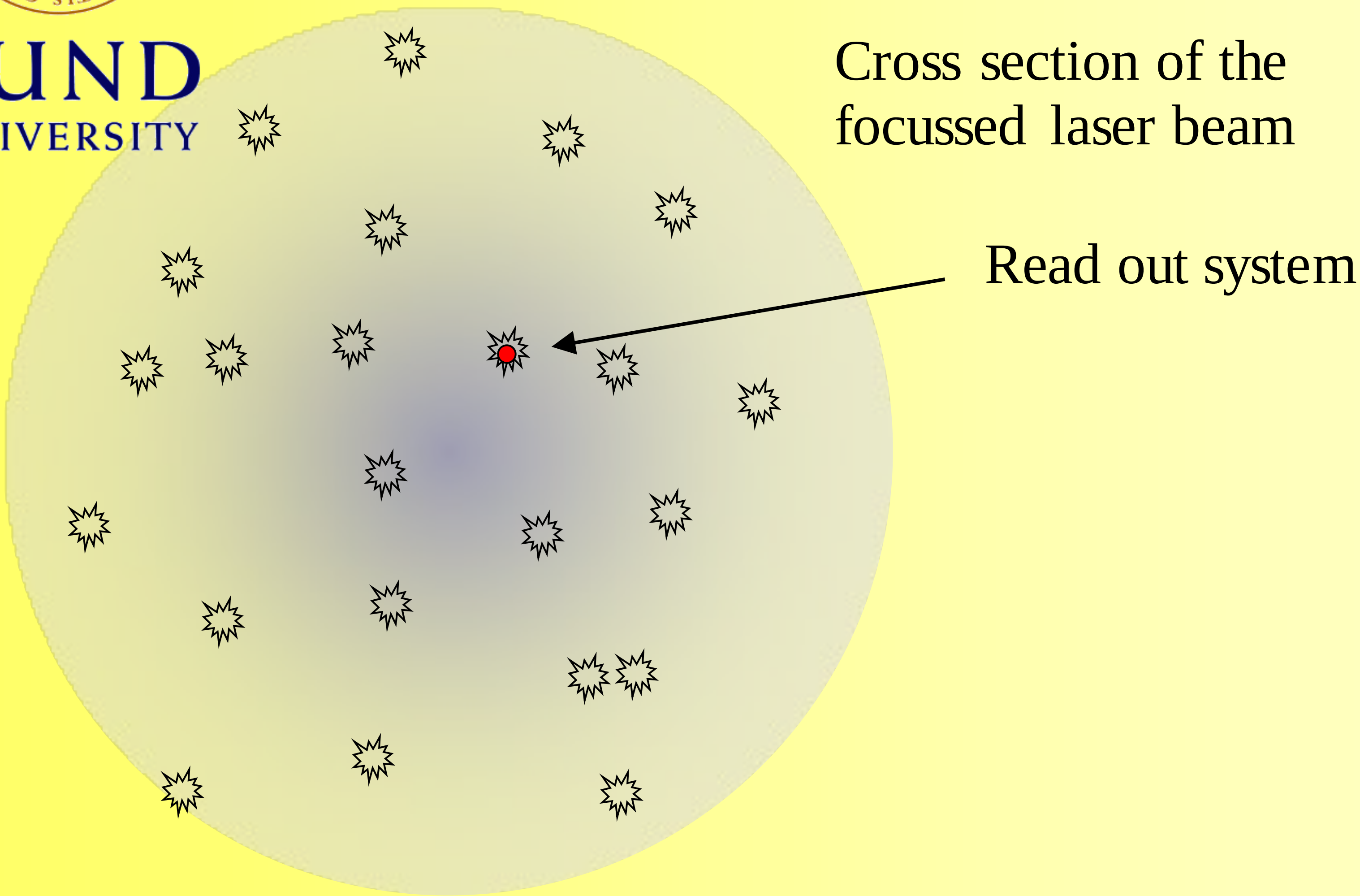
- Coherent two-level systems acting as qubits
- Possibility to manipulate the qubits individually (one-bit gates)
- Coupling between any two qubits (two-bit gates)
- **Possibility for reliable read-out of the individual qubits**
- Scalability

