, 100084

gllong@tsinghua.edu.cn

2008 11 13

- -

- - - -

-
- ENIAC

-
-
- Shor
- Grover
-

- **Where a calculator on the Eniac is equipped with 18000 vacuum tubes and weighs 30 tons, computers in the future may have only 1000 tubes and weigh only 1 1/2 tons**
- **Popular Mechanics, March 1949**

- **Anyone who is not shocked by quantum theory has not understood it.**
- **Niels Bohr**

- **I think I can safely say that no body understands quantum mechanics.**
- **Richard Feynman**

[Quantum]theory has, indeed, two powerful bodies of fact in its favour, and only one thing against it. First, in its favour are all the marvellous agreements that the theory has had with every experimental result to date. Second,and to me almost as important, it is a theory of astonishing and profound mathematical beauty. **The one thing that can be said against it is that it makes absolutely no sense!**

Roger Penrose

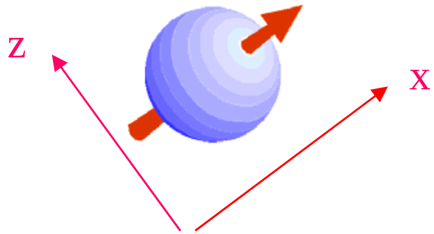
-
-
- (,)
-
-

$|\Phi$

$$S_x = \frac{\hbar}{2} \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}, \quad S_y = \frac{\hbar}{2} \begin{matrix} 0 & -i \\ i & 0 \end{matrix}, \quad S_z = \frac{\hbar}{2} \begin{matrix} 1 & 0 \\ 0 & -1 \end{matrix}$$

=>

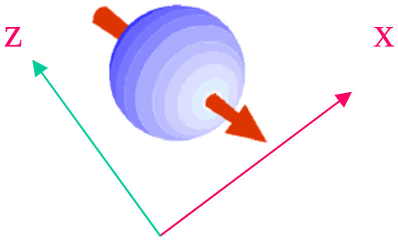
$$S_z = +\frac{\hbar}{2},\ \left|S_z = +\frac{\hbar}{2}\right\rangle = \begin{pmatrix}1\\0\end{pmatrix}; \quad S_z = -\frac{\hbar}{2},\ \left|S_z = -\frac{\hbar}{2}\right\rangle = \begin{pmatrix}0\\1\end{pmatrix};$$

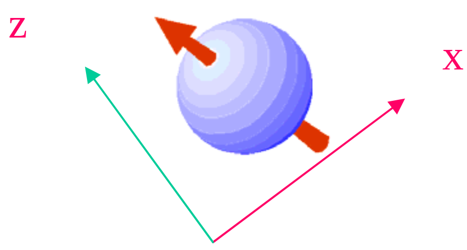


$$|\Phi\rangle = |+x\rangle = \sqrt{\frac{1}{2}}\,|+z\rangle + \sqrt{\frac{1}{2}}\,|-z\rangle$$

z

± z **1/2**





$$|\Phi\rangle \rightarrow |+z\rangle$$

+z

Schroedinger

$$i\hbar \frac{\partial}{\partial t} | \Phi \rangle = H \ | \Phi \rangle$$

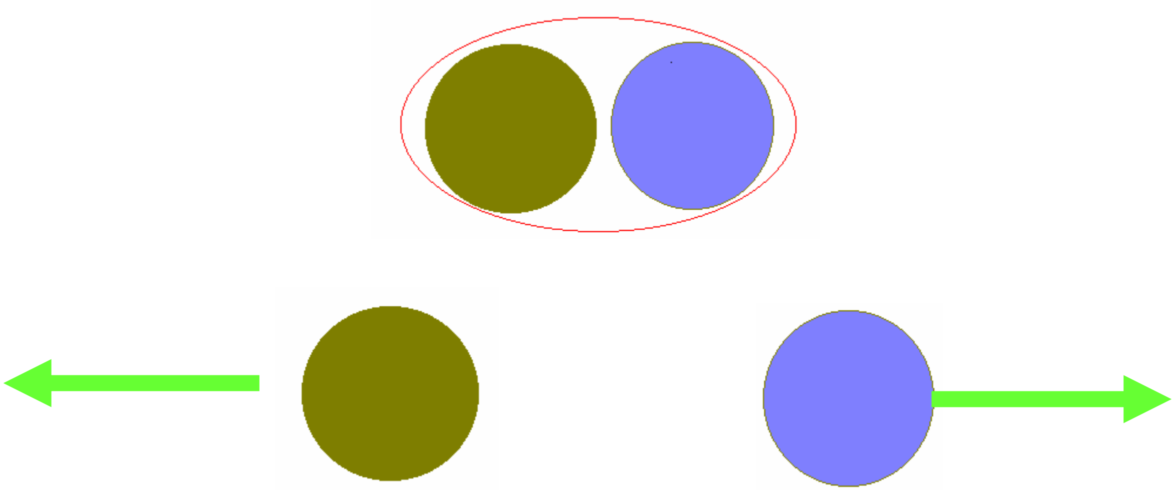
“ ”

H,

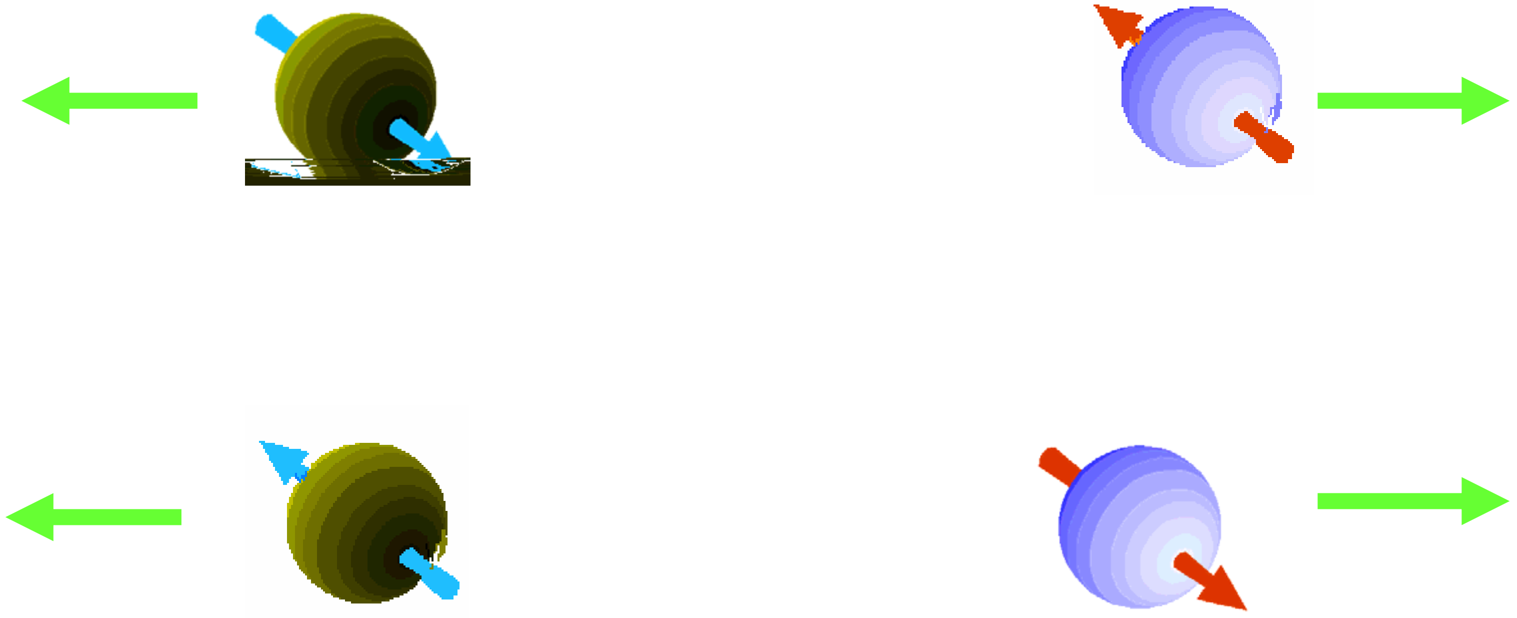
EPR

1935 Einstein,Podolsky,Rosen. Bohm

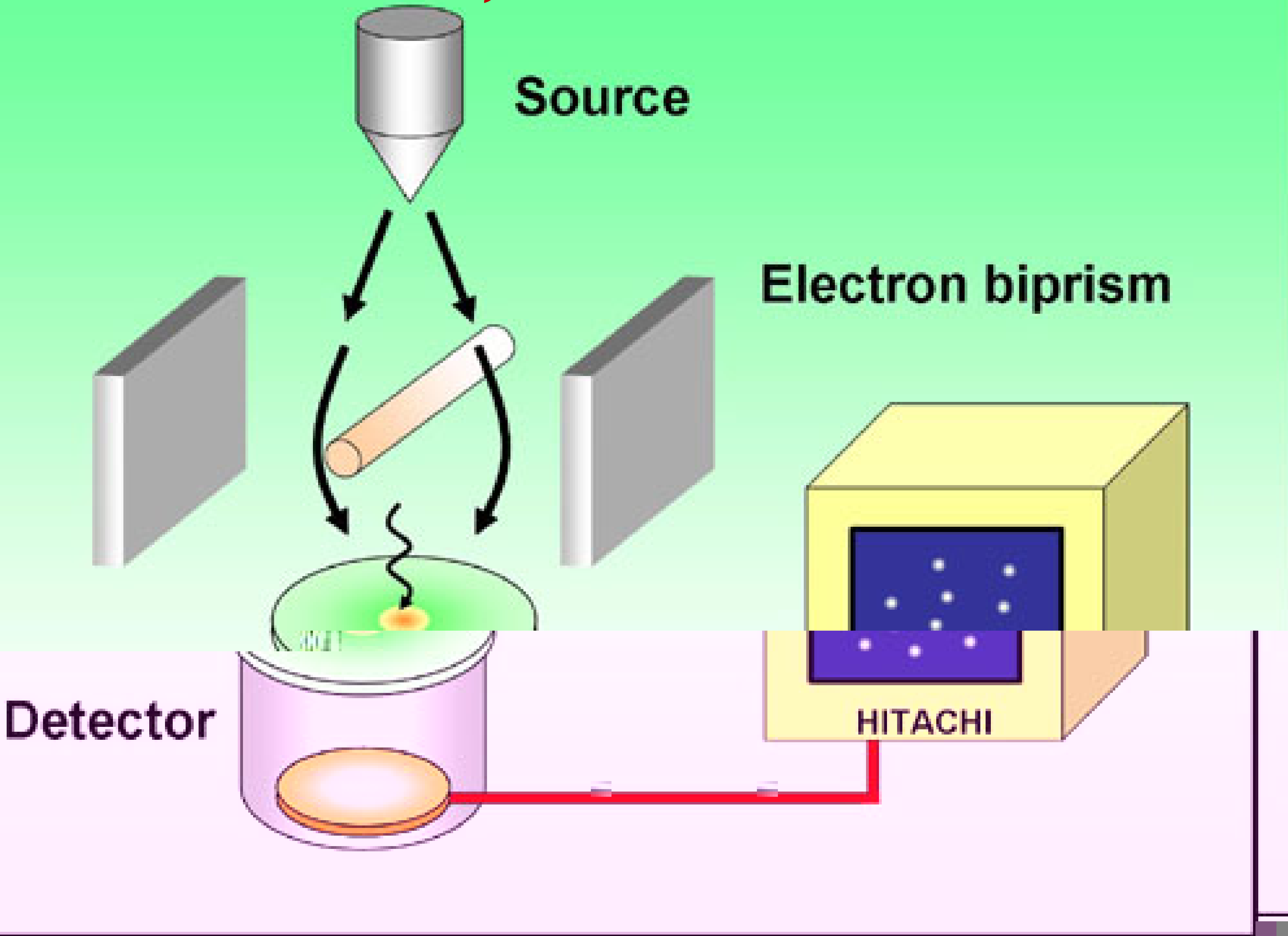
$$t = 0 \qquad |\Phi^-\rangle = \left(|\uparrow_A \downarrow_B\rangle - |\downarrow_A \uparrow_B\rangle\right) \otimes$$



t >T

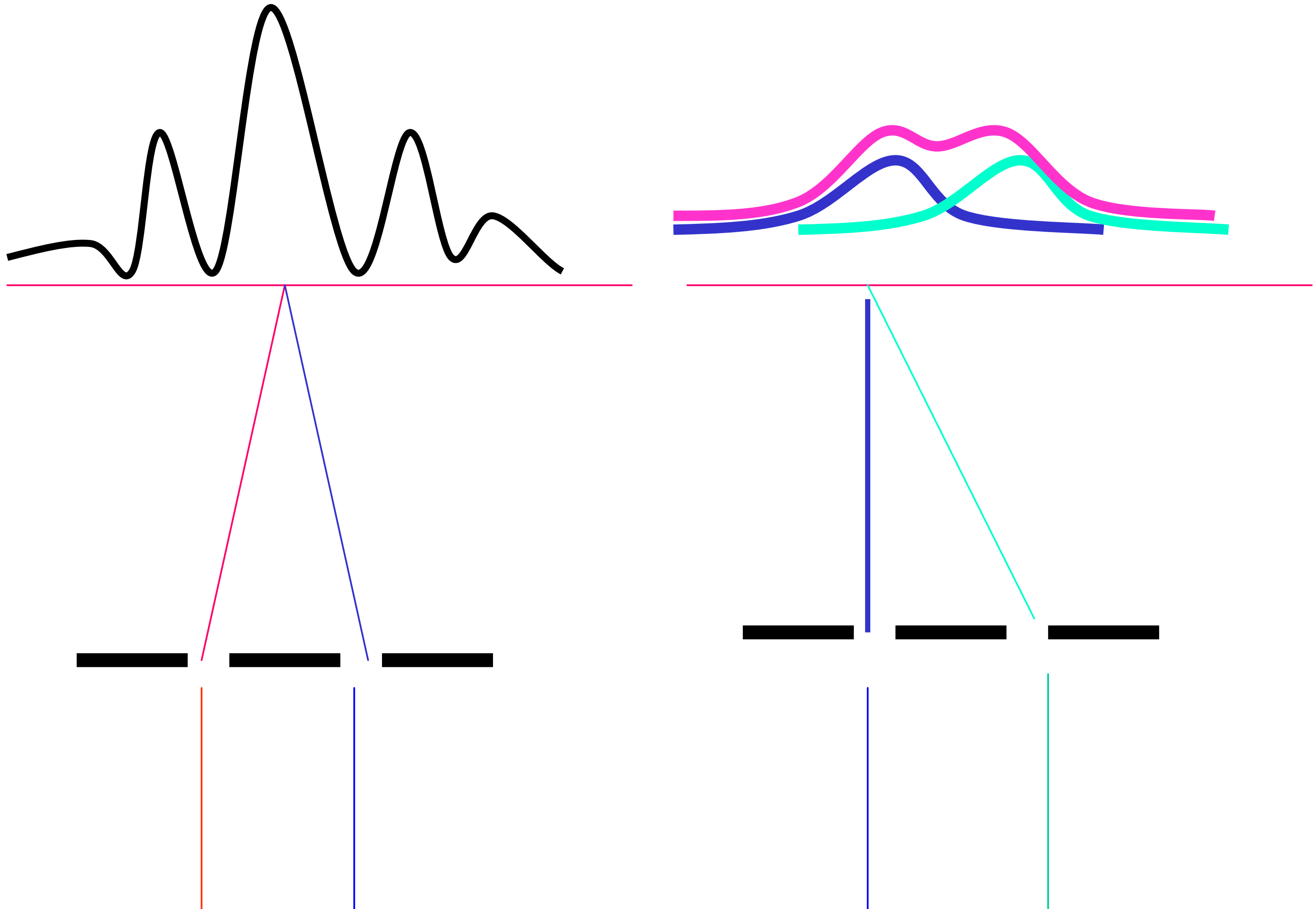


, ! 2

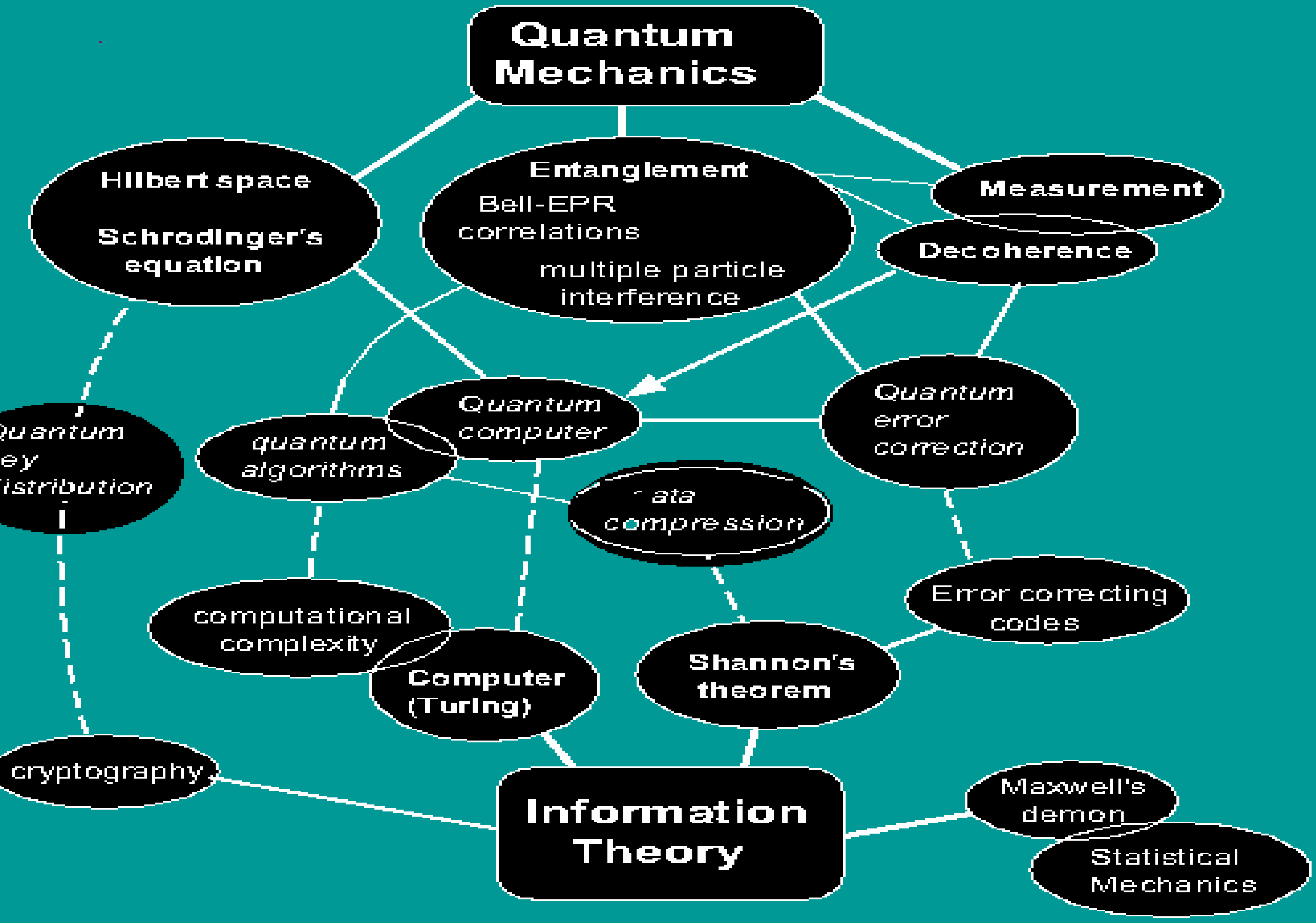


3

Which-way experiment

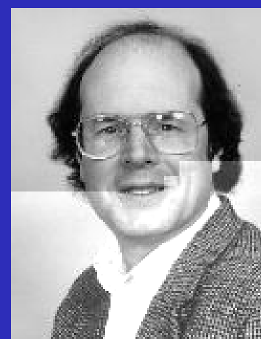


- :
- :



