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

QUBITS

Classical bit : 2 states 0 and 1

Quantum bit : 2 states $| 0 \rangle$ and $| 1 \rangle$, plus arbitrary superpositions :

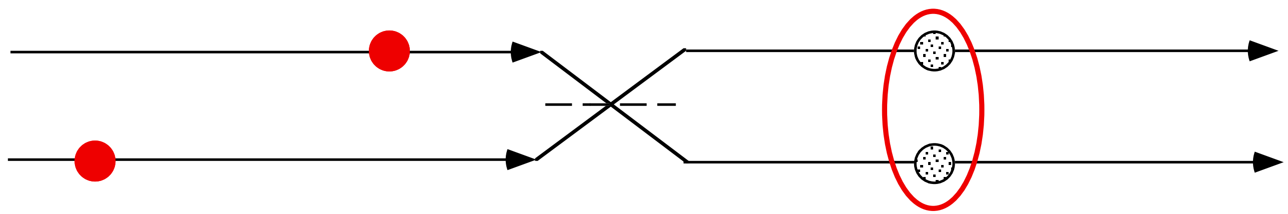
$$| \psi \rangle = \cos(\theta)\, e^{i\varphi} | 0 \rangle + \sin(\theta)\, e^{-i\varphi} | 1 \rangle$$

Simple exemples :

Polarised photon

$| 0 \rangle$ $\quad$ $| 1 \rangle$ $\quad$ $\cos(\theta) | 0 \rangle + \sin(\theta) | 1 \rangle$

"Split photon"



-> very useful for quantum cryptography

QUANTUM COMPUTING : REGISTERS

"Analog" classical computing ? (continuous values) : no

N bits with possible values 0 and 1

Register : | ε(1) | ε(2) | ε(3) | ε(4) |.... | ε(N) | (ε=0 ou 1)

State of a classical analog computer : N continuous variables ε(i)

Possible state of the computer : $| \varepsilon(1), \varepsilon(2), \varepsilon(3), \varepsilon(4) .... \varepsilon(N) \rangle$ (ε=0 or 1)

General state of the computer : $\Sigma\ c_x\ | \varepsilon(1), \varepsilon(2), \varepsilon(3), \varepsilon(4) .... \varepsilon(N) \rangle$

State of a quantum computer : 2^N continuous (complex) variables c_x !!!

The computer states live in a huge 2^N-dimensional Hilbert space

Most of these states are "entangled" (individual qubits have no state)

QUANTUM COMPUTING : REGISTERS

General state of the computer : $\Sigma\ c_x\ |\ \varepsilon(1), \varepsilon(2), \varepsilon(3), \varepsilon(4)....\ \varepsilon(N)\ \rangle$

(linear superposition of all possible register states)

- During the computer evolution, all 2^N states $|\varepsilon(1)....\ \varepsilon(N)\ \rangle$ are involved

-> **"quantum parallelism"**

- When the state of the computer is "measured", **a single binary state** is detected (the probabilities for all other ones cancel out)

-> one keeps all the **advantages of a binary calculation.**

Very peculiar mixture of analog and binary ingredients !

"Doors can be open and closed at the same time"

CALCULATING FUNCTIONS

Classical function : Input register –> Output register

The value x of the register becomes f(x); generally not reversible

Quantum function : Input state –> Output state

$| x > = | \varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots \varepsilon_N >$: N bits, 2^N possible values

$| x > \rightarrow | f(x) >$: non-unitary !

$| x > \otimes | 0 > \rightarrow | x > \otimes | f(x) >$: ok !

More interesting : **superposition** $| \psi > = 1/\sqrt{2^N} \sum_x | x >$

$$| \psi > \otimes | 0 > \rightarrow 1/\sqrt{2^N} \sum_x (| x > \otimes | 0 >)$$

$$\rightarrow 1/\sqrt{2^N} \sum_x (| x > \otimes | f(x) >)$$

2^N values of the function are calculated in a single step !

Any function can be realized using one-qubit and two-qubit gates

QUANTUM LOGICAL GATES

Classical logical gates : **Input register –> Output register**

NOT gate:
(1 bit)
(flip)

In	Out
0	1
1	0

XOR gate :
(2 bits)
("controlled not",
or "cnot")

In	Out
0, 0	0
0, 1	1
1, 0	1
1, 1	0

Generally not reversible !

Classical logical gates : **Input state –> Output state**

"$\sqrt{\text{NOT}}$" :
(1 bit)
$\varphi = \pi/4$

In	Out	In	Out
$\|0\rangle$	$(e^{i\varphi}\|0\rangle + e^{-i\varphi}\|1\rangle)/\sqrt{2} =$	$\|u\rangle$	$(e^{i\varphi}\|u\rangle + e^{-i\varphi}\|v\rangle)/\sqrt{2} = \|1\rangle$
$\|1\rangle$	$(e^{-i\varphi}\|0\rangle + e^{i\varphi}\|1\rangle)/\sqrt{2} =$	$\|v\rangle$	$(e^{-i\varphi}\|u\rangle + e^{i\varphi}\|v\rangle)/\sqrt{2} = \|0\rangle$

CNOT :
(2 bits)

In	Out
0, 0	0, 0
0, 1	0, 1
1, 0	1, 1
1, 1	1, 0

Hamiltonian Evolution :
Unitarity et Reversibility !