Within a small volume all ions interact strongly

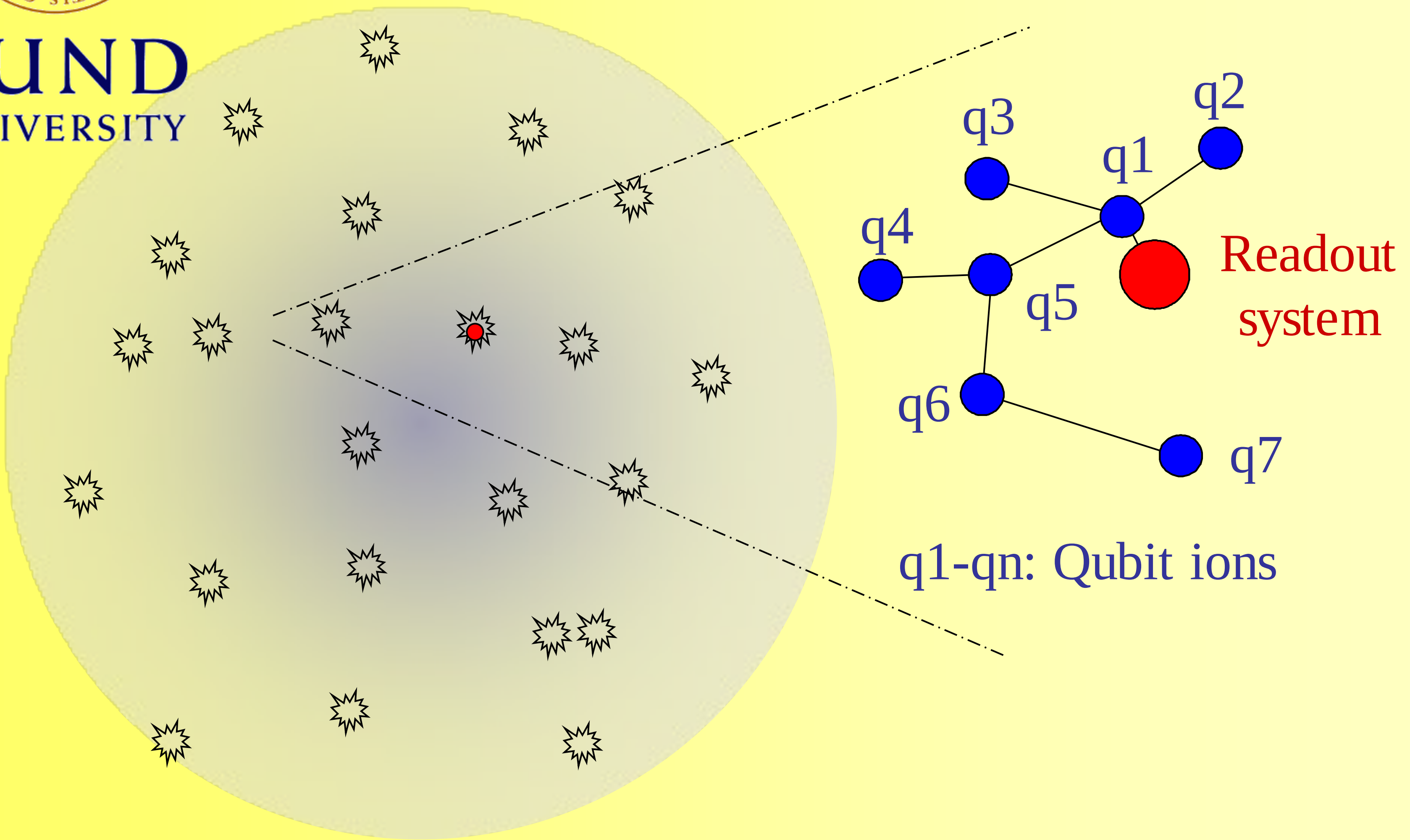


All ions interact strongly, but single ions are difficult to detect

Single ion readout

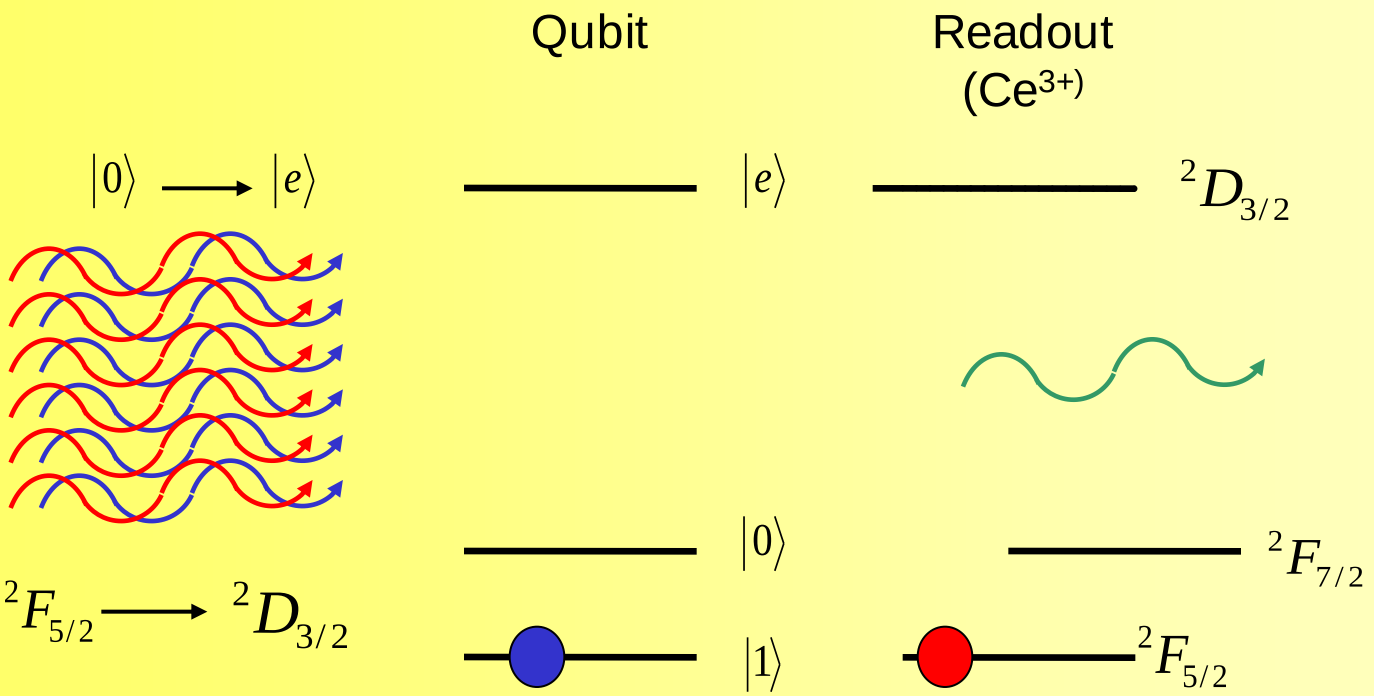


Single ion readout



Single ion readout concept

- The qubit state can be determined from the rate of Ce fluorescence photons



Seelected results

- Multiple instance qubits
  - Qubits initiated in well defined states
  - 97.5% state-to-state transfer efficiency
  - Qubit distillation >90%
  - Arbitrary single qubit operations F>0.9
- Single instance scheme
  - Better fidelities
  - Scalable to severable qubits

Outline

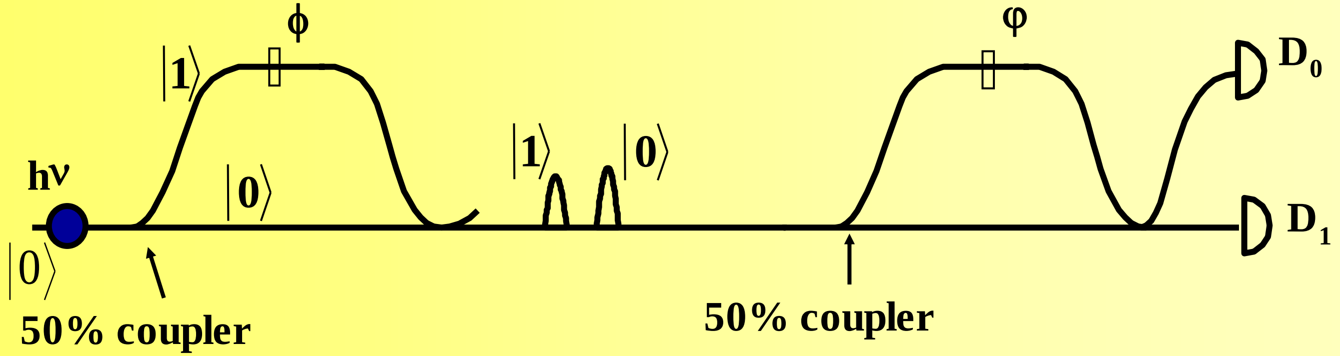
- Some reflections regarding the beginning of the field of quantum computing and why might quantum computers be interesting
- How to construct quantum computers
- The Lund approach to quantum computing
- Quantum memories for quantum cryptography
  - The most efficient quantum memories today, how do they work and how are they made

Why develop quantum memories?

- Effective use of quantum resources, such as superposition of states and entanglement, in quantum information requires new devices
  - Storage of intermediate results in quantum computations, communication between quantum computers
  - Quantum memories required in quantum repeaters for long distance quantum cryptography

Quantum memory for time-bin qubits for quantum key distribution

time-bin qubits Sender Receiver



Requirements

Need to store amplitude and phase of a wave-packet (on average less than one photon) in a superposition between two different times