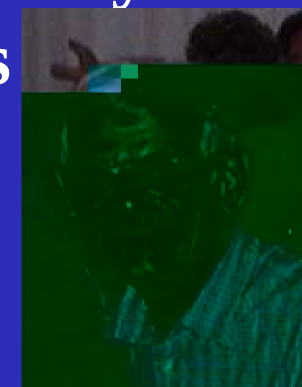
Quantum Mechanics
Hilbert space
Schrodinger's equation
Entanglement
Bell-EPR correlations
multiple particle interference
Measurement
Decoherence
Quantum computer
quantum algorithms
Quantum error correction
uantum
ey
istribution
ata compression
computational complexity
Computer (Turing)
Shannon's theorem
Error correcting codes
cryptography
Information Theory
Maxwell's demon
Statistical Mechanics

Reversible computer
Bennett 1973

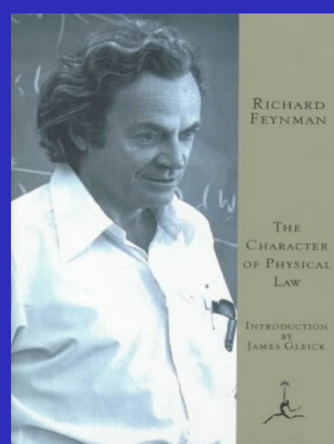


Reversible Computer by quantum mechanics

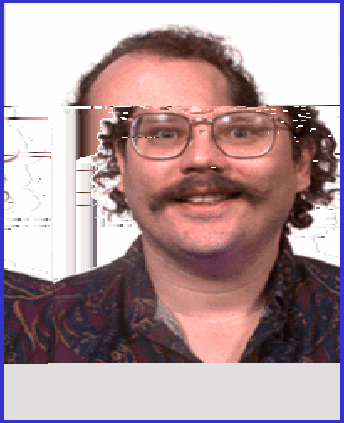
P Benioff 1976



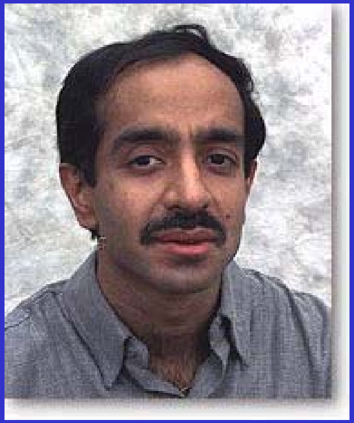
Feynman 1982



Deutsch 1985



Shor, AT&T 1995



Grover, Lucent 1996

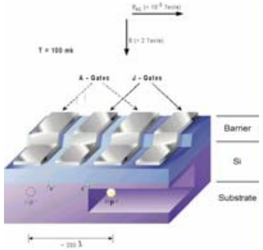
J Jones,Oxford

I Chuang,MIT

1997

(2)

- 1997 NMR
- 1998 NMR
- 1999
  Steane
- 2000 NMR 5
  IBM 7
  NMR
- 2001



2002: 1

2003:2

2005 3

:

2000 2002: 2 7

2003 CORE, 2-Step QKD

2004 , QSS

Parallel QC

2005 10 QC,

•

300

$2^{300} \approx 10^{90}$

________________________________:

Prime factorization (Shor, 1994)	$p_1 p_2 = N$	$\exp\left(n^{1/3}\right) \rightarrow poly(n)$
Pell's equation (Hallgren, 2002)	$x^2 - dy^2 = N$	$\exp\left(n^{1/2}\right) \rightarrow poly(n)$

and also:

- Grover search – appointment scheduling
- period finding – group theory computations
- quantum simulation
- Raz algorithm – distributed simulation
- sampling complexity: disjoint subsets
- finite-round interactive proofs
- pseudo-telepathy (Bell inequalities, game playing)
- quantum cryptography
- quantum data hiding & secret sharing
- quantum digital signature

(BUT, some computations are not sped up at all!)

See DiVincenzo & Loss, cond-mat/9901137

Factorization: heart of encryption

RSA-129

221=13 × 17

114381625757888867669235779976146612010
218296721242362562561842935706935245733
897830597123563958705058989075147599290
026879543541=? Factorized in 1994

349052951084765094914784961990389813341 7
7646384933878439908205 77 X

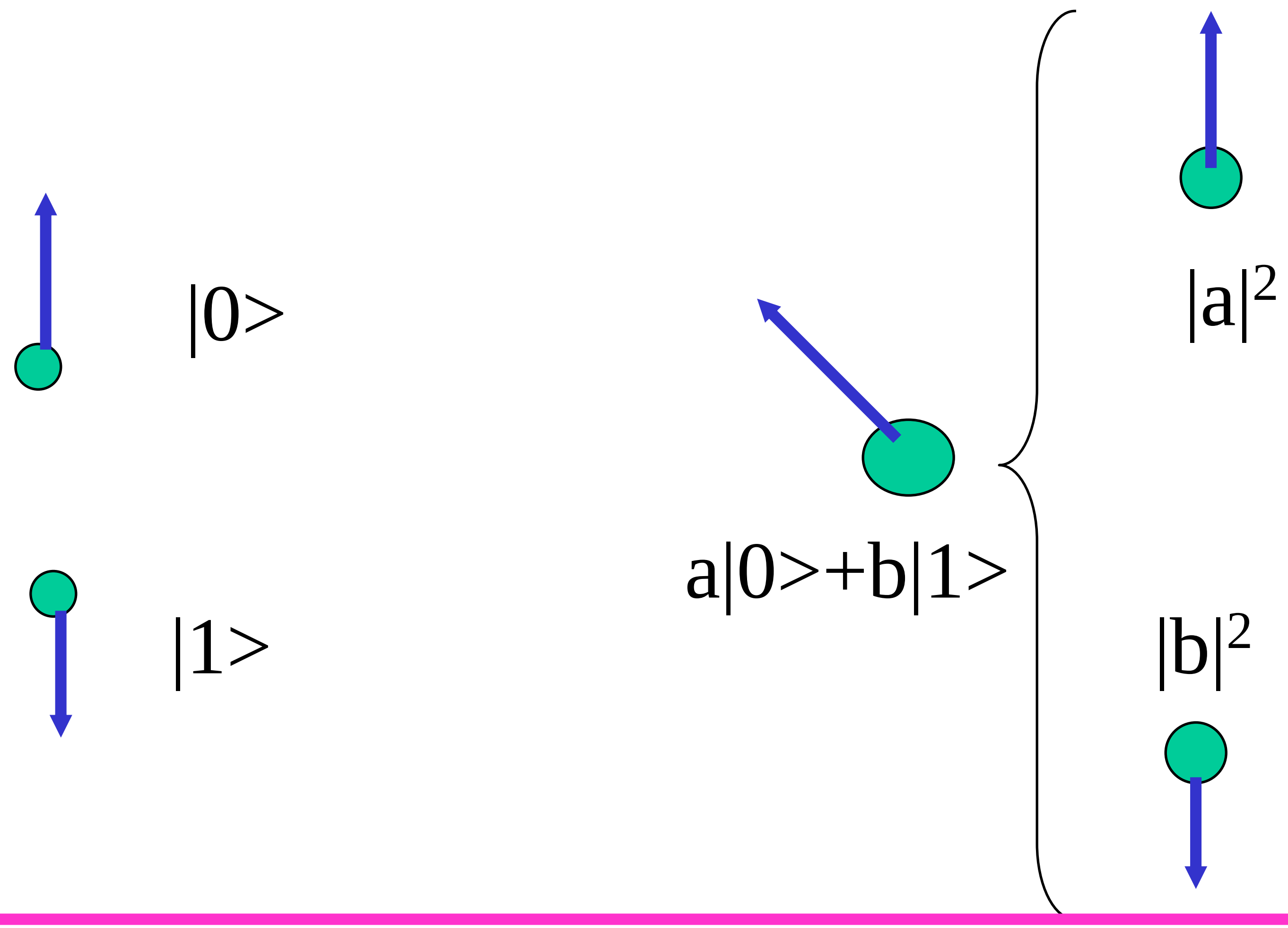
32769132993266709549961988190834461413 1776
4296799294253979828 8533

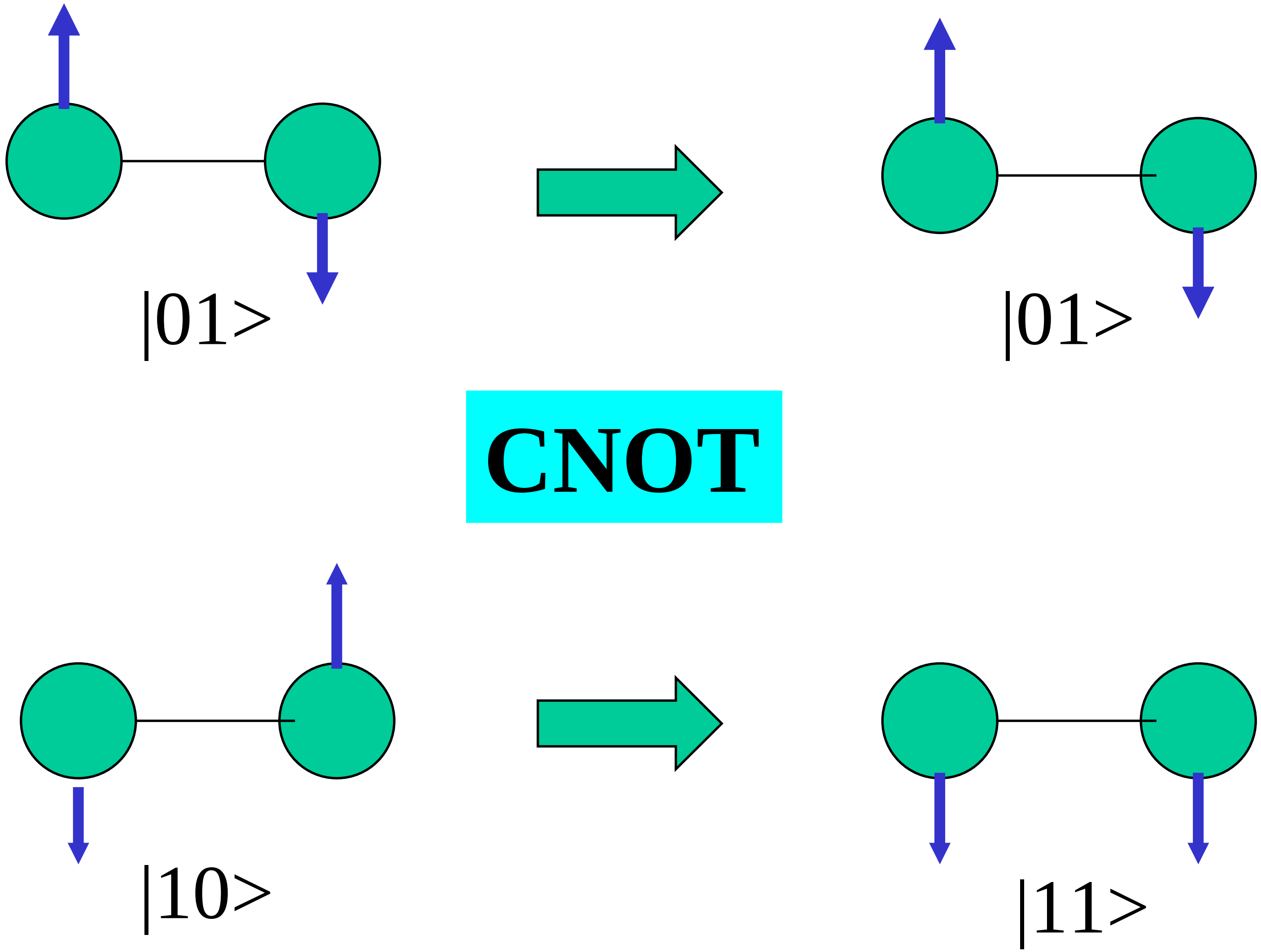
- **Step1: 8 months /600 volunteers /20+ countries**
- **Step2: 45 hours (on a 16K MasPar MP-1 massively parallel computer).**
- **Bank of England uses a 155 digit number for its cryptography.**

- ,

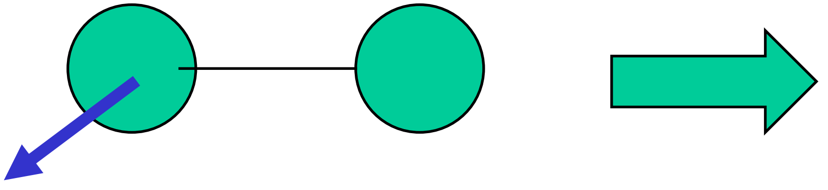
CMOS Device Performance

New device structures are needed to maintain performance...


|0>
|1>
a|0>+b|1>
$|a|^2$
$|b|^2$


|01>
|01>
CNOT
|10>
|11>

$$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|0\rangle \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$$



-

n bits 0, 1, 2, …N-1, $N=2^n$

,

10 → 1K; 23 → 1 M; 30 → 128 M; 33 → 1 G;

50 → **131072 G**; 500 → 10^{467} G; 1000 → 10^{967} G; 5000 → 10^{4967} G

•

$$|\varphi\rangle = \frac{1}{\sqrt{N}}\left\{|0\rangle + |1\rangle + |2\rangle + \cdots + |N-1\rangle\right\}$$

$$U_f|\varphi\rangle = \frac{1}{\sqrt{N}}\left\{|U_f(0)\rangle + |U_f(1)\rangle + \cdots + |U_f(N-1)\rangle\right\}$$

CC requires N operations for the same task CC parallelism=

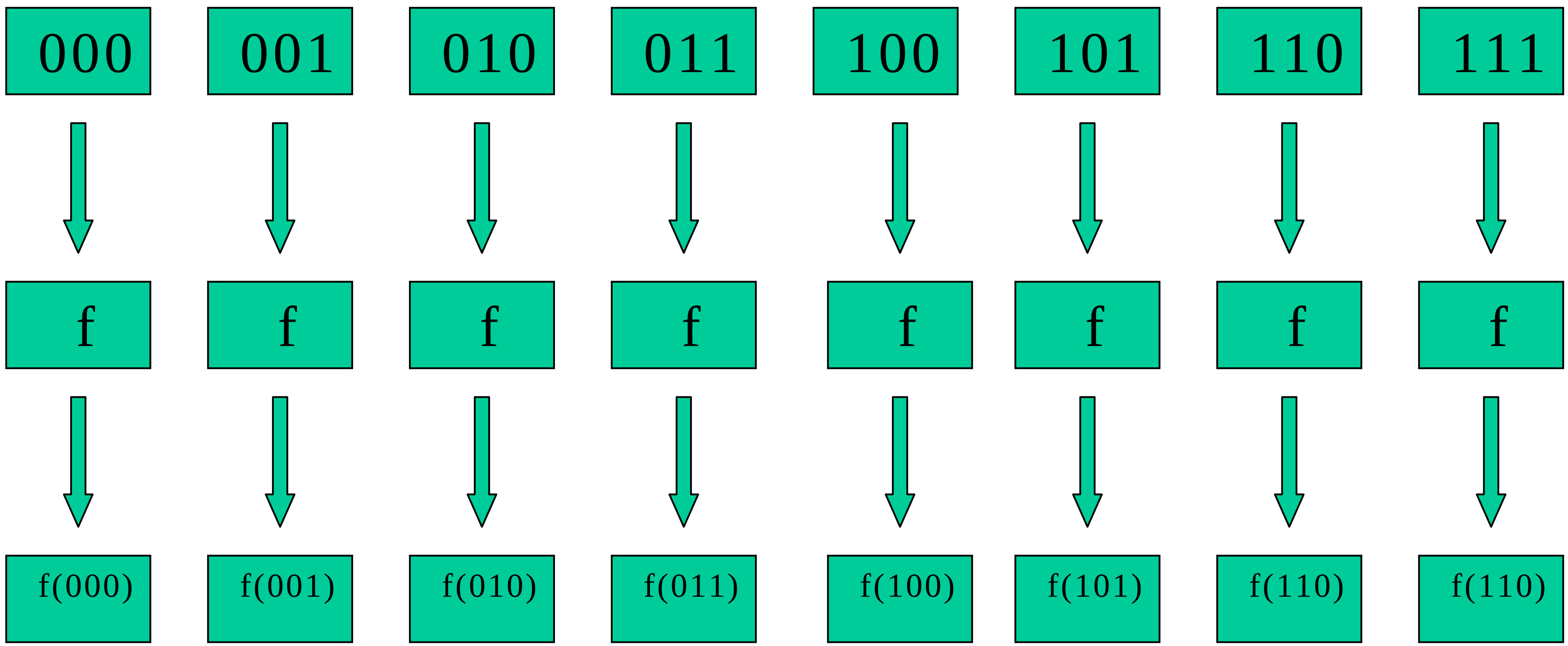
QC parallelism = .