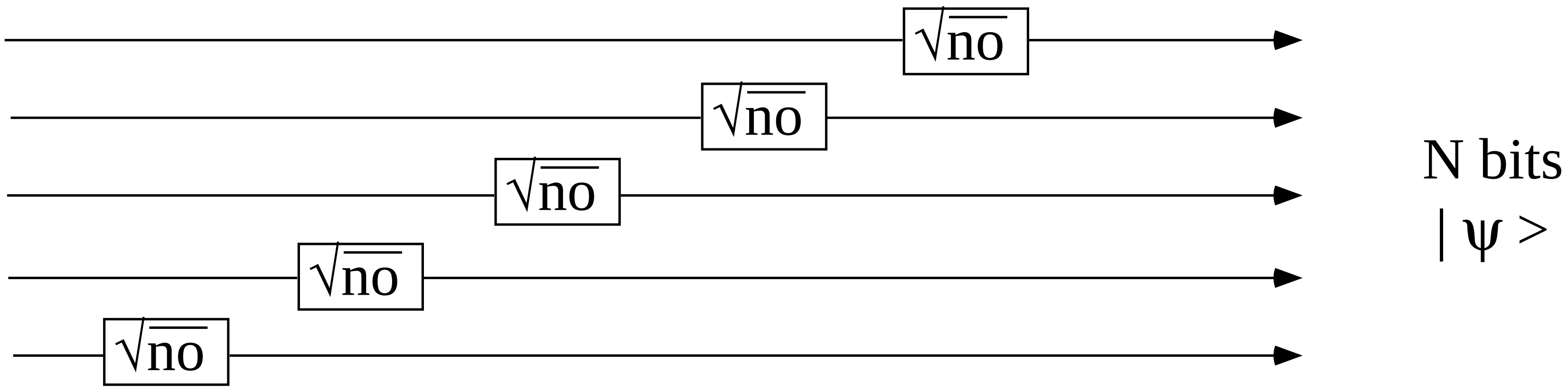
Symmetric superposition

How to get the completely symmetric state $| \psi > = 1/\sqrt{2^N} \sum_x \; | x > ?$

$(\sqrt{\overline{not}} \otimes \sqrt{\overline{not}} \otimes \sqrt{\overline{not}} \otimes \ldots) |0, 0, 0 \ldots > \; =$

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

$1/\sqrt{2^N} (| 0, 0, \ldots 0> + | 0, 0, \; \ldots 1> + \ldots + | 1, 1, \; \ldots 0> + | 1, 1, \; \ldots 1>) = | \psi > !$



This requires N $\sqrt{\overline{not}}$ gates : ok

QUANTUM COMPUTING

Discrete Fourier transform

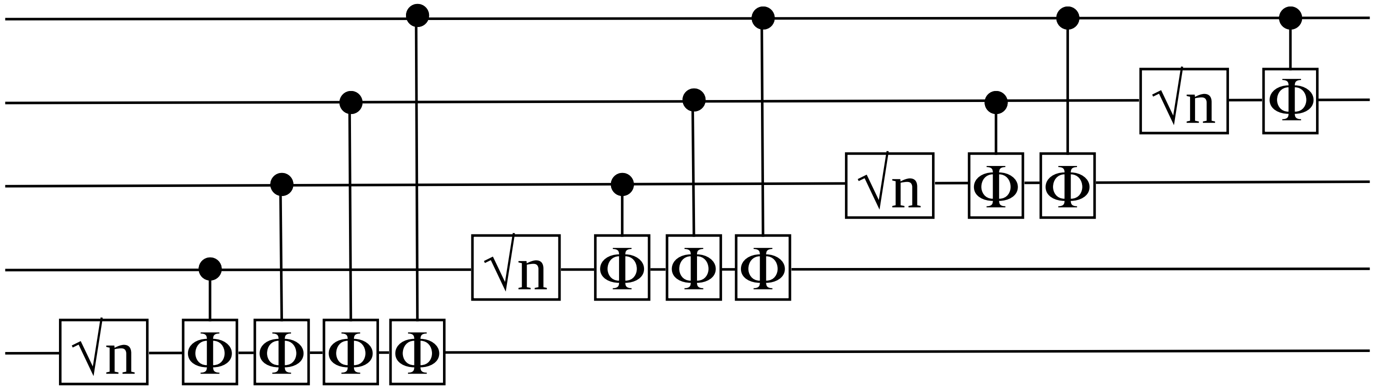
$| x > \longrightarrow \text{DFT}(| x >) = 1/\sqrt{L} \sum_u e^{2i\pi\, u\, x / L} | u >$ $\qquad L = 2^N$ values for x

Ex : $| x = 0 > \longrightarrow 1/\sqrt{L} \sum_u | u >$: superposition with equal weights

$| x = 1 > \longrightarrow 1/\sqrt{L} \sum_u e^{2i\pi\, u/L} | u >$: weights = roots of unity...

$| x = 2 > \longrightarrow 1/\sqrt{L} \sum_u e^{4i\pi\, u/L} | u >$: ...

N bits
$| x >$



N bits
$\text{DFT}(| x >)$

This requires N gates $\sqrt{n}$ et N(N-1)/2 gates Φ : ok

FACTORIZATION ALGORITHM
(PETER SHOR 1994)

A - Mathematical Principle

B - Quantum Calculation

C - It works, but...

QUANTUM COMPUTING

Factoring algorithm : mathematical side

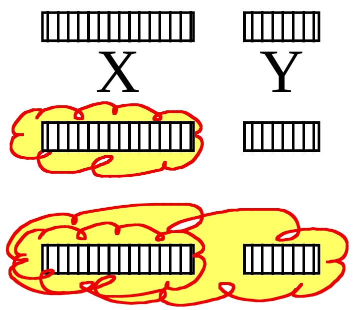
Let n to be factorised	$n = 35$
1 - Choose a coprime with n	$a = 13$
Th1 : the function $f_{a,n}(x) = a^x \bmod n$	1, 2, 3, 4, 5, 6, 7, 8 ...
is periodic	13, 29, 27, 1, 13, 29, 27, 1 ...
2 - Find the period, denoted as T	$T = 4$
3 - Calculate $g_+ = \gcd(n,\ a^{T/2} + 1)$	$\gcd(35\ ,\ 13^2 + 1) = 5$
$g_- = \gcd(n,\ a^{T/2} - 1)$	$\gcd(35\ ,\ 13^2 - 1) = 7$
Th2 : If $g_\pm \neq -1 \bmod n$, then g_+ et g_-	
are the factors of n	**ok !**