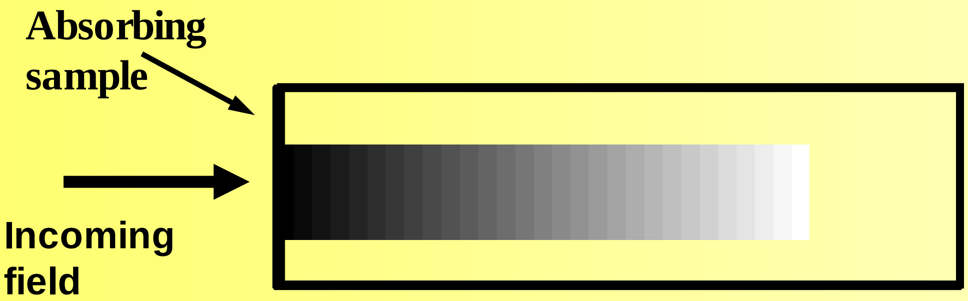
Quantum memories

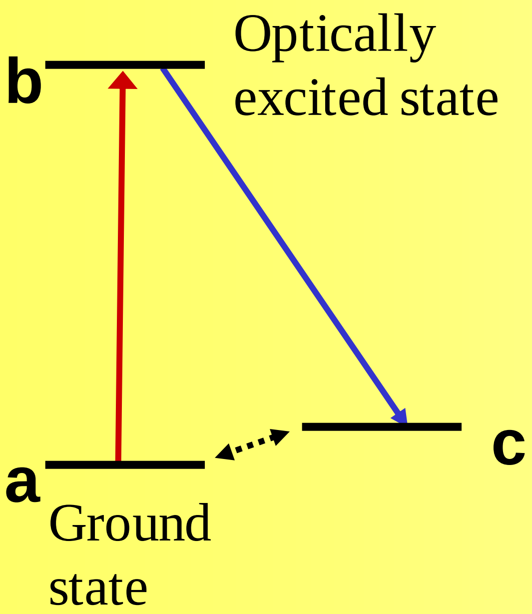
- We would like to store and recall the state, Ψ, of a quantum system
- Generally a quantum system at time t_2 can be related to its state at some earlier time, t_1, by a unitary transformation U
- $\Psi(t_2)=U\Psi(t_1)$
- Clearly, if we expose the system at time t_2 to U^{-1}, the original state is obtained
- $U^{-1}\,\Psi(t_2) = U^{-1}\,U\,\Psi(t_1) = \Psi(t_1)$

Quantum memories

- We presently focus on developing quantum memories for quantum cryptography, where the information is stored in wave-packets consisting of, on average, less than one photon
- Our approach is to absorb the wave-packet and, when the information is to be read out, time-reverse the absorption process such that the original light state is reconstructed