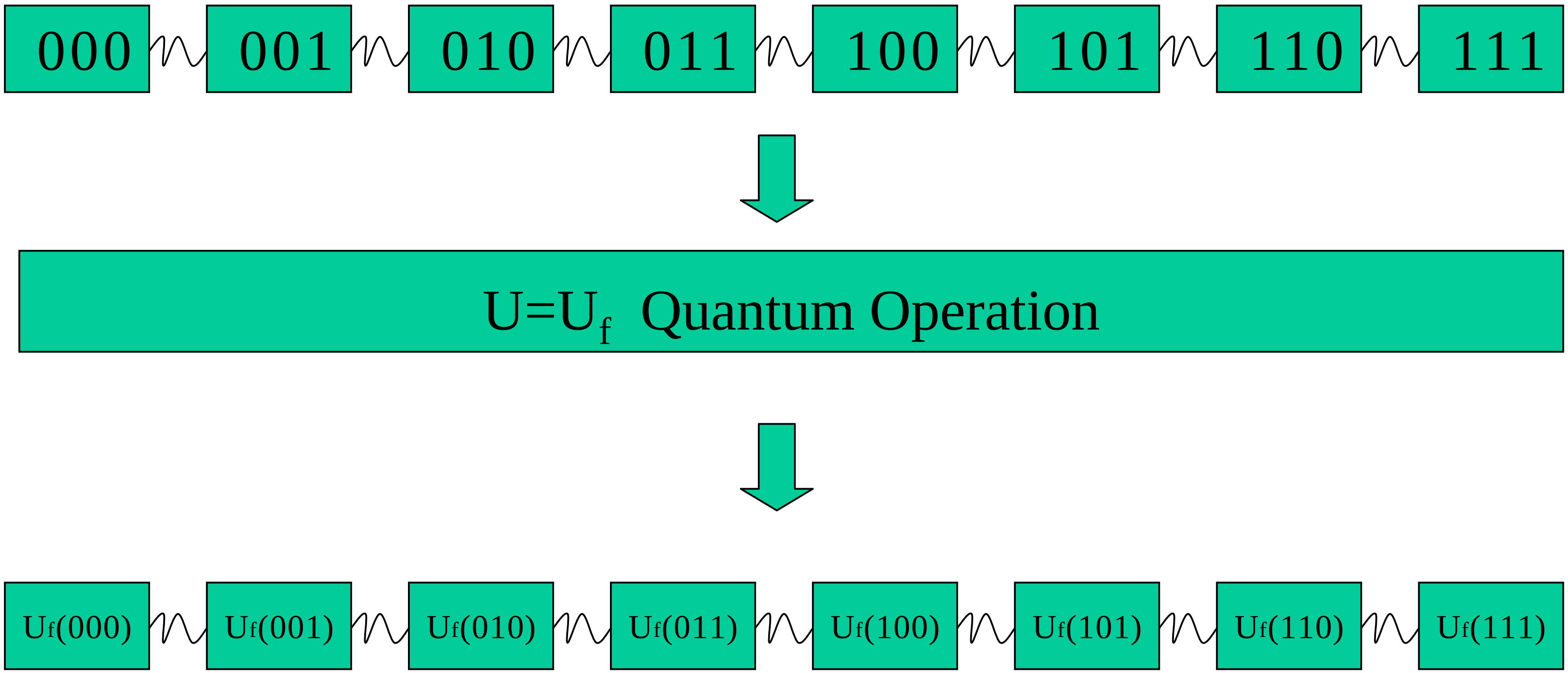
1

N

$\mathrm{Log}_2(N)$

2


000
001
010
011
100
101
110
111
f
f
f
f
f
f
f
f
f(000)
f(001)
f(010)
f(011)
f(100)
f(101)
f(110)
f(110)


000
001
010
011
100
101
110
111
U=Uf Quantum Operation
Uf(000)
Uf(001)
Uf(010)
Uf(011)
Uf(100)
Uf(101)
Uf(110)
Uf(111)

—Shor

- N $f_{y,N}(x) = y^x \bmod N$ r y N r $\left(y^{r/2} \pm 1, N\right)$ N
- r $e^{\log_2 N}$
- $\log_2 N$

$$f_{y,N}(x) = y^x \bmod N$$

y=7, N=15

x	0	1	2	3	4	5	6	7	8
7^x	1	7	49	343	…				
7^x mod 15	1	7	4	13	1	7	4	13	1

$(7^{4/2}+1,15)=(50,15)=5,$

$(7^{4/2}\quad 1,15)=(48,15)=3$

Shor (1)

- N : 1
  2
- $q = 2^L$ $N^2 < q < 2N^2$ L
- 1 L 2
- 1
  (Hadamard $\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}\left|x\right\rangle$)

…

Shor (2)

1. N y

$y^{x} \bmod N$

2

$$\frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle \left| y^{x} \bmod N \right\rangle$$

$N=15, y=7, q=256, L=10$

$$N = 15, y = 7$$

$$
\begin{aligned}
&\left(|0\rangle + |4\rangle + |8\rangle + \cdots + |1020\rangle\right)|1\rangle \\
+&\left(|1\rangle + |5\rangle + |9\rangle + \cdots + |1021\rangle\right)|7\rangle \\
+&\left(|2\rangle + |6\rangle + |10\rangle + \cdots + |1022\rangle\right)|4\rangle \\
+&\left(|3\rangle + |7\rangle + |11\rangle + \cdots + |1023\rangle\right)|13\rangle
\end{aligned}
$$

3. $x = x_0 + jr$

$j = 0, 1, 2,$

$\cdots, M,\ M$ 1

$$\boxed{\left|\phi_{x_0}\right\rangle = \frac{1}{\sqrt{M+1}} \sum_{j=0}^{M} \left|x_0 + jr\right\rangle = \sum_{j=0}^{q/r - 1} \left|x_0 + jr\right\rangle}$$

Fourier

$$U_{QFT}|x\rangle = \frac{1}{2^{L/2}} \sum_{y=0}^{2^L-1} e^{2\pi i x y / 2^L} |y\rangle$$

$$\sum_{y=0}^{2^L-1} C_y |y\rangle$$

C_y

$$|0\rangle + |256\rangle + |512\rangle + |768\rangle$$

256,

$$r = \frac{2^{10}}{256} = 4$$

- N

$N/2$ N

- (L.K.Grover)

1

$O(\sqrt{N})$

•

Quantum mechanics helps in searching a needle in a haystack, PRL 79(1997) 325.

Grover

$$|\psi\rangle = \frac{1}{\sqrt{N}}\left\{|0\rangle + |1\rangle + |2\rangle + \cdots + |\tau\rangle + \cdots + |N-2\rangle + |N-1\rangle\right\} = H|0\rangle$$

$$I_\tau = 1 - 2|\tau\rangle\langle\tau|$$

$$D_{ij} = \begin{cases} \dfrac{2}{N}, & i \neq j \\ \dfrac{2}{N} - 1, & i = j \end{cases}$$

•**Hadmard-Walsch**

•

$$I_0 = 1 - 2|0\rangle\langle 0|$$

•**Hadmard-Walsch**

Hadmard-Walsch W

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|\psi\rangle_0 = \frac{1}{\sqrt{8}}\{|0\rangle+|1\rangle+|2\rangle+|3\rangle+|4\rangle+|5\rangle+|6\rangle+|7\rangle\}$$

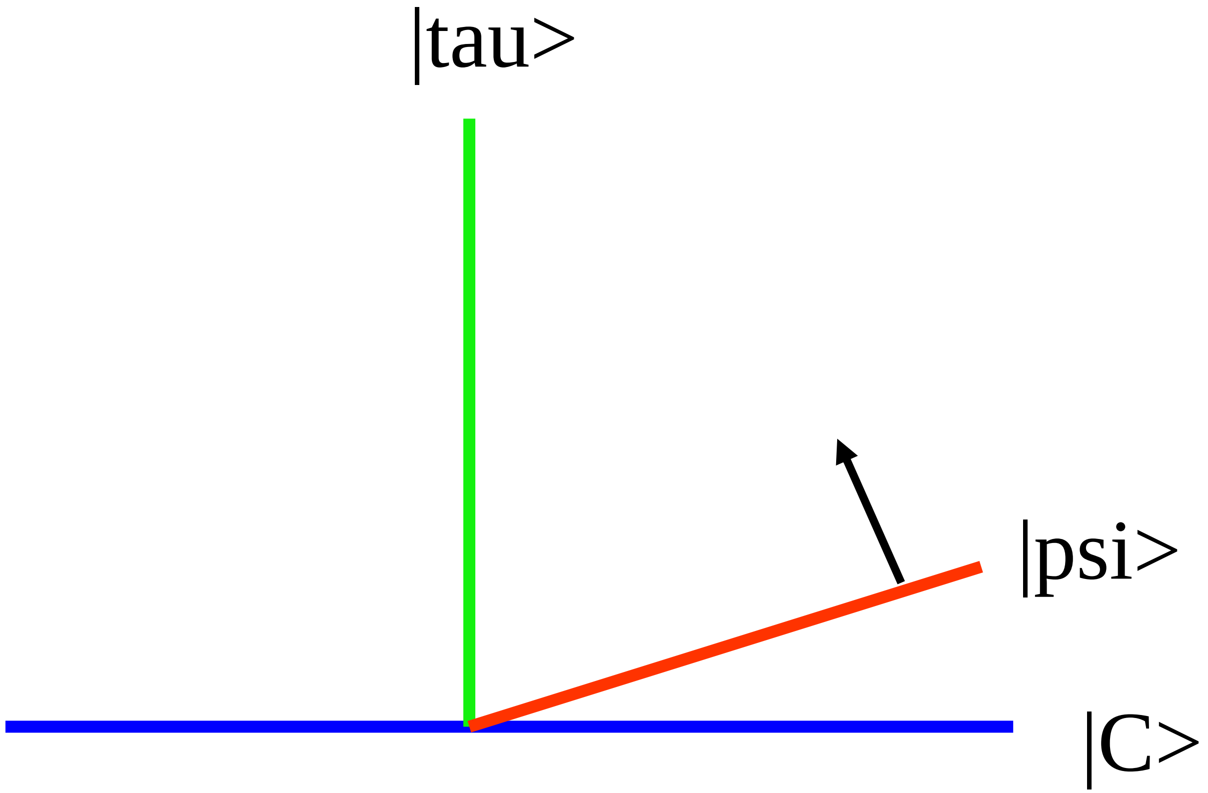
P=0.125

$$|\psi\rangle_1 = \frac{1}{2\sqrt{8}}\{|0\rangle+|1\rangle+|2\rangle+5|3\rangle+|4\rangle+|5\rangle+|6\rangle+|7\rangle\}$$

P=0.781

$$|\psi\rangle_2 = \frac{1}{4\sqrt{8}}\{-|0\rangle-|1\rangle-|2\rangle+11|3\rangle-|4\rangle-|5\rangle-|6\rangle-|7\rangle\}$$

P=0.945



- 2θ j

$$|\varphi_j\rangle = \cos[(2j+1)]\theta|c\rangle + \sin[(2j+1)\theta]|\tau\rangle$$

- |τ> (1)

$$\sin(2j+1)\theta = 1$$

$$(2j+1)\theta = \frac{\pi}{2}$$

$$\therefore j_c = \frac{\pi}{4\theta} - \frac{1}{2} \approx \frac{\pi}{4}\sqrt{N}$$

1

2

3

-

: |0 , |τ>

Zalka |τ> 0-- pi : **By continuity, it is now clear that we can adjust the absolute value of the amplitude of the marked states to any value between these extremes . …"**

Grover: "The above derivation easily extends to the case when the amplitudes in states of , **instead of being inverted by I_γ and I_τ , are rotated by arbitrary phases.** However, the number of operations required to reach τ will be greater. Given a choice, it would be clearly better to use the inversion rather than a different phase rotation, …"

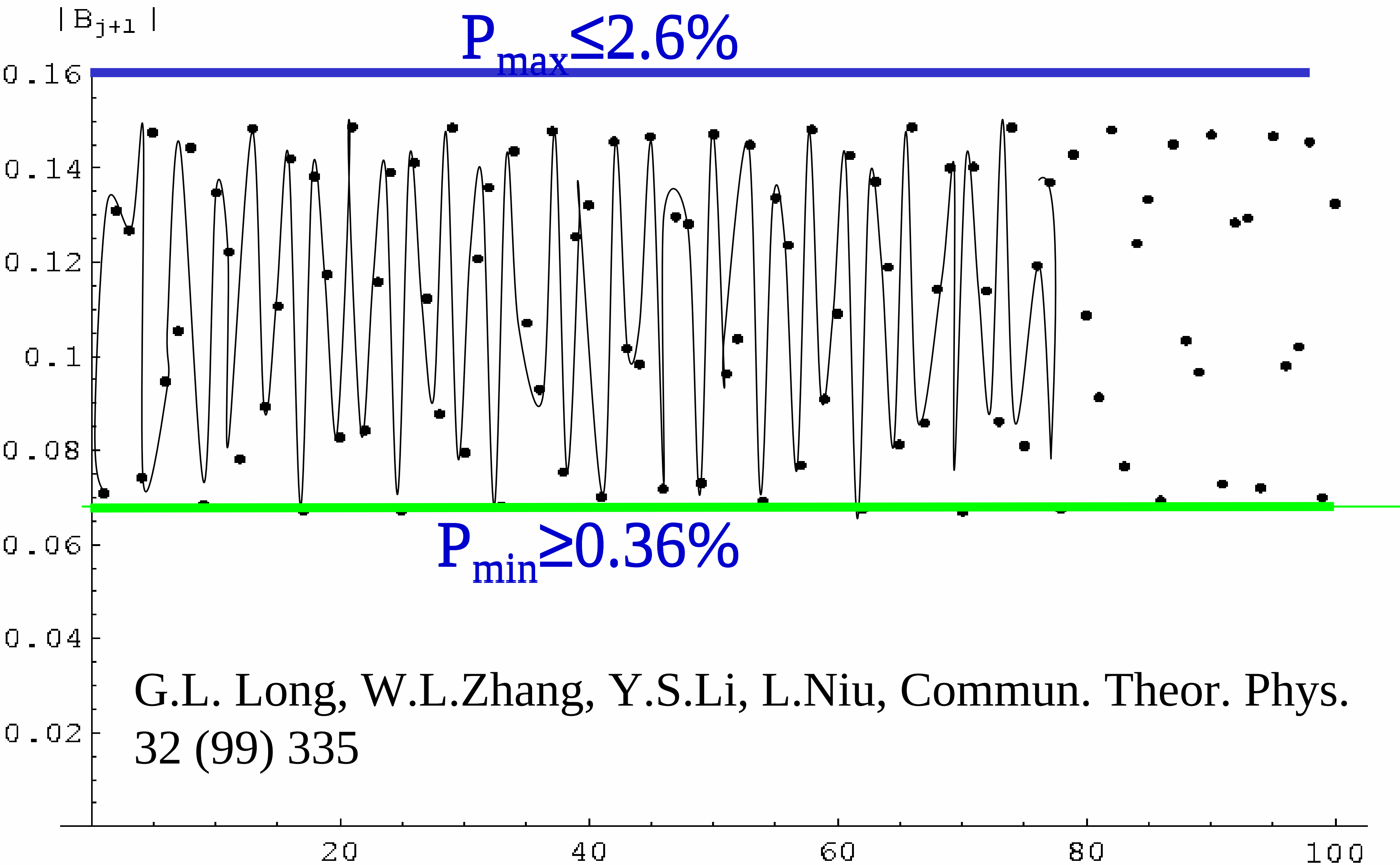
Replacing the phase inversion of the marked state

$$|\psi_j\rangle = A_j\,|c\rangle + B_j\,|\tau\rangle$$

$$\begin{pmatrix} A_{j+1} \\ B_{j+1} \end{pmatrix} = \begin{pmatrix} -e^{i\theta}\dfrac{N-2}{N} & \dfrac{2\sqrt{N-1}}{N} \\ e^{i\theta}\dfrac{2\sqrt{N-1}}{N} & \dfrac{N-2}{N} \end{pmatrix} \begin{pmatrix} A_j \\ B_j \end{pmatrix} = \begin{pmatrix} -e^{-i\theta}\cos 2\beta & \sin 2\beta \\ e^{i\theta}\sin 2\beta & \cos 2\beta \end{pmatrix} \begin{pmatrix} A_j \\ B_j \end{pmatrix}$$

Using direct calculation, we found that the algorithm did not search in the way as expected: it fails totally!

θ=π/4



G.L. Long, W.L.Zhang, Y.S.Li, L.Niu, Commun. Theor. Phys. 32 (99) 335

$$I_0 = I + \left(e^{i\phi} - 1\right)|0\rangle\langle 0|$$

$$I_\tau = I + \left(e^{i\theta} - 1\right)|\tau\rangle\langle\tau|$$

It fails in general unless if the phase rotations satisfy the phase matching condition:

$$\theta = \phi$$

G L Long et al, Phys.Lett. A 262 (99) 27.