Efficiency ? Poor for a classical computer : step 2 requires a number of operations increasing exponentially with Log(n) (multiple evaluations of $f_{a,n}$)

SHOR'S ALGORITHM

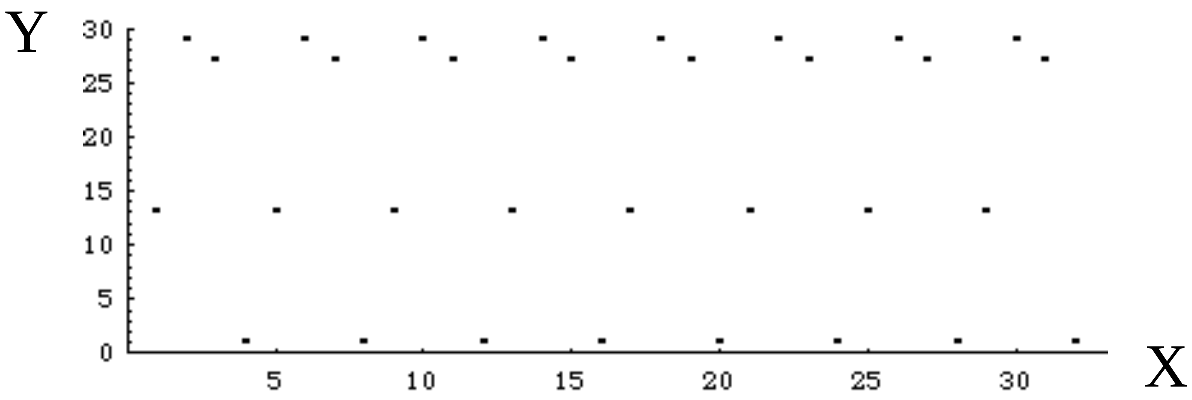
Number to be factorized: n encoded on N bits -> numbers from 0 to 2^N-1

2 Registers with resp. 2N bits (denoted X) and N bits (denoted Y)



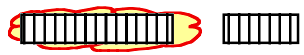
1 - Prepare the superposition : $(1/\sqrt{2^{2N}} \sum_x | x >_X) \otimes | 0 >_Y$

2 - Apply $f_{a,n} \rightarrow 1/\sqrt{2^{2N}} \sum_x (| x >_X \otimes | a^x \bmod n >_Y)$



Exemple : Calculation of $f_{13,\,35}(x) = 13^x \bmod 35$

3 - Perform a quantum measurement on the register Y



$\rightarrow$ find one among the possible values of y

The register X is projected on the quantum state $C \sum_k | d + k T >$

where d : shift depending of the value of y, k :integer , **T : period**

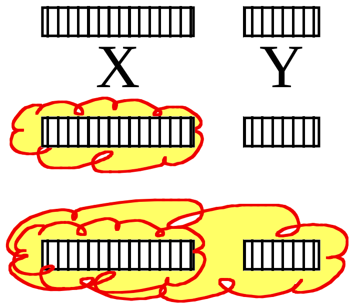
SHOR'S ALGORITHM

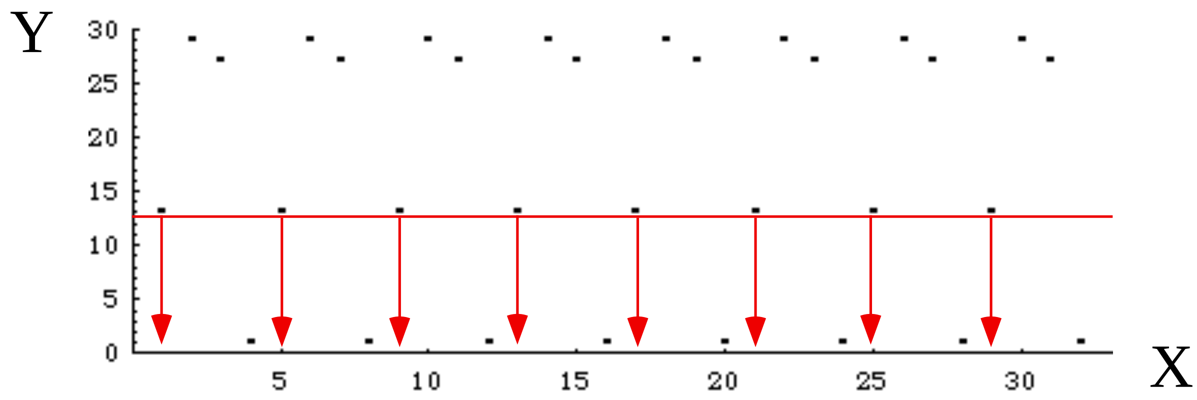
Number to be factorized: n encoded on N bits -> numbers from 0 to 2^N-1

2 Registers with resp. 2N bits (denoted X) and N bits (denoted Y)

1 - Prepare the superposition : $(1/\sqrt{2^{2N}}\ \Sigma_x \mid x >_X) \otimes \mid 0 >_Y$

2 - Apply $f_{a,n} \rightarrow 1/\sqrt{2^{2N}}\ \Sigma_x (\mid x >_X \otimes \mid a^x \bmod n >_Y)$