Storing the input quantum field





•We start with all atoms in the ground state, a

$$\Psi = \Phi_a$$

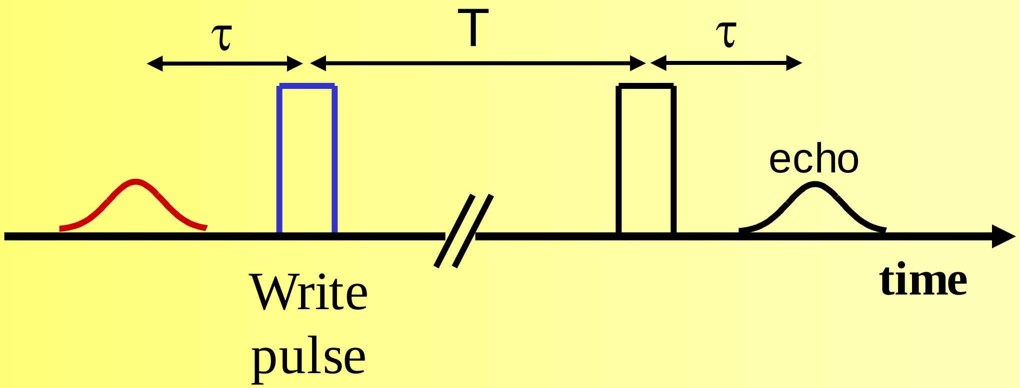
Weak pulse enters the sample

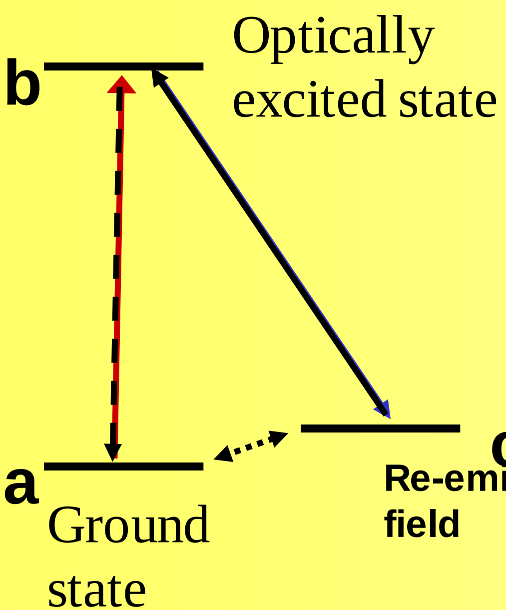
$$\Psi = \alpha\Phi_a + \beta\Phi_b$$

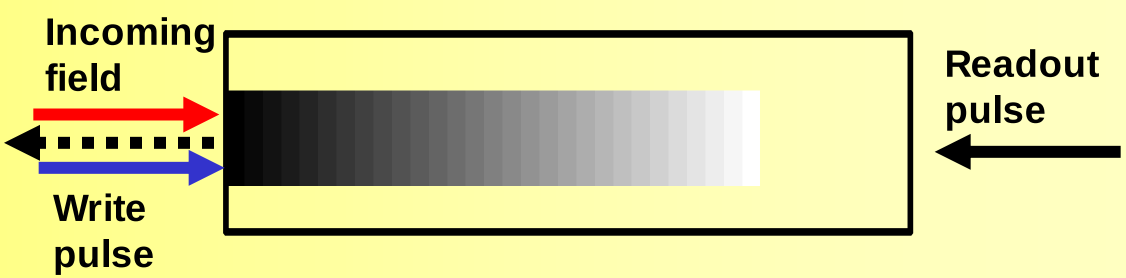
The second pulse transfers the probability amplitude in state b to state c. As state c is empty this pulse will not experience absorption.

$$\Psi = \alpha\Phi_a + \beta'\Phi_c$$

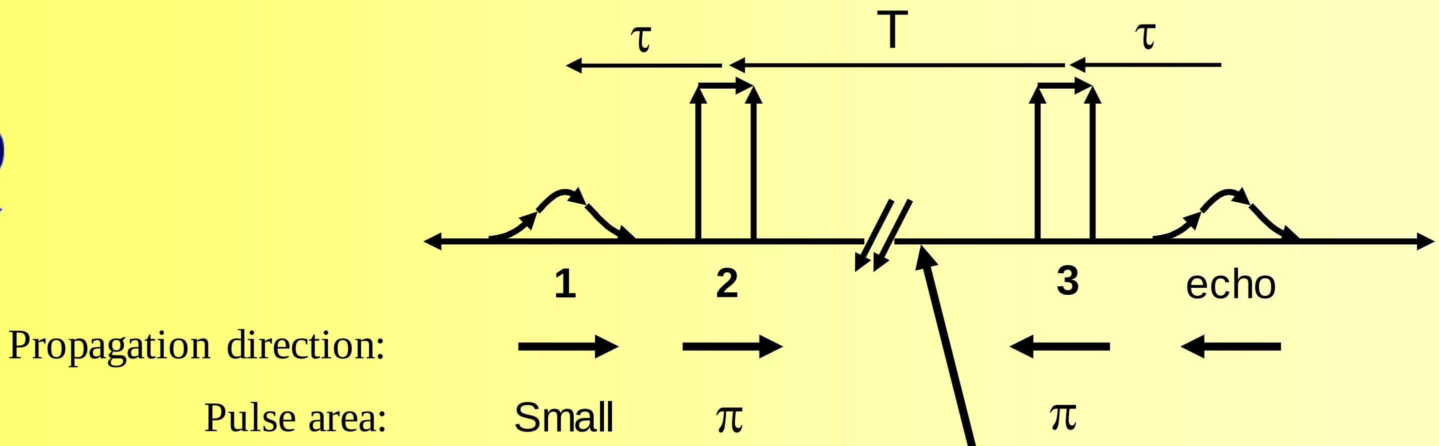
Recalling the stored field







Scheme requirement



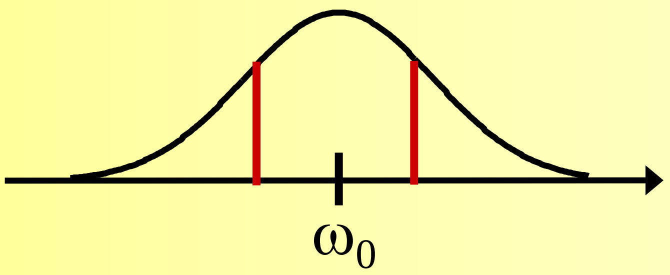
Unity efficiency can be obtained if the absorption profile where information has been stored is frequency reversed before readout

Moiseev & Kröll, PRL **87**, 173601 (2001)