2 :

Experimental NMR realization of a generalized quantum search algorithm, G L Long, H Y Yan, Y S Li et al, Phys Lett A286(2001)121

20

Bhattacharya, van Linden,Spreeuw,PRL88 (2002) 137901

- **Analysis of generalized Grover quantum search algorithms using recursion equations**

  Eli Biham, Ofer Biron, Markus Grassl, D A Lidar and Daniel Shapira, Phys. Rev. A63 (2001)012310 :

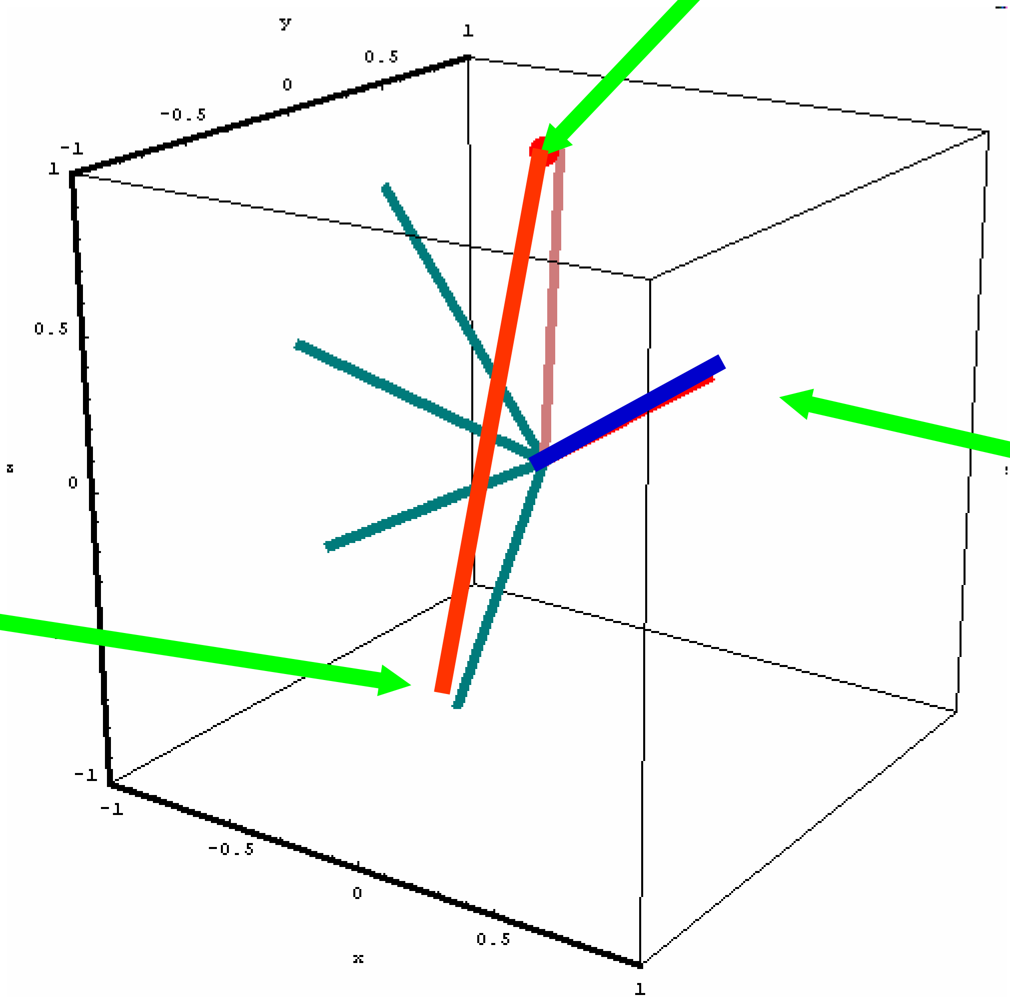
"Moreover, it was found that in order for the algorithm to apply the two rotation angles must be equal, namely, $\beta=\gamma$"

- **Peter Hoyer, Arbitrary phases in quantum amplitude amplification, Physical Review A62 (2000) 052304**
- In particular, the effects of using arbitrary phases in amplitude amplification have been studied in a sequence of papers by Long et al. [2--5]

$(r_f - r_o).\ l_n = 0$

The marked state r_f

The initial state r_o



Rotatio
axis l_n

Using the geometric picture of the quantum search algorithm, it is derived that the phase matching condition is

$$\tan\frac{\theta}{2}\left[\cos(2\beta)+\tan\theta_0\cos\delta\sin 2\beta\right]$$

$$\parallel$$

$$\tan\frac{\phi}{2}\quad 1-\tan\theta_0\sin\delta\sin 2\beta\tan\frac{\theta}{2}$$

G L Long, L. Xiao, Y. Sun, PLA294(2002)143

- (Long Algorithm)

G L Long, Phys. Rev. A 64 (2001) 022307, Grover algorithm with zero theoretical failure rate,

Long Algorithm

Grover 100

180

The maximum probability for finding the marked state in Grover algorithm is not exactly 100%.

n	**1**	**2**	**3**	**≈ 7**	**≈ 10**	**≈ 13**	**≈ 20**
N	**2**	**4**	**8**	**100**	**1000**	$\mathbf{10^4}$	$\mathbf{10^6}$
$\mathbf{P_{max}}$	**0.5**	**1.0**	**0.95**	**0.998**	**0.9996**	$\mathbf{1\text{-}10^{-6}}$	$\mathbf{1\text{-}10^{-6}}$

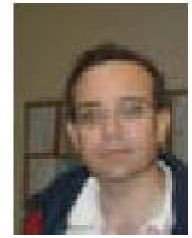
We have improved this by replacing the phase inversions with smaller phase rotations.

$$\theta = \phi = 2 \arcsin \frac{\sin \dfrac{\pi}{4J+6}}{\sin \beta}$$

TABLE II. Examples of $j_{op}+1$ and ϕ.

$N=$	2	4	8	16	100	1000	10^4	10^6	10^8	10^{10}
$j_{op}+1$	1	1	2	3	8	25	79	785	7854	78540
$\frac{\phi}{\pi}$	$\frac{1}{2}$	1	0.677007	0.608799	0.748018	0.854022	0.99989	0.999752	0.999689	0.9973

DiVincenzo criteria



- David DiVincenzo (IBM) – requirements for a scalable quantum computer:

1. The machine must have a collection of bits

   Each bit must be individually addressable, and it must be possible to scale up to a large number of bits

2. It must be possible to initiate all of the bits to zero

3. The error rate should be sufficiently low

   gate

   It must b
   operation

   Reli... readout of the final result should be possible

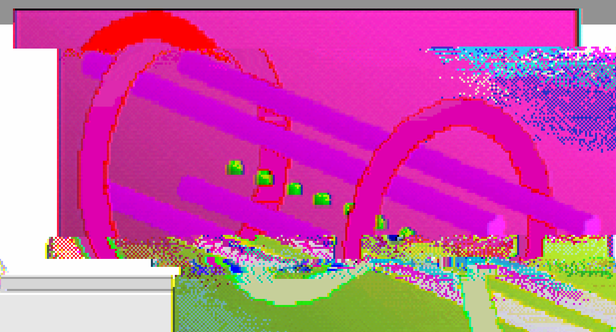
Physical implementations

Many sub-fields of physics have proposals for QC

- Liquid-state NMR
- NMR spin lattices
- Linear ion-trap spectroscopy
- Neutral-atom optical lattices
- Cavity QED + atom
- Linear optics
- Nitrogen vacancies in diamond
- Electrons in liquid He
- Superconducting Josephson junctions
  - charge qubits
  - flux qubits
  - phase qubits
- Quantum Hall qubits
- Coupled quantum dots
  - spin, charge, excitons
- Spin spectroscopies, impurities in semiconductors

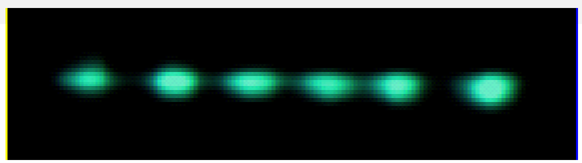
Ion traps

- Qubit: internal electronic state of atomic ion in a trap
  (ground and excited)



oupling: use
uantised vibrational
node along linear axis
phonons)

ingle qubit gates:
sing laser



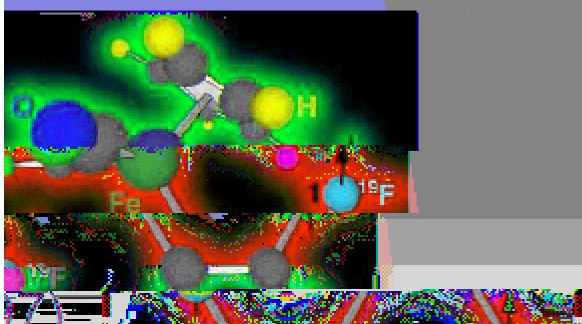
Co
q
m
(p

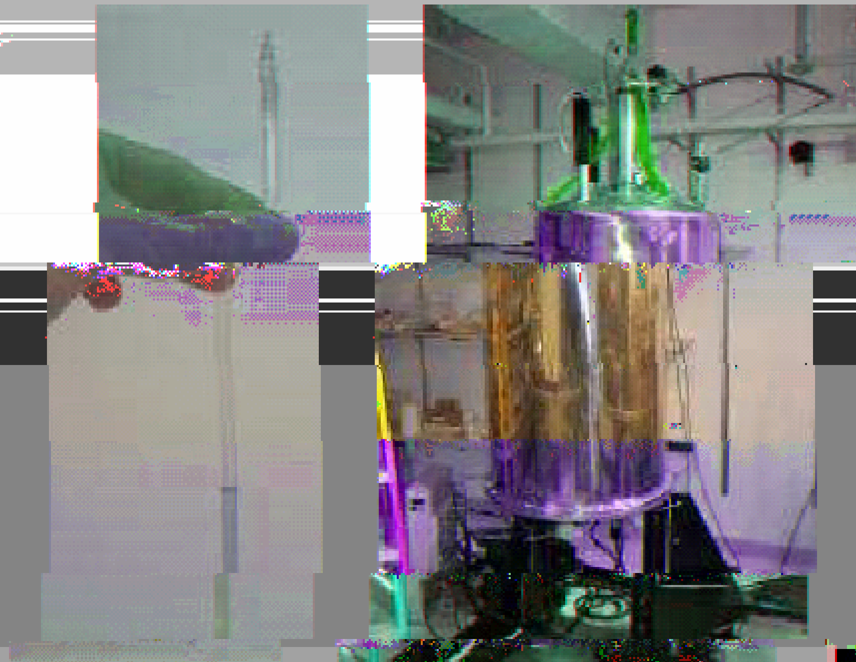
S
u

Cirac and Zoller, *Phys. Rev. Lett.* (1995)

Nuclear magnetic resonance (NMR)

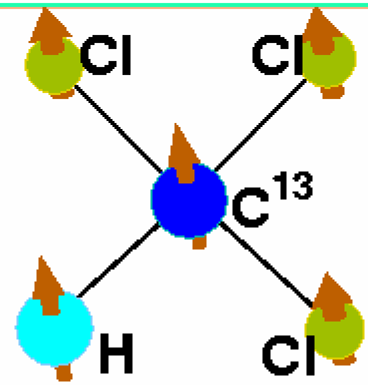
- Qubit: nuclear spins of atoms in a designer molecule
- Coupling and single-qubit gates: RF pulses tuned to NMR frequency





Gershenfeld and Chuang, Science (1997)

An Example: Labeled Chloroform at Room Temperature



Chlorine $(3/2)$ spins interact very weakly with carbon^{13} $(1/2)$ and proton $(1/2)$ spins

- Hamiltonian for the proton and carbon^{13} spins in a strong magnetic field along z:

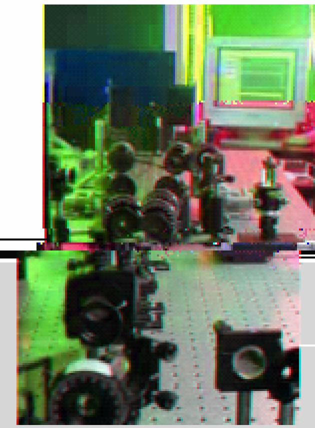
$$H = \omega_H \sigma_z^{(H)}/2 + \omega_C \sigma_z^{(C)}/2 + J\sigma_z^{(H)}\sigma_z^{(C)}/4 + H_{RF} + H_{rest}$$

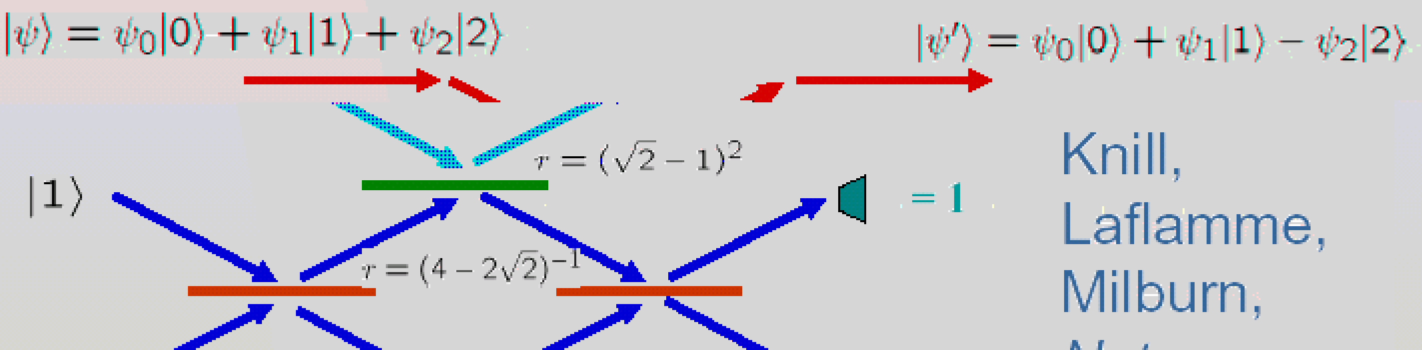
At 11.4T: $\omega_H \approx 500$MHz $\quad J \approx 215$Hz $\quad |H_{rest}| \lesssim 2$Hz

$\omega_C \approx 125$MHz

Linear optics

- Qubit: polarisation of a single photon
- Coupling: via measurement
- Single-qubit gates: polarisation rotation





Knill, Laflamme, Milburn,

Superconducting Josephson junctions

Qubit: a) Magnetic flux trapped in loop

b) Cooper pair charge on metal box

c) Charge-phase

- Coupling: capacitive/inductive
- Single-qubit gates: flux bias, charge on gate, current through junction

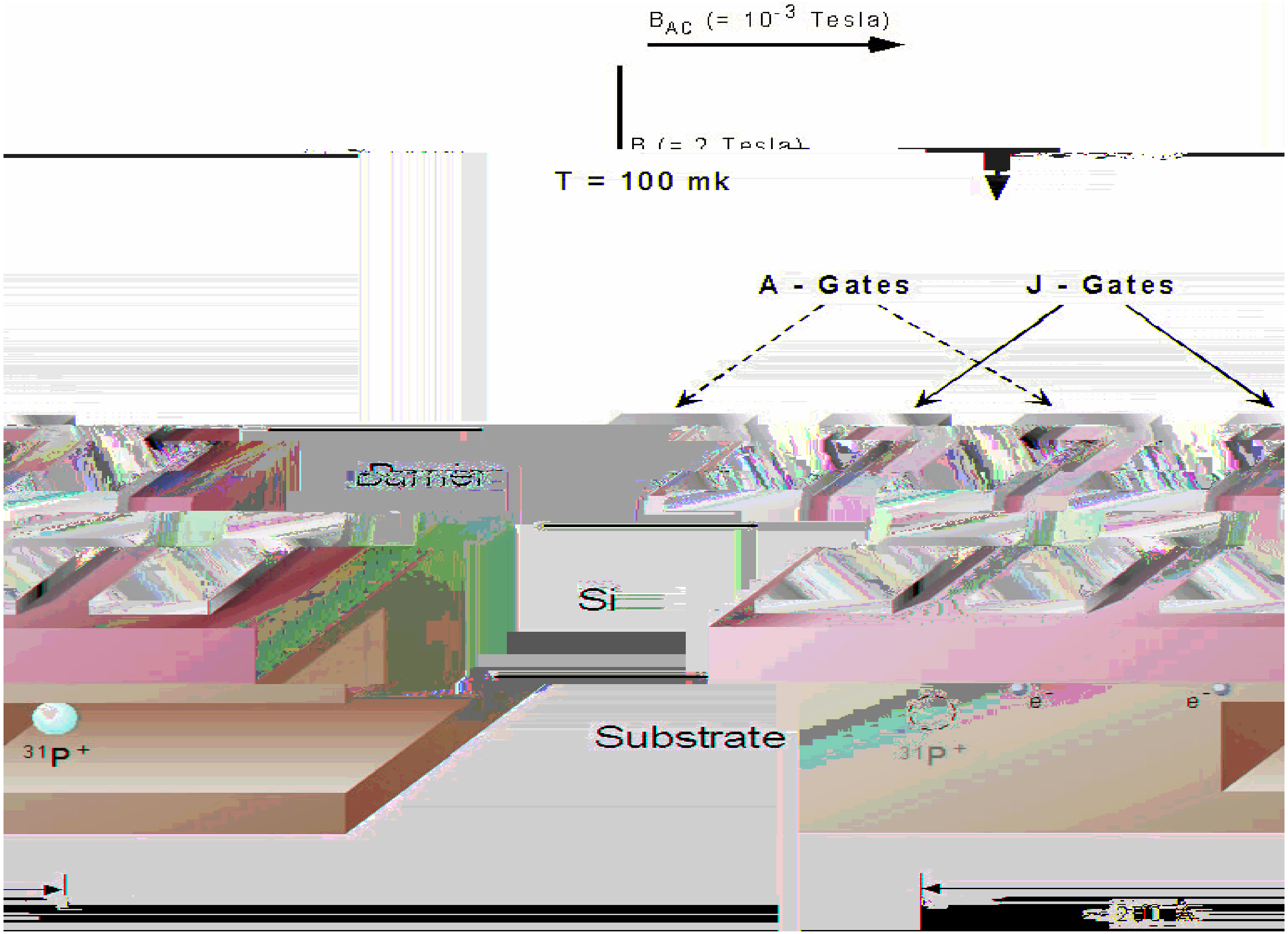
Nakamura, Pashkin, Tsai, *Nature* (1999)

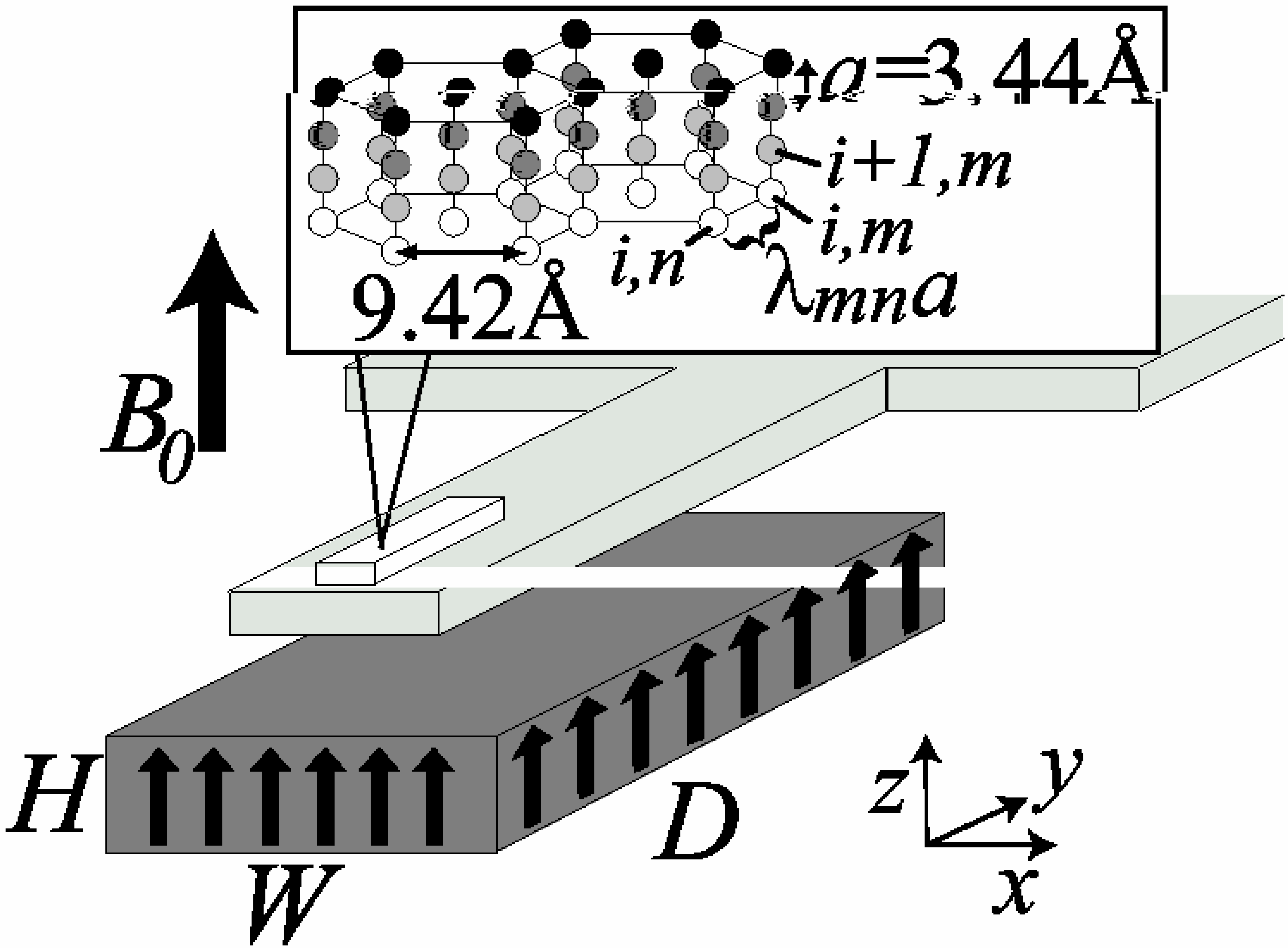
Silicon quantum computing

- Qubit:
  - Nuelcar spin of single P donor
  - Electron spin of single donor
  - Electron charge
- Coupling: gate-controlled electron-electron interaction
- Single-qubit gates: NMR pulse; gate bias in magnetic material; charge on gate