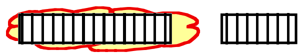




Exemple : Calculation of $f_{13,\,35}(x) = 13^x \bmod 35$

3 - Perform a quantum measurement on the register Y

$\rightarrow$ find one among the possible values of y



The register X is projected on the quantum state C $\Sigma_k \mid d + k\,T >$

where d : shift depending of the value of y, k :integer , **T : period**

SHOR'S ALGORITHM

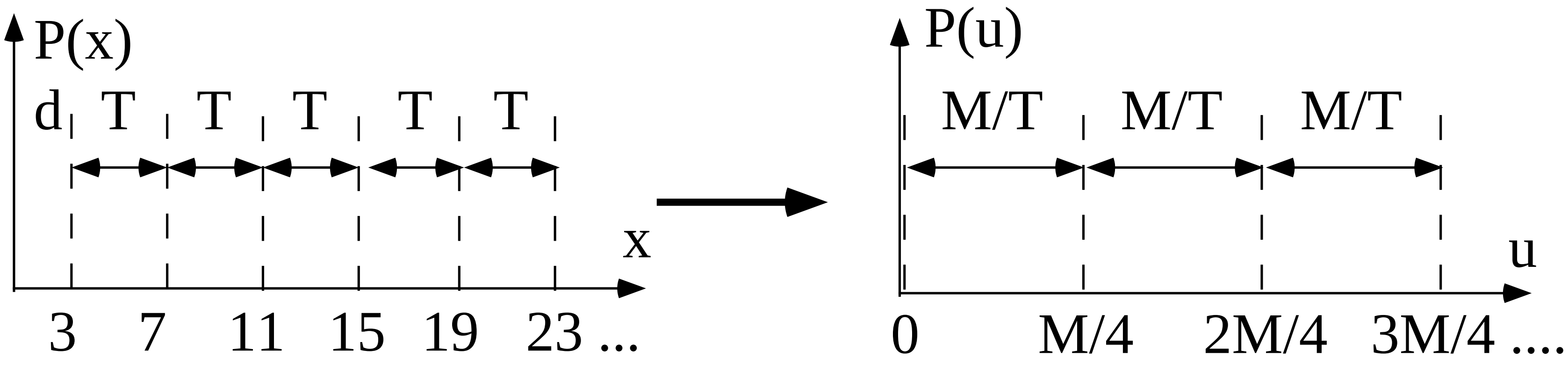
4 - Perform a discret Fourier transform

$C \sum_k | d + k T > \rightarrow C/\sqrt{M} \sum_k \sum_u e^{2i\pi u (d+k T) /M} | u >$ $M = 2^{2N}$

But : $\sum_k e^{2ik\pi u T /M}$ $= M/T$ if $u T/M = j$ integer, thus $u = j M/T$

$= 0$ otherwise

Thus $C \sum_k | d + k T > \rightarrow C\sqrt{M / T} \sum_j e^{2i\pi j d/T} | j M/T >$



5 - By repeating the whole process several times, extract the period !

QUANTUM COMPUTING

A quantum computer can perform some calculations very efficiently...

- factorization algorithm (Shor 1994) : exponential gain

- search algorithm (Grover 1996) : quadratic gain

... but it is very difficult to implement

- the quantum states $\sum c_i \mid \varepsilon(1), \varepsilon(2), \varepsilon(3), \varepsilon(4) .... \varepsilon(N) \rangle$ with N large are extremely sensitive to all interactions with environment : "**decoherence**"

- the interaction of the qubits between themselves and with the outer world must be extremely well controlled, to perform calculations and to avoid decoherence

Some encouraging results ...

- all calculations can be performed on the basis of 1 and 2 qubits gates

- errors are unavoidable, but "quantum error correcting codes" are possible

ERROR CORRECTING CODES

Classical approach	Error probability for one 1 bit = $p << 1$		
* Encoding :	$1 \rightarrow$ [1 1 1]	$0 \rightarrow$ [0 0 0]	
* Error correction :	"majority voting"		
* Errors for 3 bits ?	$(1-p)^3$	no error	ok
	$3p\,(1-p)^2$	1 wrong bit	ok
	$3p^2\,(1-p)$	2 wrong bits	error
	p^3	3 wrong bits	error
* Total error probability :	$3p^2\,(1-p) + p^3 \approx 3p^2 << p$		**OK !**

Quantum approach

* One can neither read the state of the qubit, nor copy it (no-cloning)
* There are various types of errors ("flip", "phase", or both)
* How to do it?

ERROR CORRECTING CODES

Quantum approach : encoding

b1 = a $|0\rangle$ + b $|1\rangle$ $\rightarrow$ decoherence! $\rightarrow$?

b1 = a $|0\rangle$ + b $|1\rangle$

w = xor = cnot gate

b1 w b2 $\rightarrow$ b12=a $|0,0\rangle$ + b $|1,1\rangle$

b2 = $|0\rangle$

b1 w b3 $\rightarrow$ b123=a $|0,0,0\rangle$ + b $|1,1,1\rangle$

Entangled state !

b3 = $|0\rangle$

b3 = $|0\rangle$

b123=a $|0,0,0\rangle$ + b $|1,1,1\rangle$ $\rightarrow$ decoherence! $\rightarrow$?

ERROR CORRECTING CODES

* Processing b123 after decoherence : run the encoding backwards !

b1 w b3 = b1 (still there !) and c3 (measured, destroyed)

b1 w b2 = b1 (still there !) and c2 (measured, destroyed)

* Assume zero or one bit flip error :

$a\,|0\;0\;0\rangle + b\,|1\;1\;1\rangle \rightarrow$ (c2, c3) = (0, 0) $\rightarrow$ ok

$a\,|1\;0\;0\rangle + b\,|0\;1\;1\rangle \rightarrow$ (c2, c3) = (1, 1) $\rightarrow$ flip b1 $\rightarrow$ ok

$a\,|0\;1\;0\rangle + b\,|1\;0\;1\rangle \rightarrow$ (c2, c3) = (1, 0) $\rightarrow$ error on b2 $\rightarrow$ ok

$a\,|0\;0\;1\rangle + b\,|1\;1\;0\rangle \rightarrow$ (c2, c3) = (0, 1) $\rightarrow$ error on b3 $\rightarrow$ ok

Final result : b1 = $a\,|0\rangle + b\,|1\rangle$, error probability of order p^2