Doppler-broadening

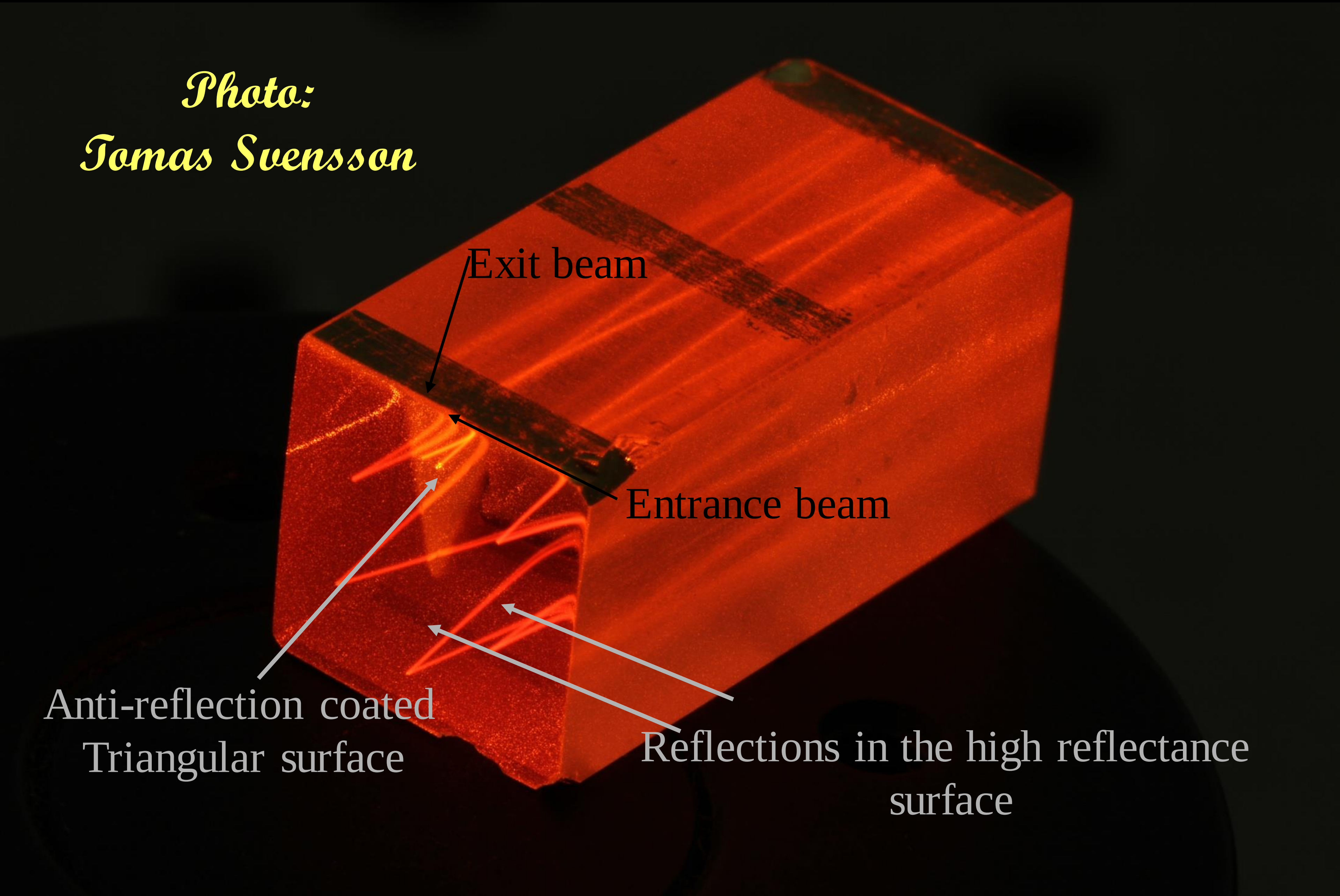
- The unshifted resonance frequency is ω_0
- **u** is a unit propagation vector for the exciting radiation
- For an atom moving with velocity **v** the transition frequency, ω, is

$$\omega = \omega_0 \left(1 + \frac{\mathbf{v} \bullet \mathbf{u}}{c}\right)$$



- For two counterpropagating photons the absorption frequency of the atom is reversed relative to the unshifted resonance frequency ω_0

Picture of crystal

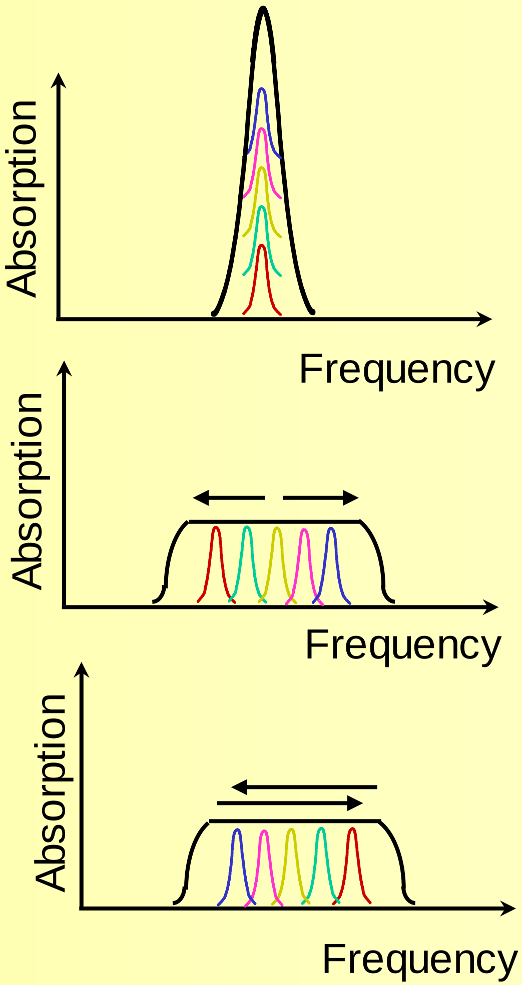


Controlled reversible inhomogeneous broadening (CRIB)