Kane, *Nature* (1998)

CENTRE FOR QUANTUM COMPUTER TECHNOLOGY
AUSTRALIAN RESEARCH COUNCIL SPECIAL RESEARCH CENTRE


B_AC (= 10^-3 Tesla)
B (= 2 Tesla)
T = 100 mk
A - Gates
J - Gates
Si
Substrate
31P+
e-
31P+
e-



a=3.44Å
i+1,m
i,m
i,n
λmna
9.42Å
B0
H
W
D
z
y
x

Table 4.0-1

The Mid-Level Quantum Computation Roadmap: Promise Criteria

QC Networkability		QC Approach	The DiVincenzo Cri[teria]				
			Quantum Computation				
#6	#7		#1	#2	#3	#4	#5
🔴	🔴	NMR	🔴	🟠	🟠	🟢	🟠
🟠	🟠	Trapped Ion	🟠	🟢	🟠	🟢	🟢
🟠	🟠	Neutral Atom	🟠	🟢	🟠	🟠	🟠
🟠	🟠	Cavity QED	🟠	🟢	🟠	🟠	🟢
🟠	🟢	Optical	🟠	🟠	🟢	🟠	🟠
🔴	🔴	Solid State	🟠	🟠	🟠	🟠	🟠
🔴	🔴	Superconducting	🟠	🟢	🟠	🟠	🟠
...with 'Promise' symbols		Unique Qubits	This field is so diverse that it is not feasible to label ...				

Entanglement and Squeezing in Solid State Circuits

Entanglement and squeezing in solid-state circuits, W Y Huo and GLL, *New Journal of Physics* **10** (2008) 013026

Generation of squeezed states of nanomechanical resonator using three-wave mixing, WY Huo and GLL, APL, 92, 133102 2008

Strong Coupling in Circuit QED system:

A. Blais, et al. Phys. Rev. A, 69: 062320 (2004),

A. Wallraff, et al . Nature, 431: 162–167 (2004),\

Sun, Wei, Liu and Nori, PRB 2006

Proposals for generation squeezed states in solid state circuits:

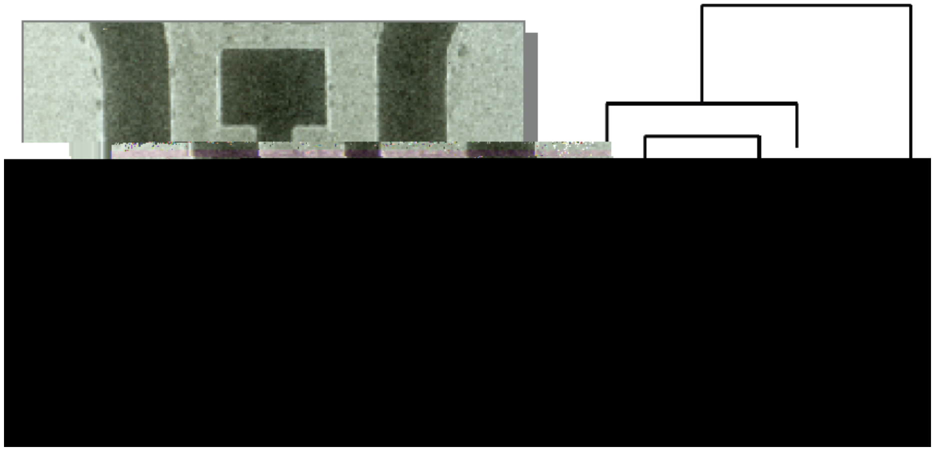
K. Moon, S. M. Girvin, PRL, 95: 140504 (2005)

Zhou X X, A. Mizel, PRL, 97, 267201 (2006)

P. Rabl, et al PRB 70 205304 (2004)

R. Ruskov, et al PRB 71 235407 (2005)

T. Ojanen, J. Salo, PRB, 75, 184508 (2007)



Superconducting Charge qubit

$$H = -\frac{E_c}{2}(1-2n_g)\sigma_z - E_J \cos(\frac{\pi\Phi_e}{\Phi_0})\sigma_x$$

$$|n=1\rangle = |\downarrow\rangle_z$$

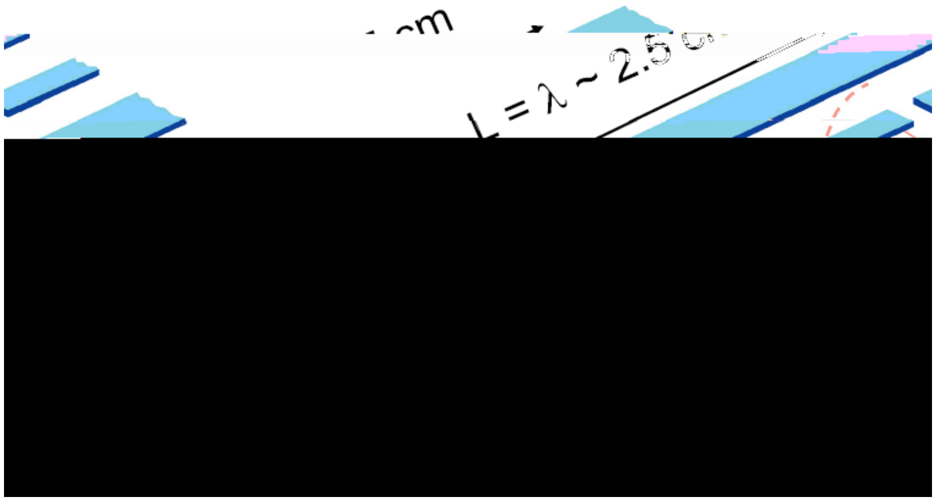
$$|n=0\rangle = |\uparrow\rangle_z$$

$$E_c = \frac{(2e)^2}{2C_\Sigma} \qquad n_g = \frac{C_g V_g}{2e}$$

V_g Gate voltage

Φ_e External flux

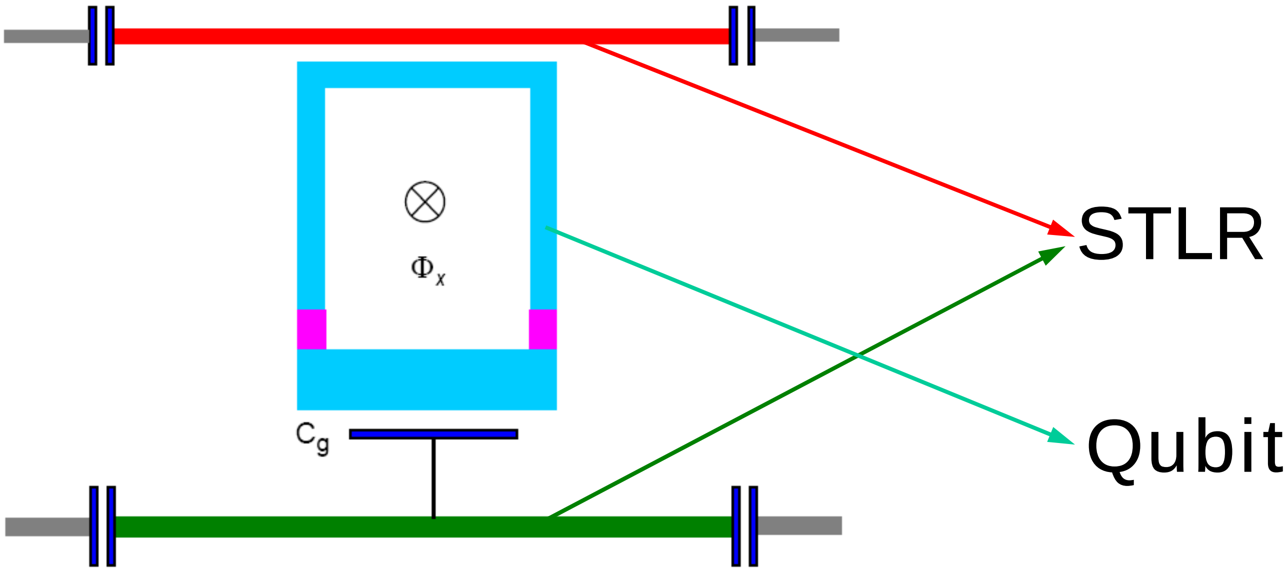
A. Blais, et al. Phys. Rev. A, 69: 062320 (2004)



One voltage mode is coupled to the charge qubit

$$H = \hbar\omega\left(a^\dagger a + \frac{1}{2}\right) - \frac{E_c}{2}(1-2n_g)\sigma_z - E_J\cos\left(\frac{\pi\Phi_e}{\Phi_0}\right)\sigma_x$$

$$n_g = \frac{C_g(V_{DC} + V_q)}{2e} \qquad V_q = V_0(a^\dagger + a)$$



[redacted]

$$-E_J \cos\frac{\pi(\Phi_e+\Phi_q)}{\Phi_0}\sigma_x + \frac{eC_gV_0}{C_\Sigma}(a^\dagger + a)\sigma_z$$

Expanding the effective Josephson coupling to the first order in Φ_q/Φ_0

$$\begin{aligned} H &= \hbar\omega_a a^\dagger a + \hbar\omega_b b^\dagger b - \frac{1}{2}E_c(1-2n_g)\sigma_z - E_J\cos\frac{\pi\Phi_e}{\Phi_0}\sigma_x \\ &\quad +\hbar\lambda_a'(a^\dagger + a)\sigma_z - i\hbar\lambda_b'(b^\dagger - b)\sigma_x \end{aligned}$$

In the eigenspace of the qubit

$$\begin{aligned} H &= \hbar\omega_a a^\dagger a + \hbar\omega_b b^\dagger b - \frac{1}{2}\hbar\Omega\rho_z + \hbar\lambda_a(a^\dagger\rho_- + a\rho_+) \\ &\quad +i\hbar\lambda_b(b^\dagger\rho_- - b\rho_+) \end{aligned}$$

Low temperature, Resonating

$$H = \hbar\Omega a^\dagger a + \hbar\Omega b^\dagger b - \frac{1}{2}\hbar\Omega\rho_z + \hbar\lambda_a(a^\dagger\rho_- + a\rho_+) + i\hbar\lambda_b(b^\dagger\rho_- - b\rho_+)$$

Initial State $|0\rangle|0\rangle|e\rangle$

State at time ***t***

$$|\psi(t)\rangle = e^{-i\frac{\Omega t}{2}}\left[\cos\Lambda t|0\rangle|0\rangle|e\rangle + \sin\Lambda t\big(\sin\alpha|0\rangle|1\rangle|g\rangle - i\cos\alpha|1\rangle|0\rangle|g\rangle\big)\right]$$

$$\Lambda = \sqrt{\lambda_a^2 + \lambda_b^2} \quad \cos\alpha = \lambda_a/\Lambda \quad \sin\alpha = \lambda_b/\Lambda$$

When $\Lambda t = \pi/2$

The entangled state of the two STLRs, also the single-photon entangled state

$$|\Psi\rangle = \sin\alpha|0\rangle|1\rangle - i\cos\alpha|1\rangle|0\rangle$$

External biased flux $\Phi_e = 0$

$$
\begin{aligned}
H &= \hbar\omega_a a^\dagger a + \hbar\omega_b b^\dagger b - \frac{1}{2}E_c(1-2n_g)\sigma_z - E_J \cos\frac{\pi(\Phi_e+\Phi_q)}{\Phi_0}\sigma_x \\
&\quad + \frac{eC_g V_0}{C_\Sigma}(a^\dagger + a)\sigma_z
\end{aligned}
$$

Expanding the effective Josephson coupling to the second order in Φ_q/Φ_0

$$
\begin{aligned}
H_N &= \hbar\omega_a a^\dagger a + \hbar\omega_b b^\dagger b - \frac{1}{2}\hbar\Omega\rho_z + \hbar g_a(a^\dagger\rho_- + a\rho_+) \\
&\quad + \hbar g_b(b^{\dagger 2}\rho_- + b^2\rho_+)
\end{aligned}
$$

three-body nonlinear interaction Hamiltonian

$$
\begin{aligned}
H_N &= \hbar\omega_a a^\dagger a + \hbar\omega_b b^\dagger b - \frac{1}{2}\hbar\Omega\rho_z + \hbar g_a(a^\dagger\rho_- + a\rho_+) \\
&\quad + \hbar g_b(b^{\dagger 2}\rho_- + b^2\rho_+)
\end{aligned}
$$

Large detuning

$$
\begin{aligned}
|\Delta_a| &= |\Omega - \omega_a| \gg G \\
|\Delta_b| &= |\Omega - 2\omega_b| \gg G
\end{aligned}
\qquad G = \sqrt{g_a^2 + g_b^2}
$$

Qubit: nonlinear media

Canonical Transformation $H_S = e^{-S} H e^{S}$

$$
S = \frac{g_a}{\Delta_a}\left(a^\dagger\rho_- - a\rho_+\right) + \frac{g_b}{\Delta_b}\left(b^{\dagger 2}\rho_- - b^2\rho_+\right)
$$

Keeping the qubit in the ground state, the effective Hamiltonian of the two STLRs reads

$$H_S = \hbar\omega_a a^\dagger a + \hbar\omega_b b^\dagger b - \frac{1}{2}\hbar g_a g_b \left(\frac{1}{\Delta_a} + \frac{1}{\Delta_b}\right)\left(b^{\dagger 2} a + a^\dagger b^2\right)$$

If $\omega_a = 2\omega_b = 2\omega$

In the interaction picture

$$H_I = \hbar\kappa\left(b^{\dagger 2} a + a^\dagger b^2\right)$$

$\kappa = -g_a g_b/\Delta$ Depends on the frequency and is tunable

In the parametric approximation

$$H_I = \hbar\kappa\beta\left(b^{\dagger 2}e^{-i\phi} + e^{i\phi}b^2\right)$$

β : Amplitude of the pump field

ϕ : phase of the pump field

Evolution operator $U(t) = e^{-i\kappa\beta t\left(b^{\dagger 2}e^{-i\phi}+e^{i\phi}b^2\right)}$

$$\Updownarrow$$

Squeezing operator $S(\xi) = e^{-i\frac{\xi}{2}(b^{\dagger 2}e^{-i\phi}+b^2e^{i\phi})}$

Setting the phase $\phi = \pi/2$

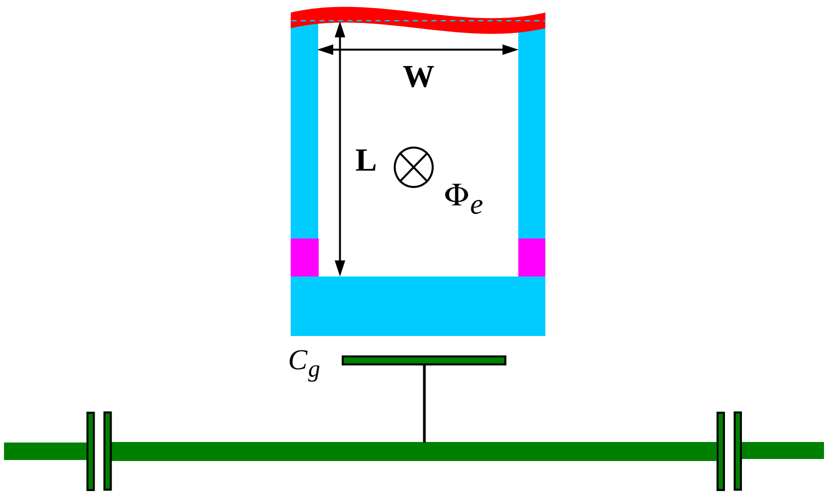
The two conjugate operators

$$X_1 = \frac{1}{2}\left(b + b^\dagger\right), X_2 = \frac{1}{2i}\left(b - b^\dagger\right)$$

The variances of the two operators become

$$\Delta X_1 = \sqrt{\langle X_1^2 \rangle - \langle X_1 \rangle^2} = \frac{e^{-\xi}}{2}$$

$$\Delta X_2 = \sqrt{\langle X_2^2 \rangle - \langle X_2 \rangle^2} = \frac{e^{\xi}}{2}$$



A nanomechanical resonator is fabricated as one part of the SQUID. The effective area of the SQUID is

$$S = W(L + x)$$

$x = \sqrt{\hbar/(2M\omega_b)}(b^\dagger + b)$ is the displacement operator

The effective flux threading the SQUID becomes

$$\Phi_e = \Phi_e^0 + BWx$$

Generation of squeezed states of nanomechanical resonator using three-wave mixing, WY Huo and GLL, APL, 92, 133102 2008

The Hamiltonian of the system

$$
\begin{aligned}
H &= \hbar\omega_a a^\dagger a + \hbar\omega_b b^\dagger b - \frac{1}{2}E_c(1-2n_g)\sigma_z \\
&\quad - E_J \cos\frac{\pi(\Phi_e^0 + BWx)}{\Phi_0}\sigma_x + \frac{eC_gV_0}{C_\Sigma}(a+a^\dagger)\sigma_z
\end{aligned}
$$