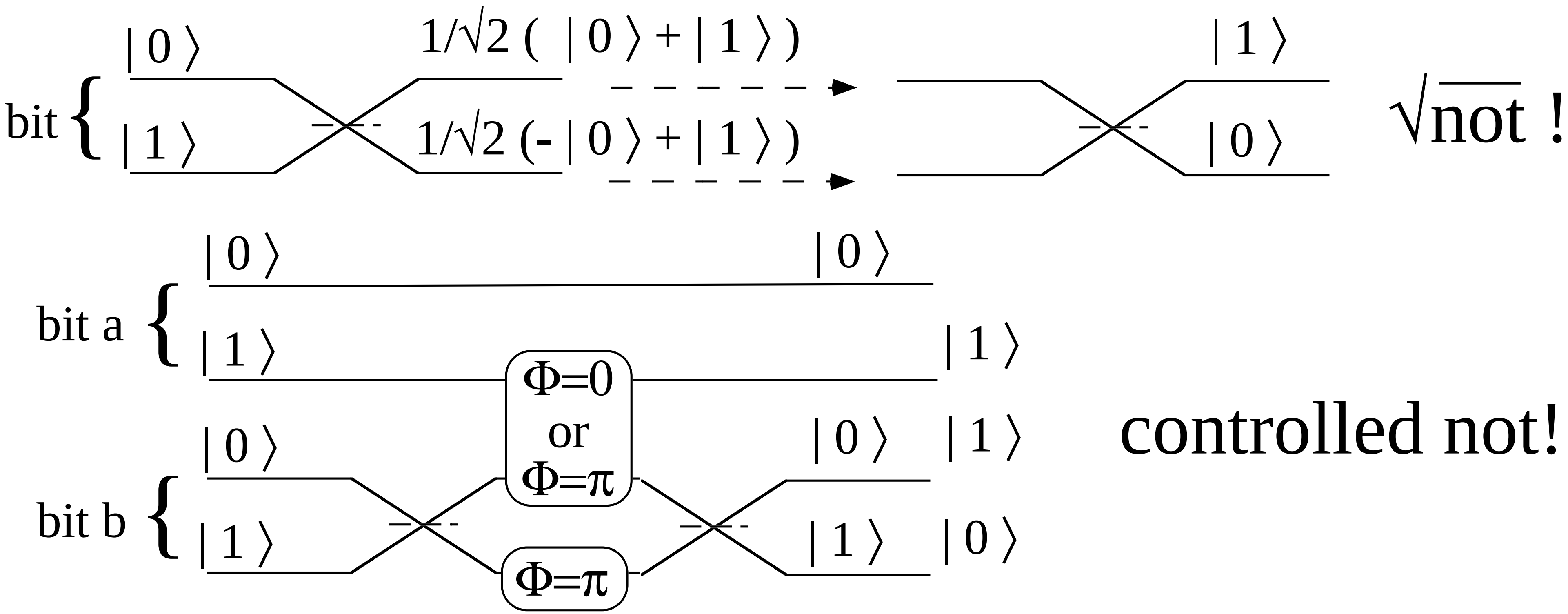
* Correct flip errors on one qubit with probability $O(p^2) \ll p$ OK !

* Phase errors : encoding on more than 3 bits (5 min, 7 or 9 ok)

*** General idea : "syndrome measurement" + suitable correction**

QUANTUM COMPUTING

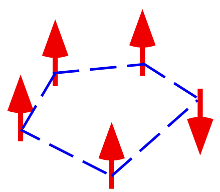
Implementations ? Most obvious : Photons



Advantages : Simplicity (useful for building "models"), good isolation from environment ...

Drawbacks : A CNOT gate requires a phase shift π per photon : difficult to implement (coupling increased by using high finesse cavities)

EXPERIMENTAL PROPOSALS

	Qubits	Gates	Main difficulty
1994	Photons	Bistables optiques	Available energy : h ν ! Very difficult to implement
1995	Semiconductors "quantum dots"	?	Strong decoherence
1996	Trapped ions	Coulomb interaction	Thermal motion
1997	Molecular spins + RMN	Spin coupling 	Complexity of the molecule Macroscopic sample !