- Prepare an ensemble of absorbers that all have the same initial resonance frequency

- Apply a (position dependent) external field that shifts the atomic resonance frequencies by different amounts

- This inhomogeneous broadening can be reversed by changing the external field

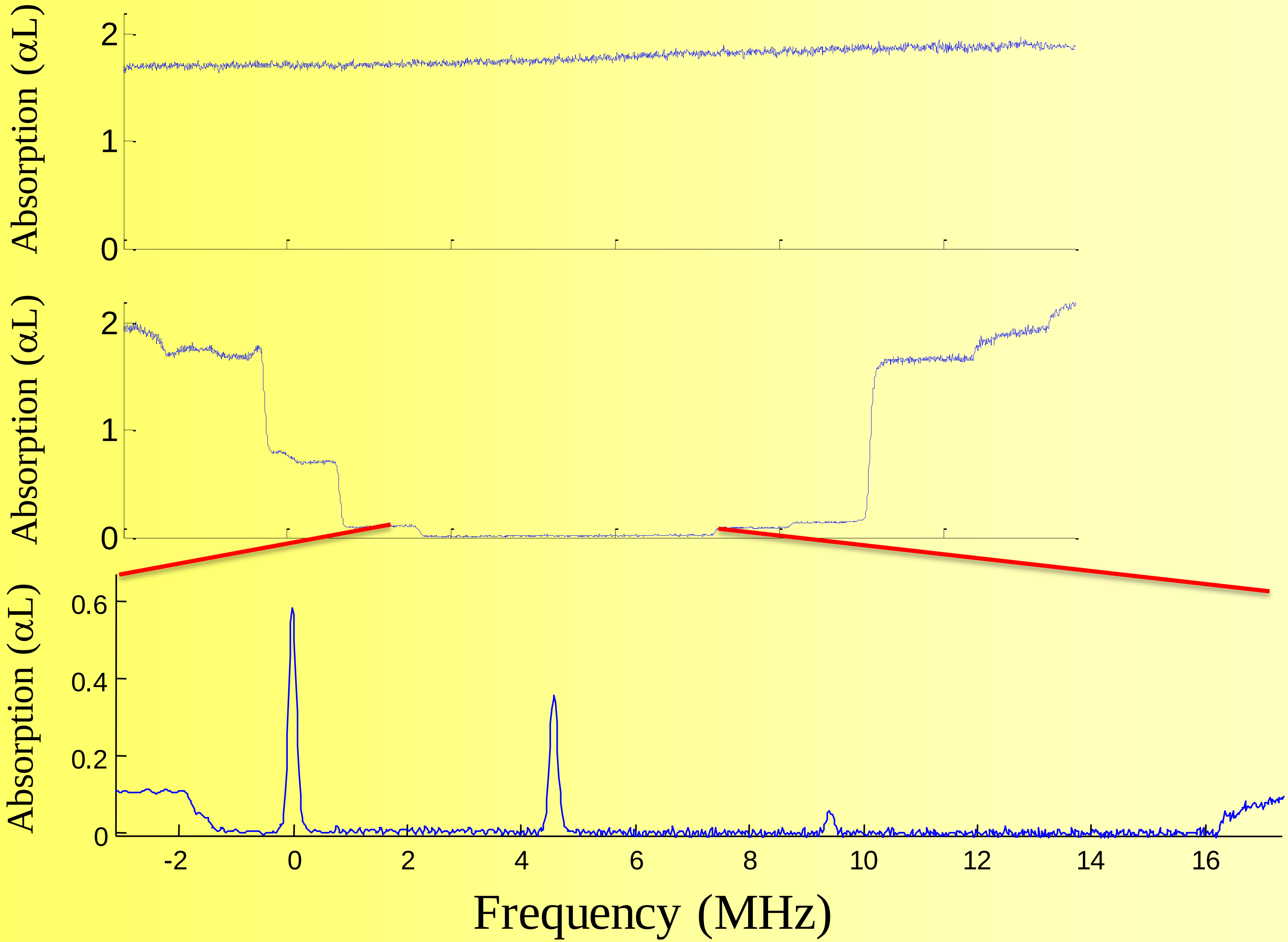


Nilsson & Kröll, Opt. Commun. **247**, 393-403 (2005)

Kraus, Tittel, Gisin, Nilsson, Kröll & Cirac, Phys. Rev. A**73**, 020302 (2006)