Following the above derivation

In interaction picture

$$H_I(t) = \hbar\kappa\beta(b^{\dagger 2}e^{-i\phi} + b^2 e^{i\phi})$$

Squeezing operator

$$S(\xi) = e^{-i\frac{\xi}{2}(b^{\dagger 2}e^{-i\phi}+b^2e^{i\phi})} = e^{-i\kappa\beta t(b^{\dagger 2}e^{-i\phi}+b^2e^{i\phi})}$$

ϕ $\pi/2$

$$\Delta x = \sqrt{\langle x^2\rangle - (\langle x\rangle)^2} = x_0 e^{-\xi}$$

$$\Delta p = \sqrt{\langle p^2\rangle - (\langle p\rangle)^2} = p_0 e^{\xi}$$

Considering the influence of fluctuation

$$\Delta x = x_0\sqrt{e^{-2\xi} + (\frac{\gamma t}{2})e^{2\xi}}$$

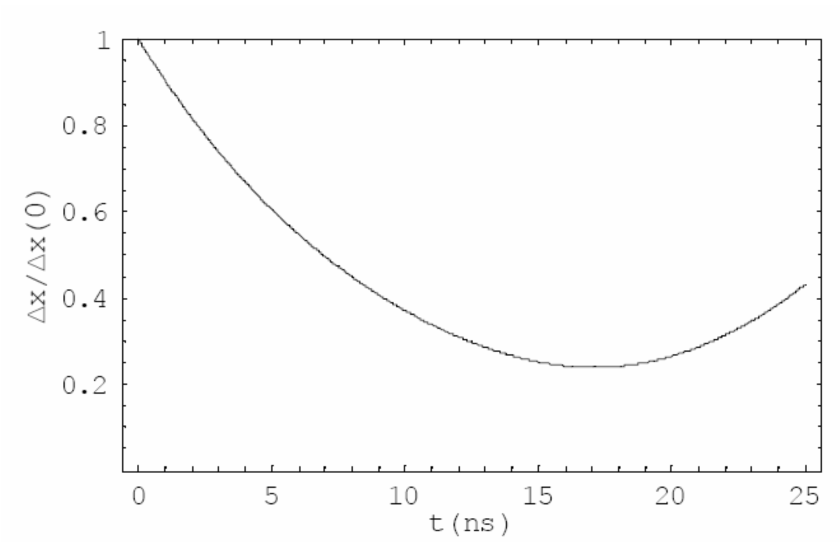
γ is the linewidth， ξ is the squeezing parameter

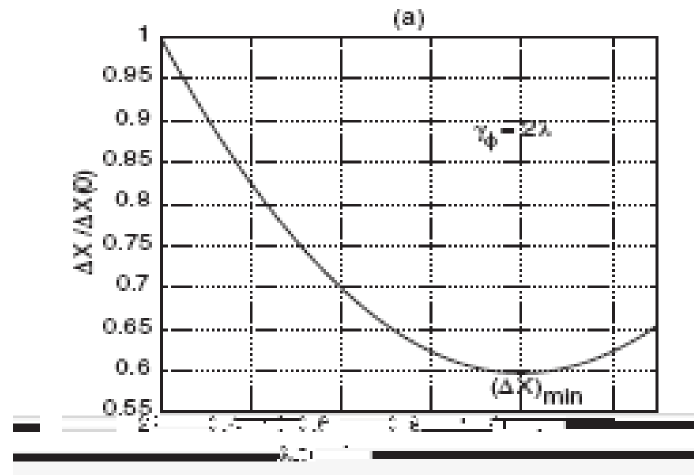
Choosing the following experimental parameters

$$E_J/2\pi = 4 \text{ GHz}, \, \Omega/2\pi = 10 \text{ GHz},$$
$$\omega_a/2\pi = 2\omega_b/2\pi = 3 \text{ GHz},$$
$$C_g/C_\Sigma = 0.1, \, B = 0.2 \text{ T}, \, W = 5 \ \mu\text{m},$$
$$V_0 = 2 \ \mu\text{V}, \, x_0 = 5 \times 10^{-13} \text{ m},$$
$$Q = 10^5, P = 8 \text{ W}, \tau = 0.1 \text{ ns}$$

nonlinear coupling constant $\kappa/2\pi \approx 4 \text{ Hz}$

Effective Rabi frequency $\Omega_p/2\pi \approx 16 \text{ MHz}$





$\Delta x / \Delta x(0)$ minimum ~ 24

XX ZHou et al PRL, 97, 267201(2006)

Motion detection of a micromechanical resonator embedded in a d.c. SQUID

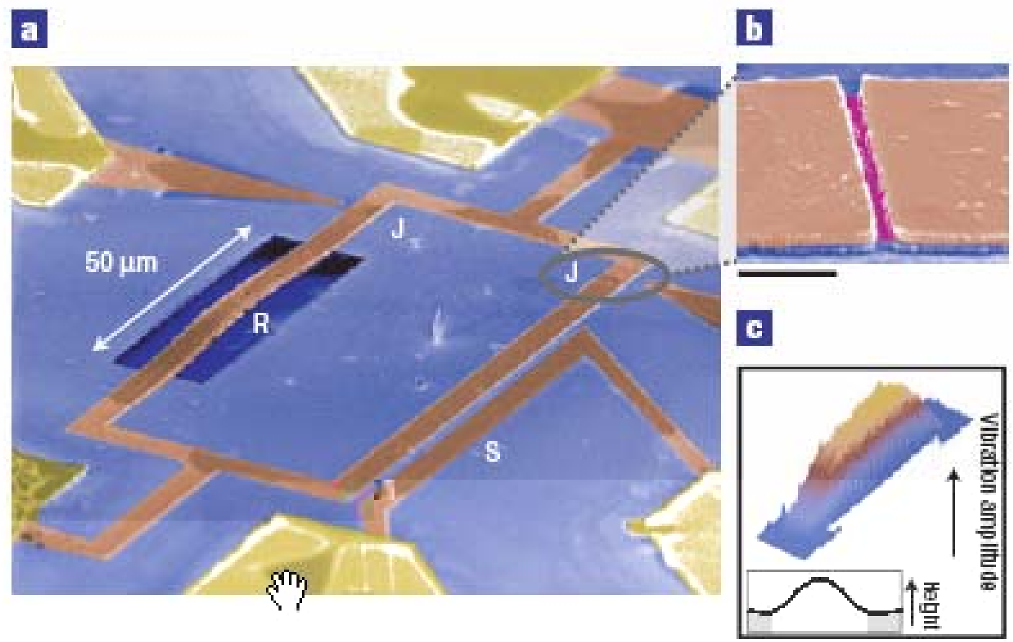
S. ETAKI[1,2]*, M. POOT[1], I. MAHBOOB[2], K. ONOMITSU[2], H. YAMAGUCHI[2] AND H. S. J. VAN DER ZANT[1]*

[1]Kavli Institute of Nanoscience, Delft University of Technology, Post Office Box 5046, 2600 GA Delft, Netherlands

[2]NTT Basic Research Laboratories, NTT Corporation, Atsugi-shi, Kanagawa 243-0198, Japan

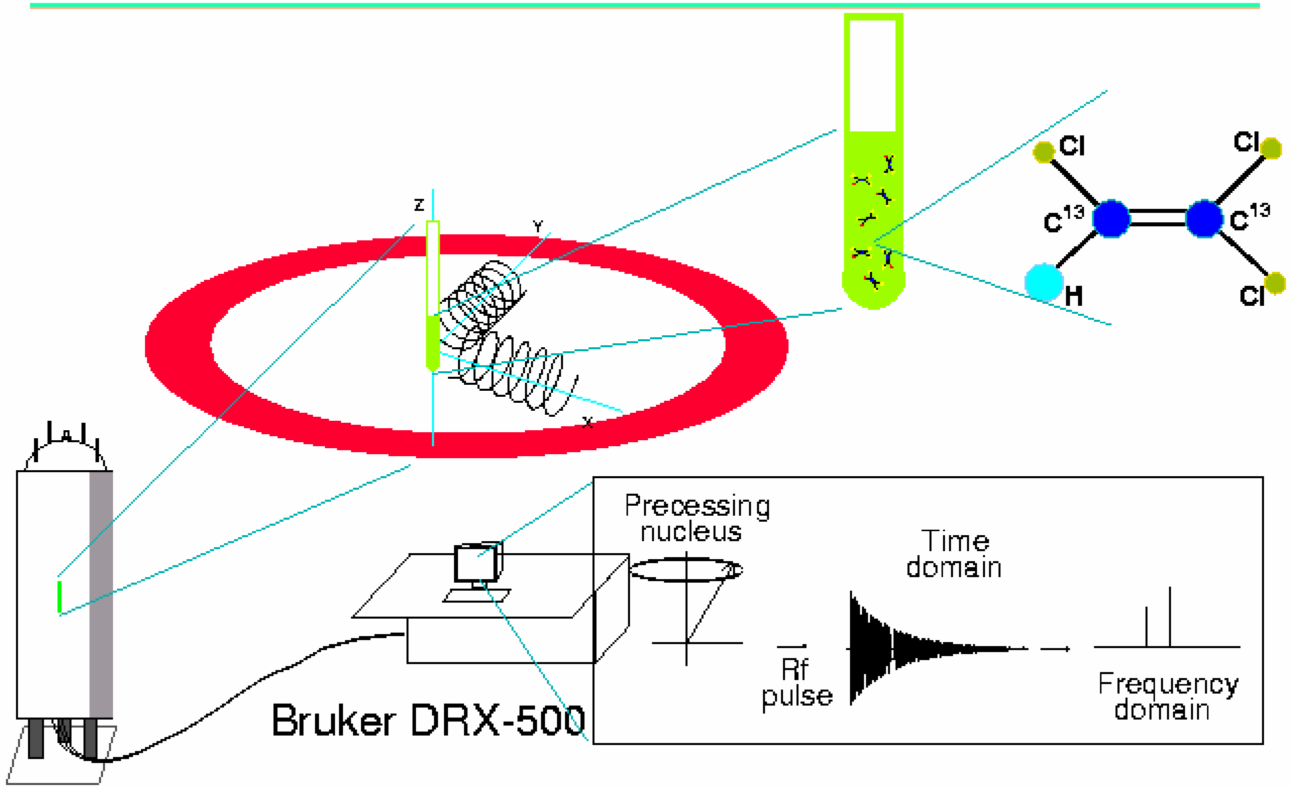
*e-mail: [illegible]

36



---NMR

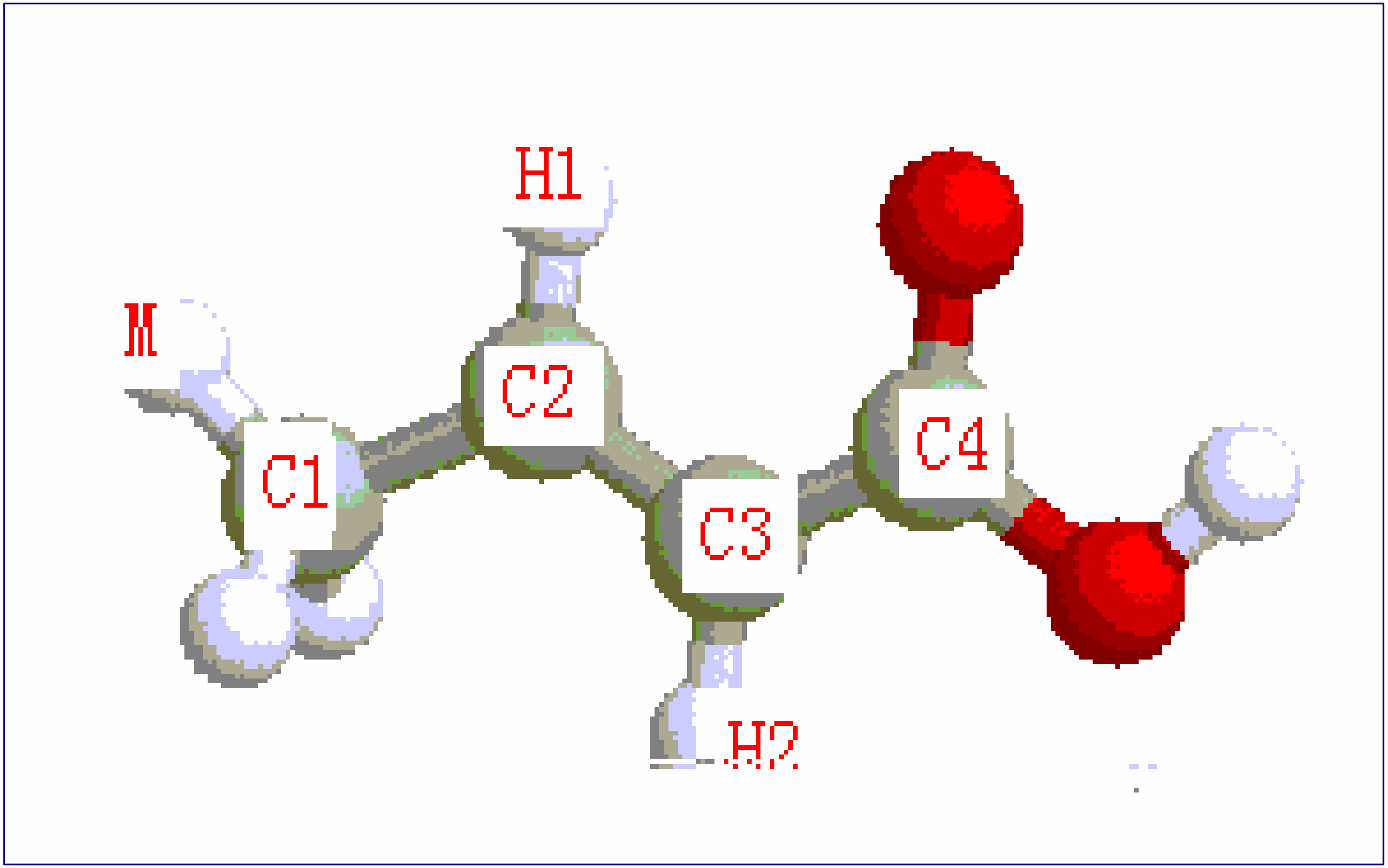
NMR System Overview



Further Reading: Abragam[1], Ernst[8]

Experimental realization in a 7 qubit NMR QC

(G.L. Long and L. Xiao, J Chem Phys 2003)



^{13}C labeled crotonic acid. 7 qubits system.

An algorithmic benchmark for quantum information processing

E. Knill*, R. Laflamme*, R. Martinez* & C.-H. Tseng†

* *Los Alamos National Laboratory, MS B265, Los Alamos, New Mexico 8*
USA
† *Department of Nuclear Engineering, MIT, Cambridge, Massachusetts 0*

Nature,404,368(2000)

NMR experimental realization of seventh-order coupling transformations and the seven-qubit modified Deutsch-Joz algorithm

Daxiu Wei, Jun Luo, Xiaodong Yang, Xianping Sun, Xizhi Zeng, Maili Liu, Shangwu Ding, and Mingsheng Zhan

Quant-ph/0301041, 2003

Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance

Lieven M. K. Vandersypen*†, Matthias Steffen*†, Gregory Breyta*, Costantino S. Yannoni*, Mark H. Sherwood* & Isaac L. Chuang*†

* *IBM Almaden Research Center, San Jose, California 95120, USA*
† *Solid State and Photonics Laboratory, Stanford University, Stanford, California 94305-4075, USA*

Nature,414,883(2001)

, 100084

gllong@tsinghua.edu.cn

2008 11 13

:

: 11

1918

6 3 6 1

1979	Wiesner	
1984	Bennett, Brassard	BB84
1992	Bennett	B92
1991	Ekert	EPR

M G_k C

K

$$G_K(M) = C$$

$$G_K^{-1}(C) = M$$

-
-
- Shor 1995
  RSA

Vernam

-
- 0,1
-
-

Example of (Quantum) Cryptography

- **Alice** and **Bob** generate shared key material (random numbers) using single [illegible]

[illegible]

Sample of key material

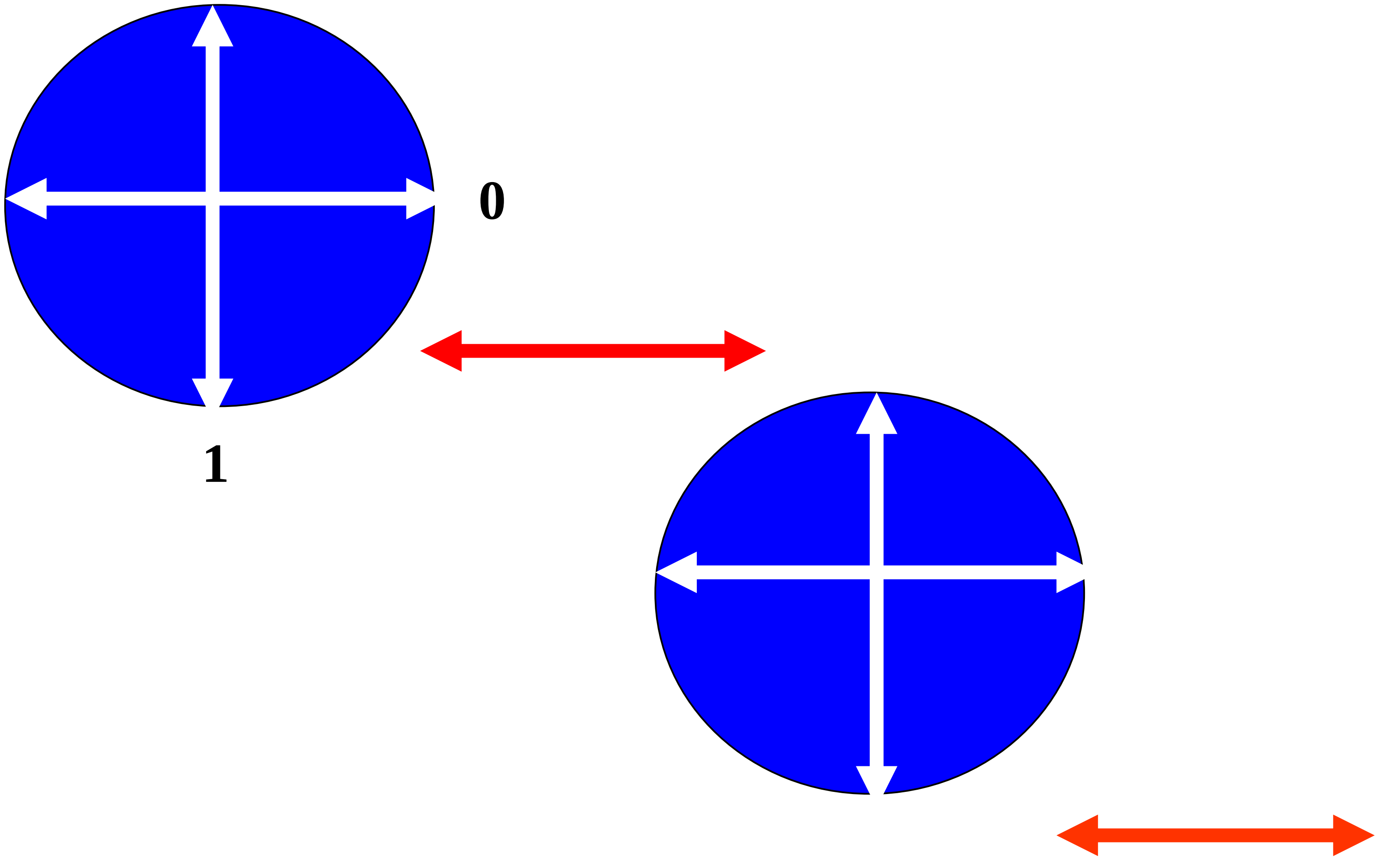
B	00001010	01111111	01010111	01011010	00010011
A	00001010	01111111	01010111	01011010	00010001
B	00000011	11100111	11011111	00000100	00001100
A	00000011	11100111	11011111	00000100	00001100