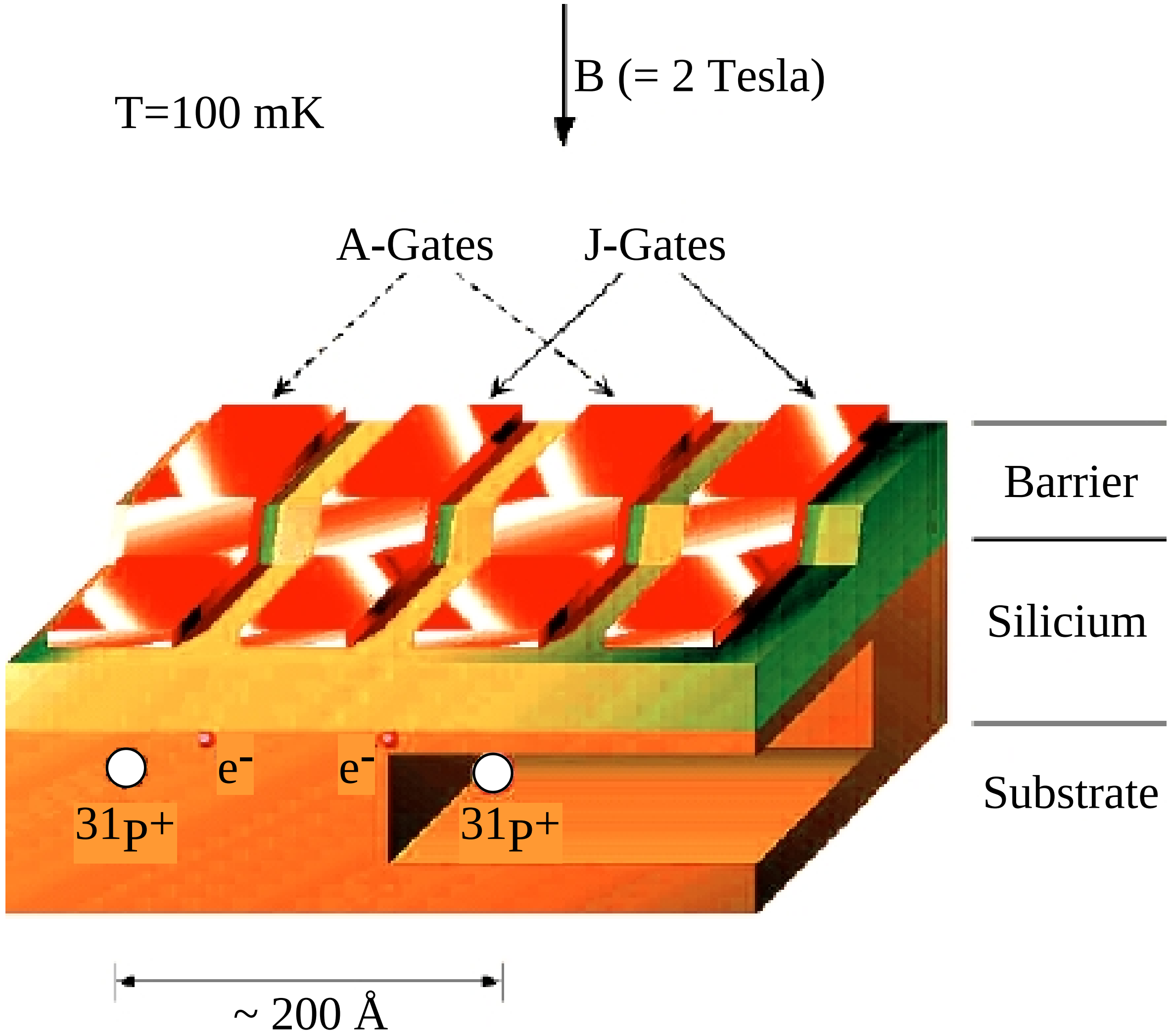
QUANTUM COMPUTER IN SILICON

Qubit : magnetic moment
of phosphorus atoms
individually implanted
below electrodes

"A" : 1 qubit gates
"J" : 2 qubits gates

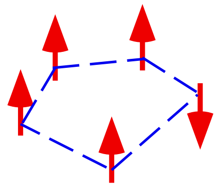
*** Technically possible**

*** Decoherence ???**



B. E. Kane, "A silicon-based nuclear spin quantum computer",
Nature, Vol. 393, p. 133, 1998

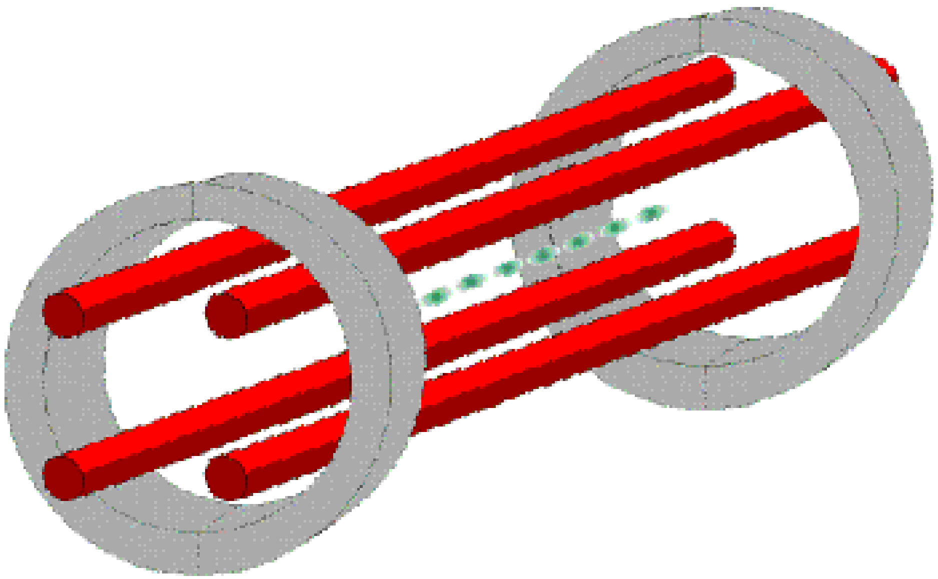
EXPERIMENTAL PROPOSALS

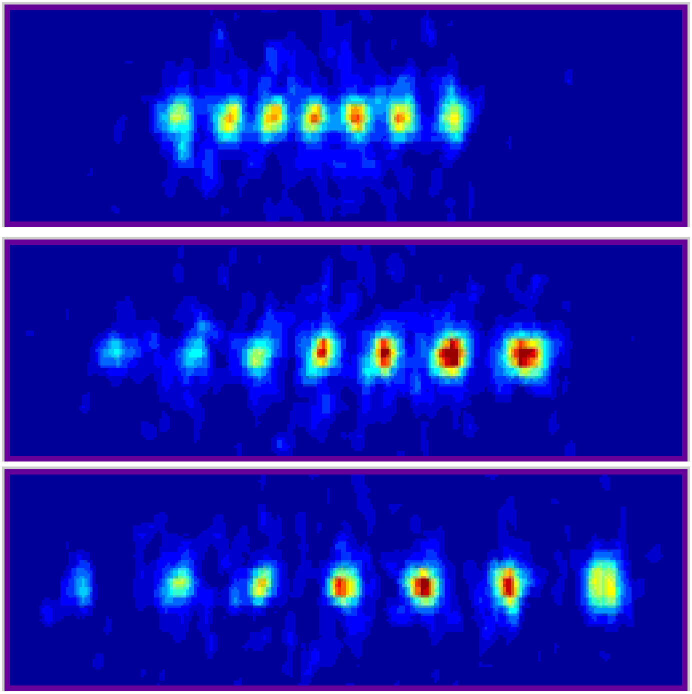
	Qubits	Gates	Main difficulty
1994	Photons	Bistables optiques	Available energy : h ν ! Very difficult to implement
1995 1998 1999	Semiconductors "quantum dots"	? Individual Spins	Strong decoherence Implanted in silicon ? Carbon nanotubes ?
1996 1999	Trapped ions	Coulomb interaction	Thermal motion Laser cooling in linear traps
1997 1998	Molecular spins + RMN $CHCl_3$	Spin coupling 	Complexity of the molecule Macroscopic sample ! First "calculations" (3 qubits)

LINEAR ION TRAPS
(Innsbruck University)

* Calcium ions trapped using electromagnetic fields -> "rows" of ions

* Laser cooling -> regular arrays (Coulomb repulsion).