**Photo:
Tomas Svensson**

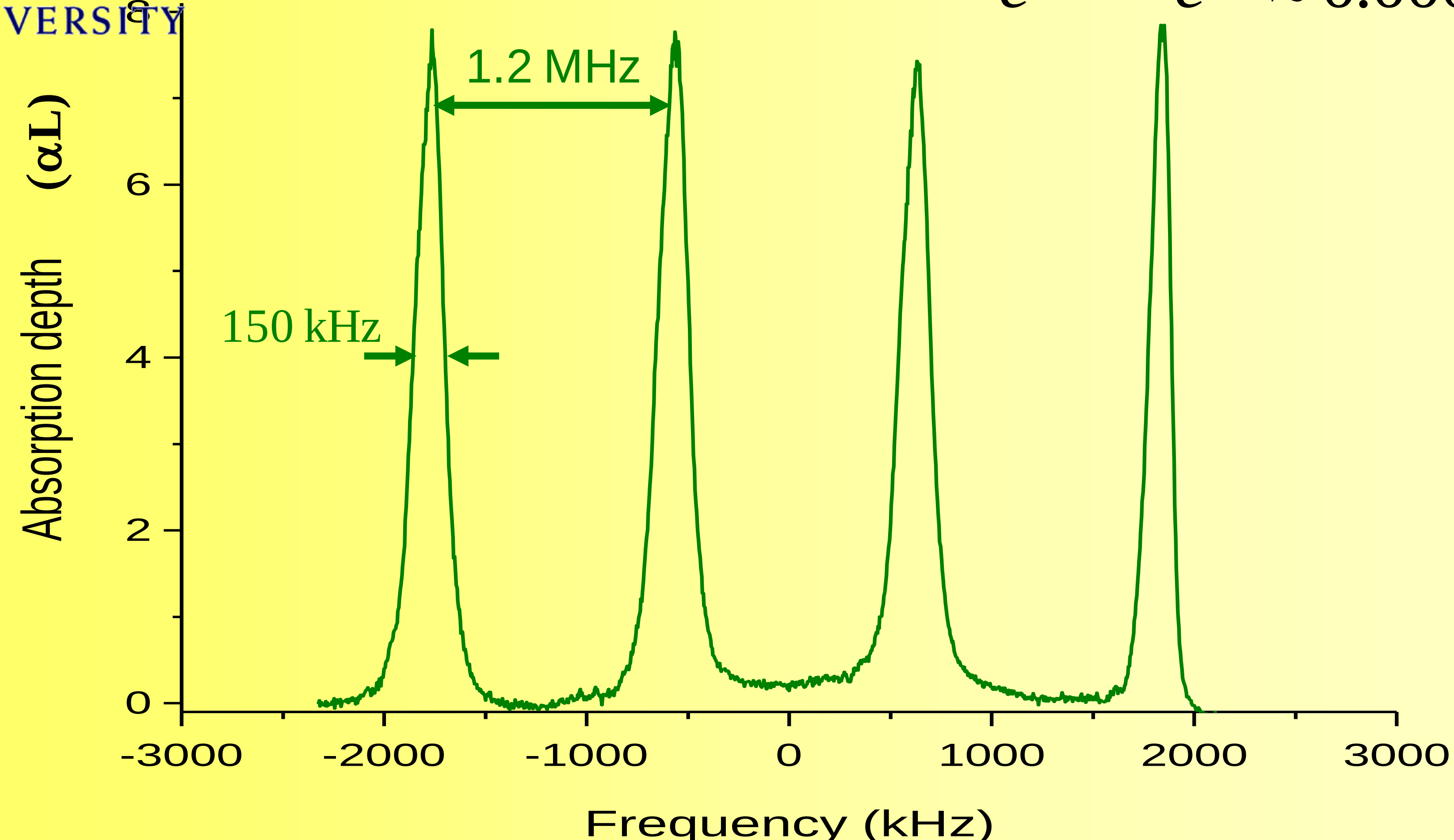
Spectral design



Atomic frequency comb

At the peaks, transmission is

$$e^{-\alpha L} = e^{-8} \approx 0.0003$$



$$150kHz \approx 5*10^{-6}cm^{-1} \approx 6*10^{-10}eV \approx 2*10^{-7}nm$$

Quantum memories (QM) Experimental data Lund

- Memory efficiency (35%)
  - Amari et al., J Lumin **130**,1579 (2010)
- Single photon memory efficiency (25%)
  - Sabooni et al., PRL **105**, 060501 (2010)
- Spin state storage, > 100 μs
  - Afzelius et al., PRL **104**, 040503 (2010)

Recent experimental quantum memory results

- 69% storage efficiency, Hedges, Longdell, Li & Sellars, Nature, **465**, 1052 (2010)
- Mapping of 64 photonic qubits into and out of one solid-state atomic ensemble, Usmani, Afzelius, de Riedmatten & Gisin, arXiv:1002.3782 (2010)
- 87% storage efficiency, Hosseini et al., arXiv:1009.0567

Outline

- Some reflections regarding the beginning of the field of quantum computing and why might quantum computers be interesting
- How to construct quantum computers
- The Lund approach to quantum computing
- Quantum memories for quantum cryptography
  - The most efficient quantum memories today, how do they work and how are they made




Lars Rippe | **Yan Ying** | **Jenny Karlsson** | **Brian Julsgaard**

Andreas Walther | **Atia Amari** | **Mahmood Sabooni** | **Mattias Nilsson**