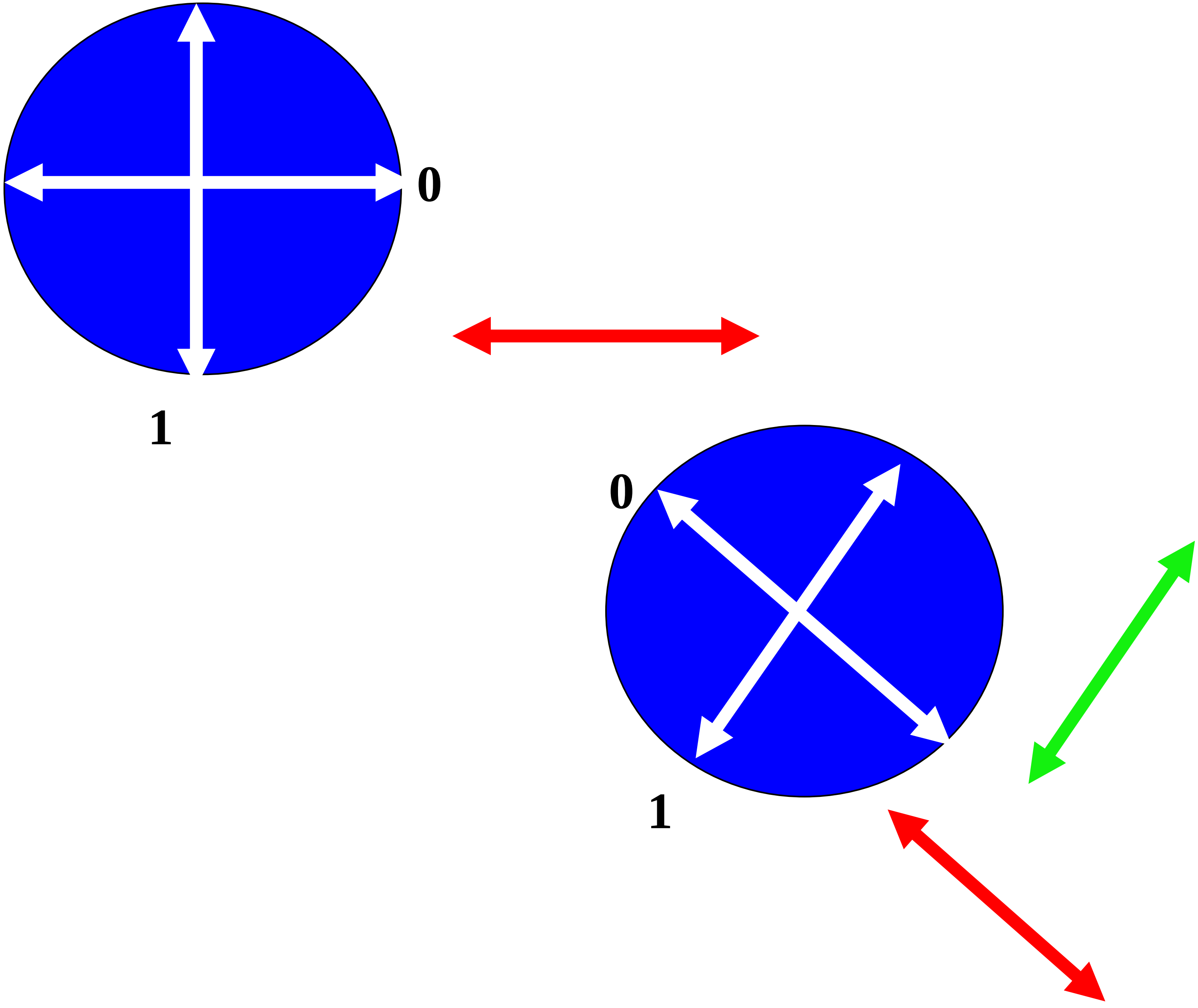
[illegible]

1.

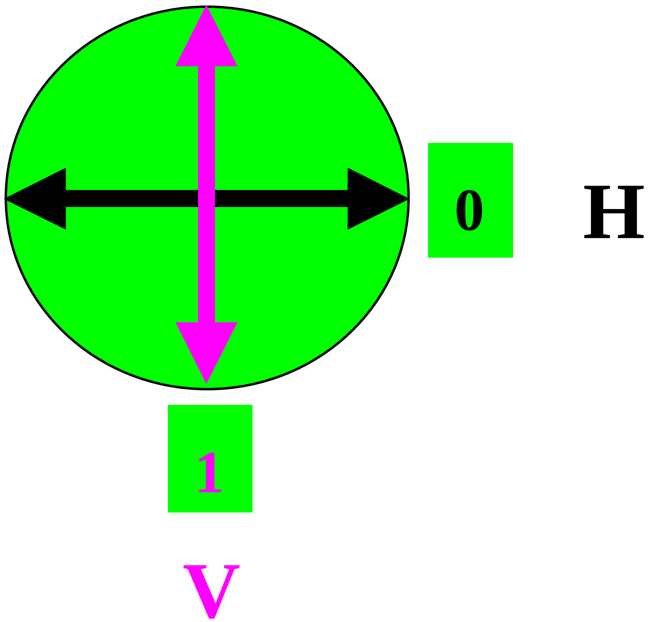
2.

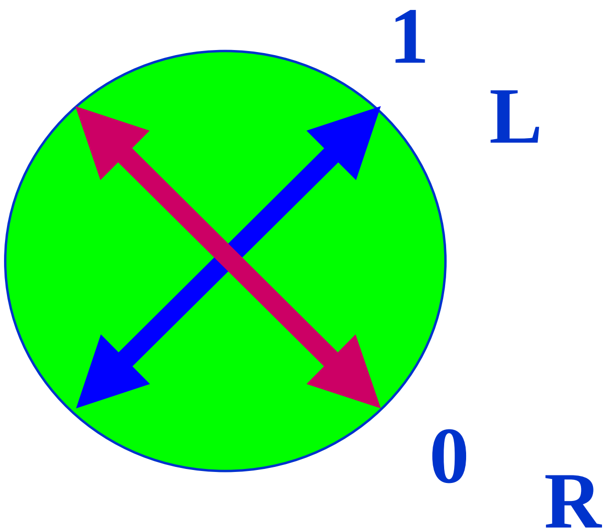
3.


0
1


0
1
0
1

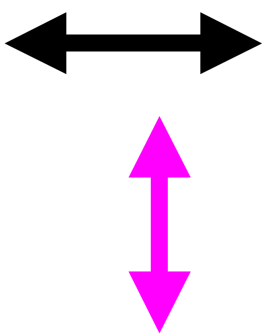
Bennett-Brassard 1984 protocol (BB84)





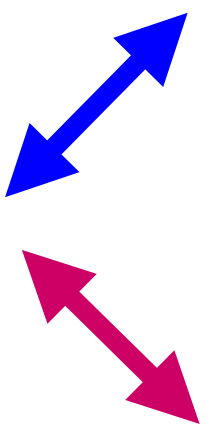
$$|H\rangle = |0\rangle$$

$$|V\rangle = |1\rangle$$



$$|L\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|R\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$



BB84 protocol without Eve present

Alice	⊕	⊗	⊗	⊗	⊕	⊗	⊕	⊗	⊕	⊗
	↓	↖	↖	↗	↓	↖	→	↗	→	↗
	1	0	0	1	1	0	0	1	0	1

Bob	⊗	⊗	⊕	⊗	⊕	⊗	⊕	⊕	⊕	⊕
	1	0	1	1	1	0	0	0	0	0

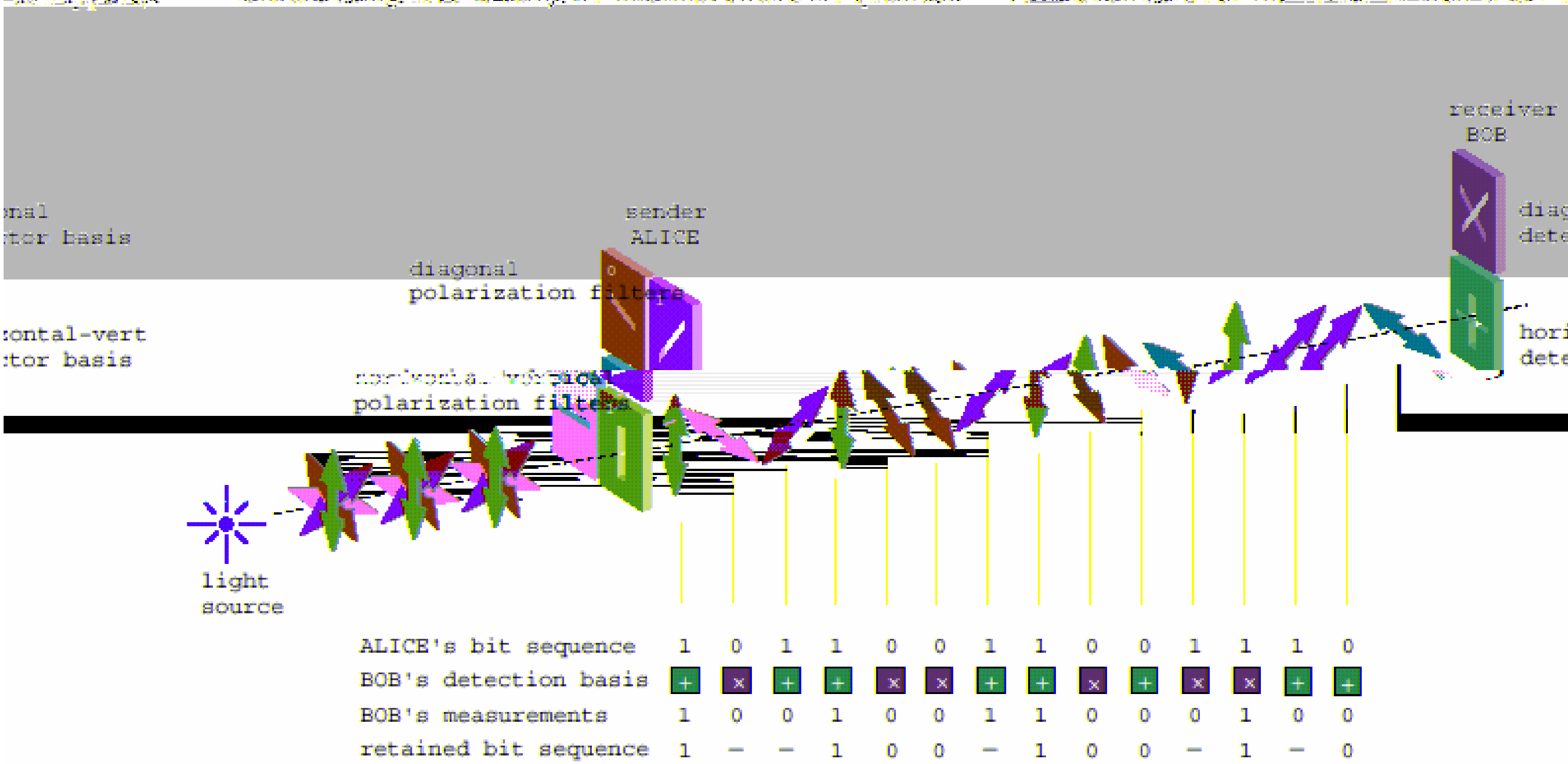
Raw Key		0		1	1	0	0		0	

BB84 Protocol With Eve Present

Alice								
	1	0	0	1	1	0	1	0

Eve								
	1	0	1	0	1	1	0	0

channel and a classical public channel. Normally single pho- of their key by an eavesdropper would be a reduction of the
tons are being used to carry the information and the quantum correlation between the values of their bits. Let us suppose

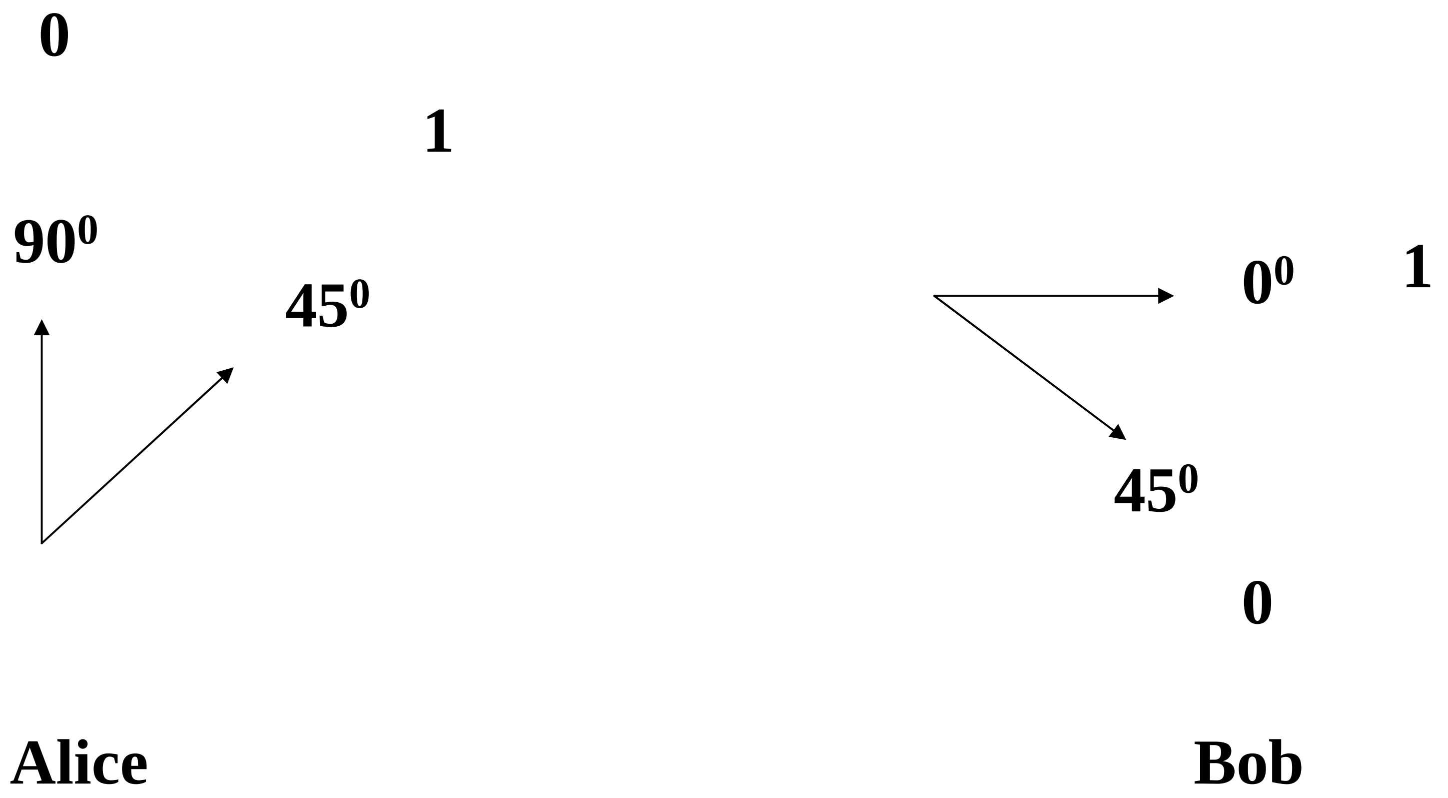


rtically, at
basis and

Fig. 1. The principle of QC according to the BB84 protocol. Alice sends down an optical fiber photons polarized randomly either horizontally, ve
$+45^\circ$, or at -45° (row 1), Bob randomly chooses one of his analyzer basis (row 2) and records his result (row 3). Then they compare the used
retain all results with compatible basis (row 4)

BB84

B92 protocol



C. H. Bennett, Phys. Rev. Lett. 68, 3121 (1992)

Hwang-Koh-Han 1998 protocol

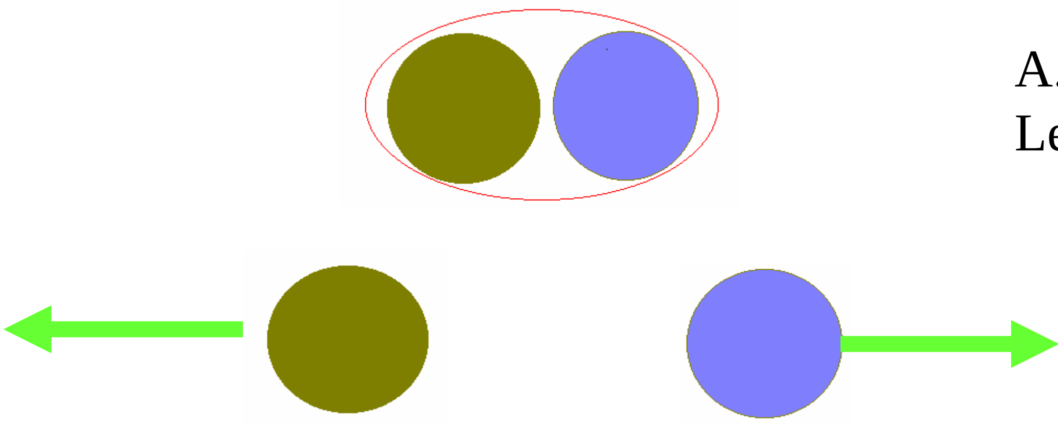
	$\overbrace{\hphantom{0 \cdots 1\ 0\ 1\ 1\ 0\ 0\ 1}}^{N_k}$	$\overbrace{\hphantom{0 \cdots 1\ 0\ 1\ 1\ 0\ 0\ 1}}^{N_k}$	
	$0 \cdots 1\ 0\ 1\ 1\ 0\ 0\ 1$	$0 \cdots 1\ 0\ 1\ 1\ 0\ 0\ 1$	$\cdots$
MB	$\otimes \cdots \oplus\ \otimes\ \oplus\ \oplus\ \otimes\ \otimes\ \oplus$	$\otimes \cdots \oplus\ \otimes\ \oplus\ \oplus\ \otimes\ \otimes\ \oplus$	$\cdots$
Alice	⤡ ··· ↔ ⤢ ↕ ↔ ⤢ ⤡ ↕	⤢ ··· ↔ ⤡ ↔ ↕ ⤡ ⤢ ↕	$\cdots$
Bob	⤡ ··· ↔ ⤢ ↕ ↔ ⤢ ⤡ ↕	⤢ ··· ↔ ⤡ ↔ ↕ ⤡ ⤢ ↕	$\cdots$