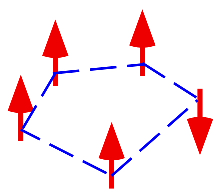




Fluorescence imaging of 7 trapped ions

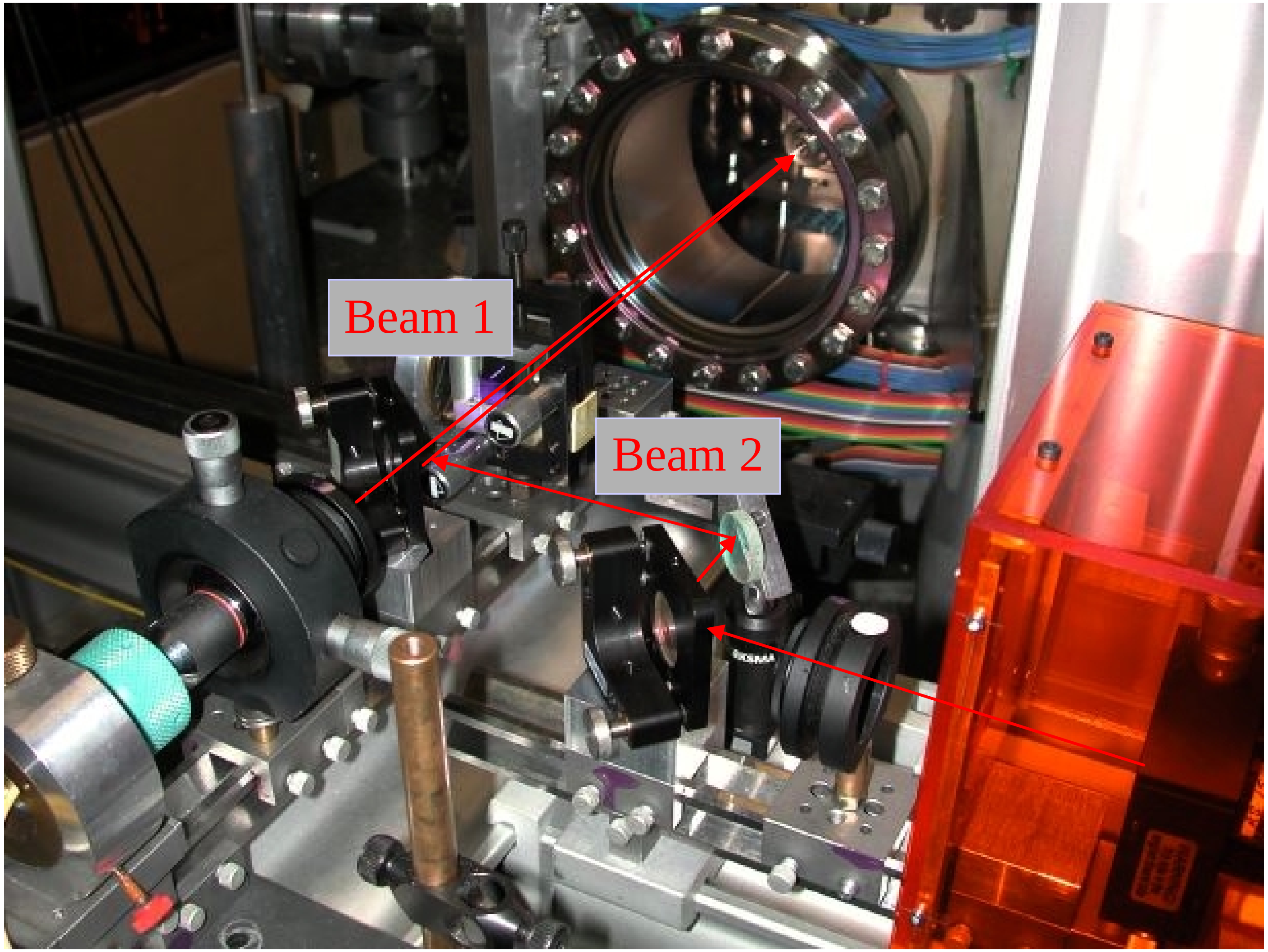
Ions isolated in vacuum :
decoherence much smaller than in solid-state materials

EXPERIMENTAL PROPOSALS

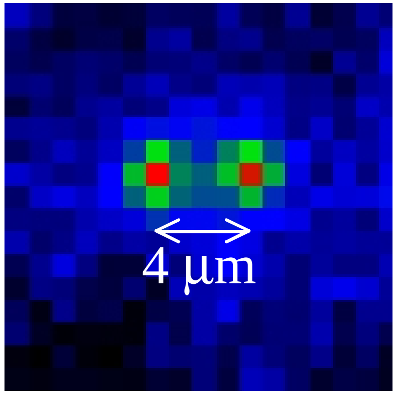
	Qubits	Gates	Main difficulty
1994	Photons	Bistables	Available energy : h ν !
		optiques	Very difficult to implement
2000	Microwave domain		but CNOT gate realized.
1995	Semiconductors	?	Strong decoherence
	"quantum dots"		
1998		Individual	Implanted in silicon ?
1999		Spins	Carbon nanotubes ?
1996	Trapped ions	Coulomb	Thermal motion
1999		interaction	Laser cooling in linear traps
2001	Trapped atoms		"Optical tweezers"
1997	Molecular spins	Spin	Complexity of the molecule
	+ RMN	coupling	Macroscopic sample !
1998	$CHCl_3$		First "calculations" (3 qubits)
2000	Fluorine 19 ($M\text{-}F_5$)		Calculations with 5 qubits

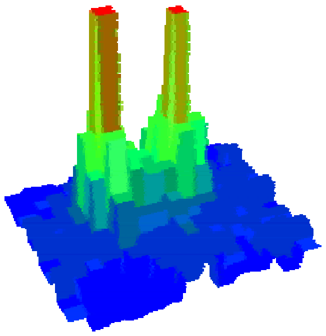
Two atoms at your fingertips

N. Schlosser et al, Nature 411, 1024 (2001)
PRL 89, 023005 (2002)

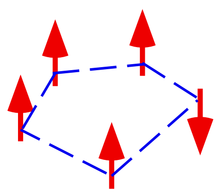


Resolution of the imaging system:
1 micron / pixel





EXPERIMENTAL PROPOSALS

	Qubits	Gates	Main difficulty
1994	Photons	Bistables optiques	Available energy : h ν ! Very difficult to implement
2000	Microwave domain		but CNOT gate realized.
1995	Semiconductors "quantum dots"	?	Strong decoherence
1998 1999		Individual Spins	Implanted in silicon ? Carbon nanotubes ?
1996	Trapped ions	Coulomb interaction	Thermal motion
1999			Laser cooling in linear traps
2002	Trapped atoms	Collisions	Optical tweezers and lattices
1997	Molecular spins + RMN	Spin coupling	Complexity of the molecule Macroscopic sample !
1998	$CHCl_3$		First "calculations" (3 qubits)
2002	Fluorine 19 ($M\text{-}F_5$)		Factorization of 15 !

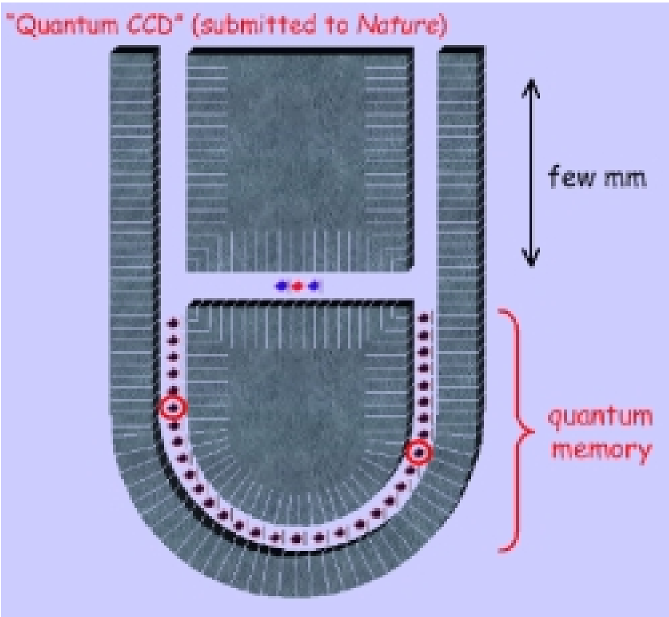
"QUANTUM CCD "

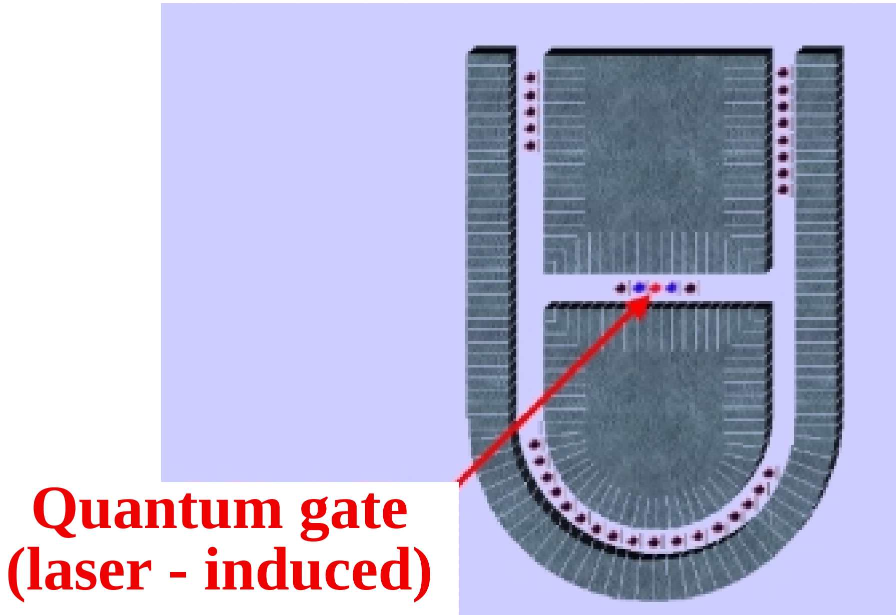
D. Kielpinsky, C. Monroe, D. Wineland. *Nature* (2002)

***** Chain of trapped ions moved from storing to interaction areas.

*** Qubits** : 2 atomic levels (spin states - laser-controlled)

***** Extraction of any two ions to the interaction area :
-> **quantum gate between any 2 qubits !**





"Scalable" proposal, but not yet implemented !

CONCLUSION

* **Quantum cryptography** appears to evolve slowly but straightforwardly towards practical implementations.

* **Quantum computing** is a much bigger scientific challenge : by principle it cannot work at a macroscopic scale, microscopic systems are difficult to control ... -> "mesoscopic scale enginering"

* Objectively, a useful quantum computer is very far away :
-> 1-10 quantum gates : **repeaters for quantum cryptography...**
-> 10-100 quantum gates : **implement quantum simulation...**
-> 100-1000 quantum gates : **efficient error correction possible...**

* On the way ... exploration of many open problems in

-> quantum mechanics (theory and experiment...)

-> information theory (algorithms, error corrections ...)