W.Y. Hwang, I.G. Koh and Y.D. Han,

Phys. Lett. A 244, 489 - 494 (1998)

Ekert 1991 protocol (Ekert 91)

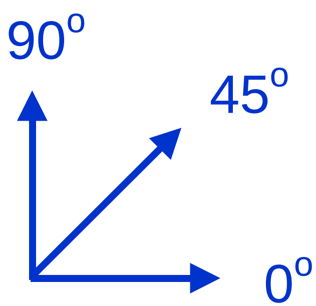
A.K. Ekert, Phys. Rev. Lett. 67, 661-663 (1991)

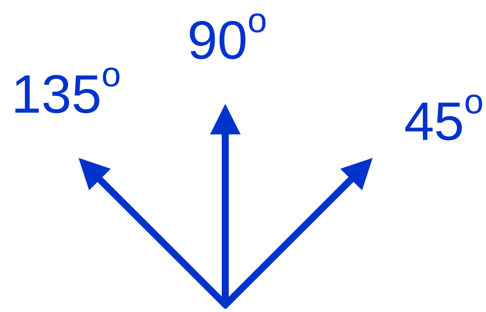


$$|\Phi^-\rangle_{AB} = \left(|\uparrow_A \downarrow_B\rangle - |\downarrow_A \uparrow_B\rangle\right)$$

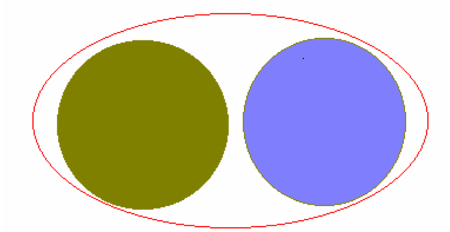
Alice

Bob





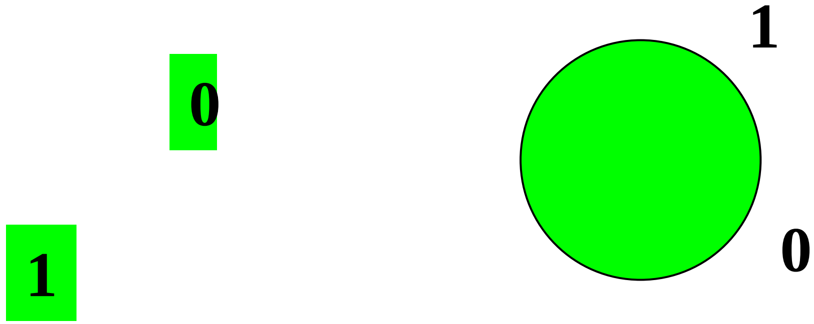
Bennett-Brassard-Mermin 1992 protocol (BBM92)



Alice

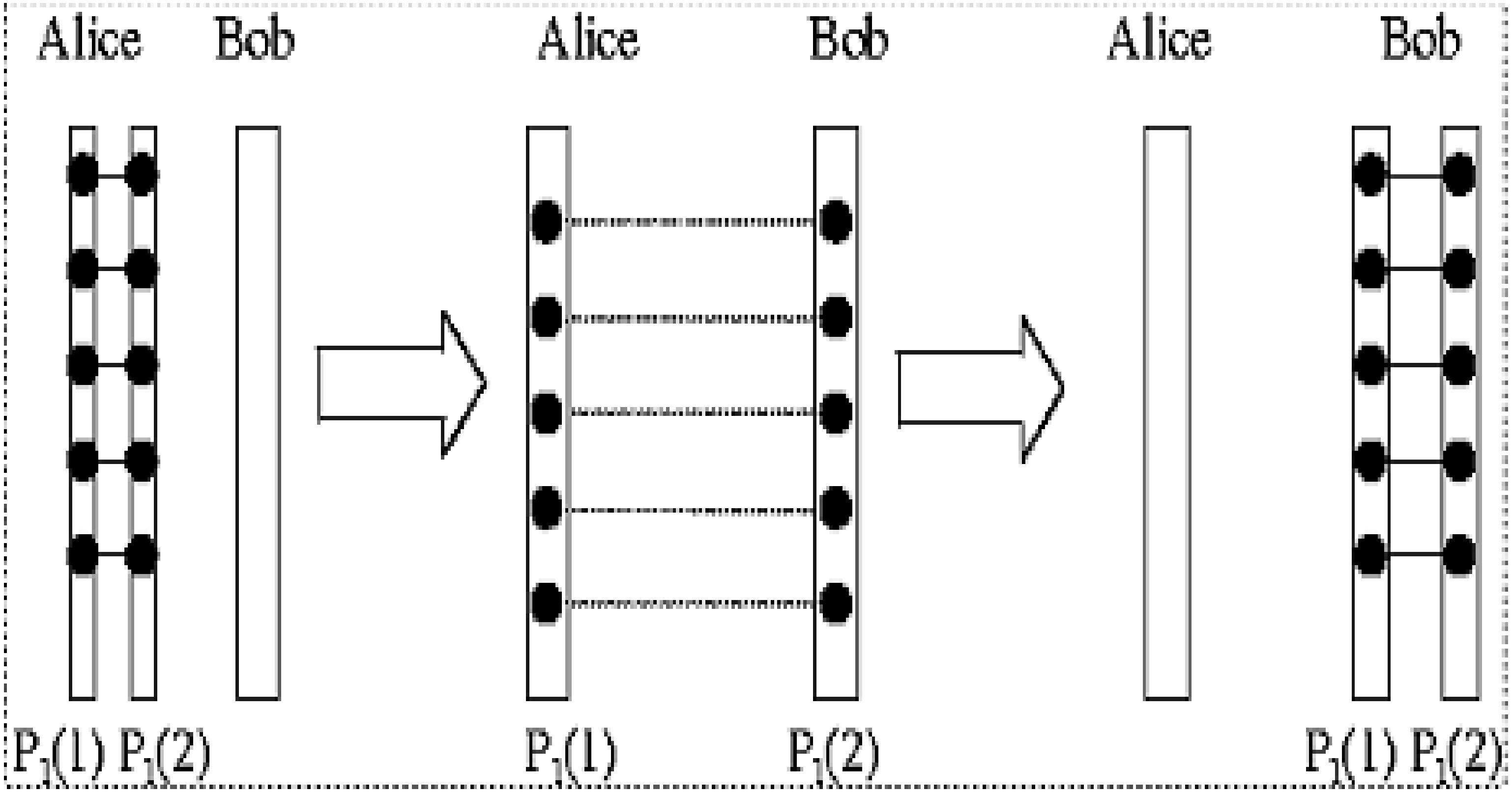
Bob

$$|\Phi^-\rangle_{AB} = \left(|\uparrow_A\downarrow_B\rangle - |\downarrow_A\uparrow_B\rangle\right)$$



Long-Liu 2002 protocol

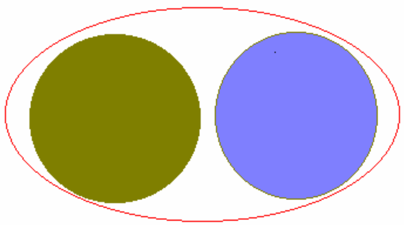
G L Long, X S Liu, Phys. Rev. A 65, 032302 (2002)



Deng-Long 2003 protocol (CORE)

Controlled Order Rearrangement Encryption for quantum key distribution

F G Deng and G L Long **Phys. Rev. A 68, 042315 (2003).**



EPR pair

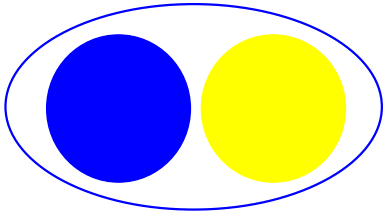
$$\left|\psi^{-}\right\rangle_{AB}=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_{A}\left|1\right\rangle_{B}-\left|1\right\rangle_{A}\left|0\right\rangle_{B}\right)$$

$$\left|\psi^{+}\right\rangle_{AB}=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_{A}\left|1\right\rangle_{B}+\left|1\right\rangle_{A}\left|0\right\rangle_{B}\right)$$

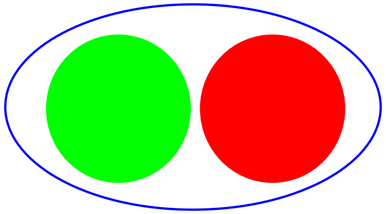
$$\left|\phi^{-}\right\rangle_{AB}=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_{A}\left|0\right\rangle_{B}-\left|1\right\rangle_{A}\left|1\right\rangle_{B}\right)$$

$$\left|\phi^{+}\right\rangle_{AB}=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_{A}\left|0\right\rangle_{B}+\left|1\right\rangle_{A}\left|1\right\rangle_{B}\right)$$

CORE c 1



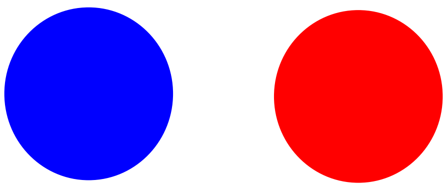
A_1 B_1



A_2 B_2

Pair A_1B_1

Pair A_2B_2

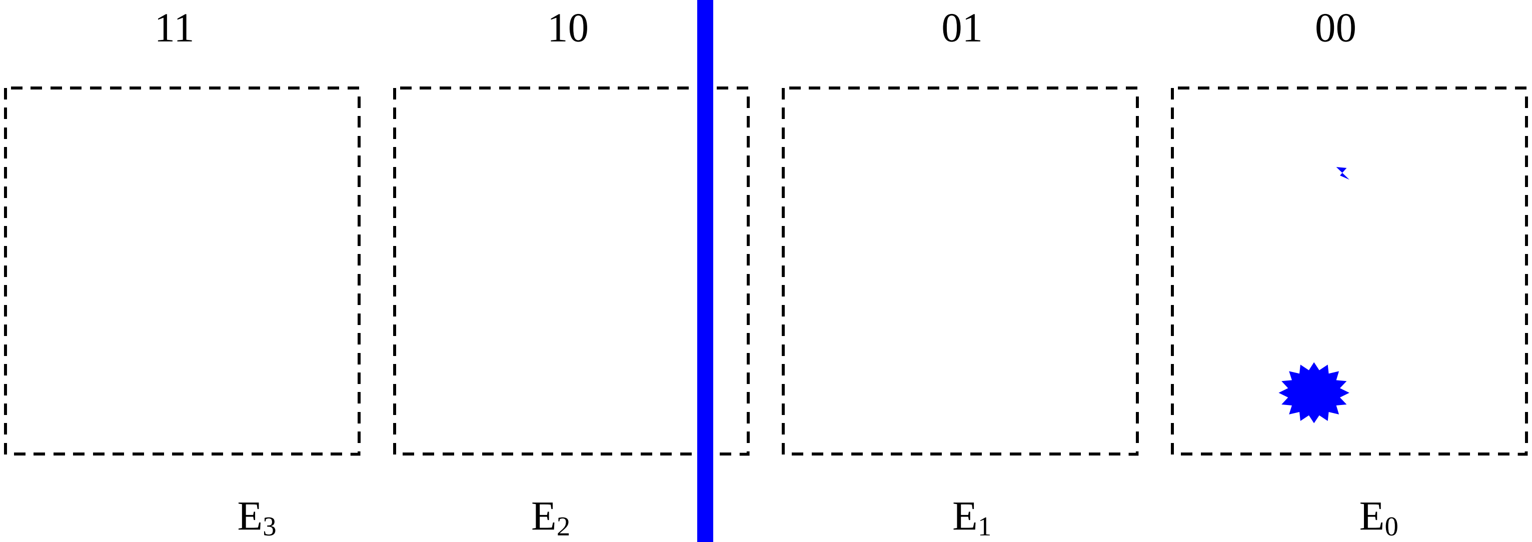


A_1 B_2

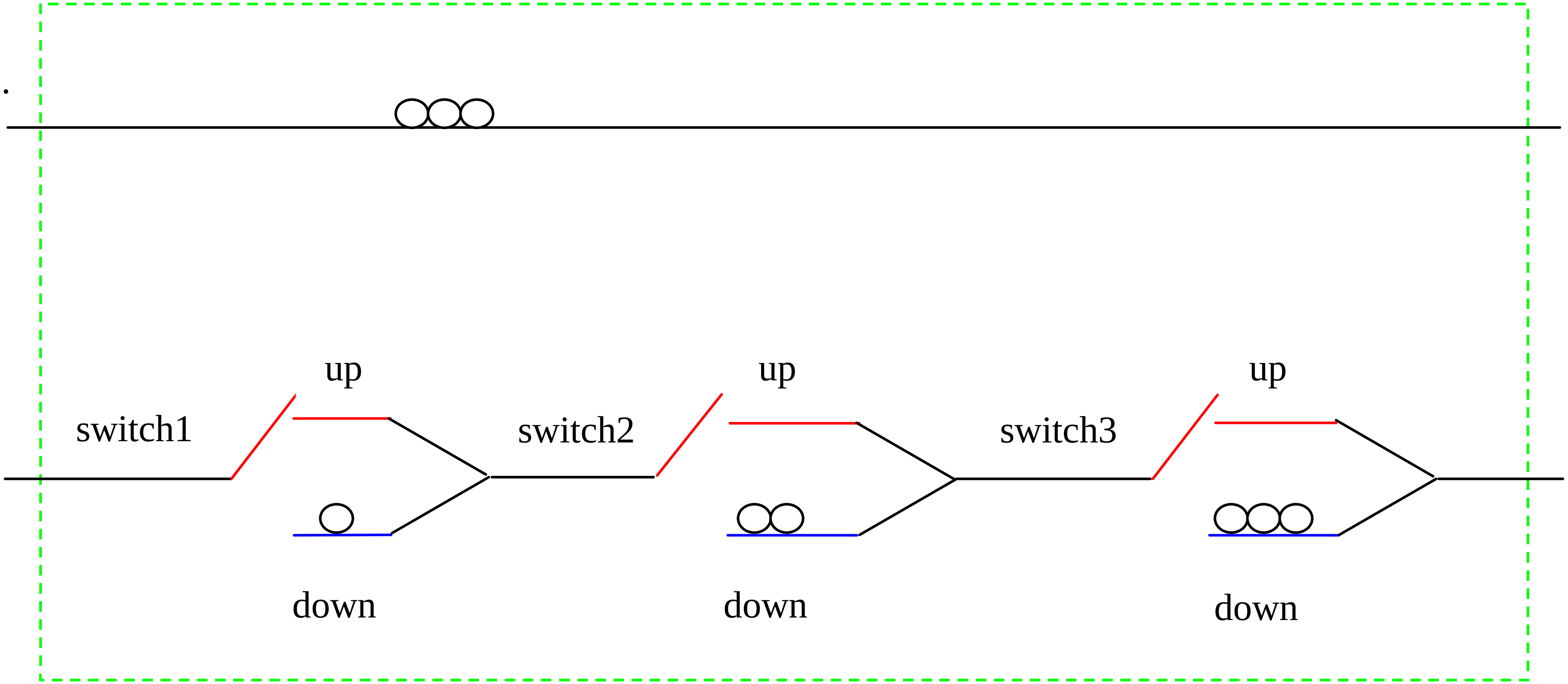
A_1 and B_2 from different pairs

$$\rho_{A_1B_2} = \overline{\rho}_{A_1} \otimes \overline{\rho}_{B_2} = \frac{1}{4}\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix}$$

CORE 3



CORE 4



Realization of CORE using optical delays

Quantum Secure Direct Communication

- Two requirements

- Alice and Bob can exchange secret information directly without first establishing a key and then send the information through a classical channel using the one-time-pad.

- The secret information can not be leaked even though Eve can intercept.

Quantum secure direct communication

Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block

F G Deng, G L Long and X S Liu **Phys. Rev. A 68, 042317 (2003).**

PHYSICAL REVIEW A **68**, 0423XX (2003)

Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block

Fu-Guo Deng,[1,2] Gui Lu Long,[1,2,3,4] and Xiao-Shu Liu[1,2]

[1]*Department of Physics, Tsinghua University, Beijing 100084, People's Republic of China*

[2]*Key Laboratory For Quantum Information and Measurements, Beijing 100084, People's Republic of China*

[3]*Center for Atomic and Molecular NanoSciences, Tsinghua University, Beijing 100084, People's Republic of China*

[4]*Institute of Theoretical Physics, Chinese Academy of Sciences, Beijing 100080, People's Republic of China*

(Received 18 June 2003)

A protocol for quantum secure direct communication using blocks of Einstein-Podolsky-Rosen (EPR) pairs is proposed. A set of ordered N EPR pairs is used as a data block for sending secret message directly. The ordered N EPR set is divided into two particle sequences, a checking sequence and a message-coding sequence. After transmitting the checking sequence, the two parties of communication check eavesdropping by measuring a fraction of particles randomly chosen, with random choice of two sets of measuring bases. After insuring the security of the quantum channel, the sender Alice encodes the se[cret] message directly on the message-coding sequence and sends them to Bob. By combining the checking a[n]d message-coding sequences together, Bob is able to read out the encoded message directly. The scheme is s[e]cure because an eavesdropper cannot get both sequences simultaneously. We also discuss issues in a noisy c[ha]nnel.

DOI: 10.1103/PhysRevA.68.0423XX PACS number(s): [illegible]

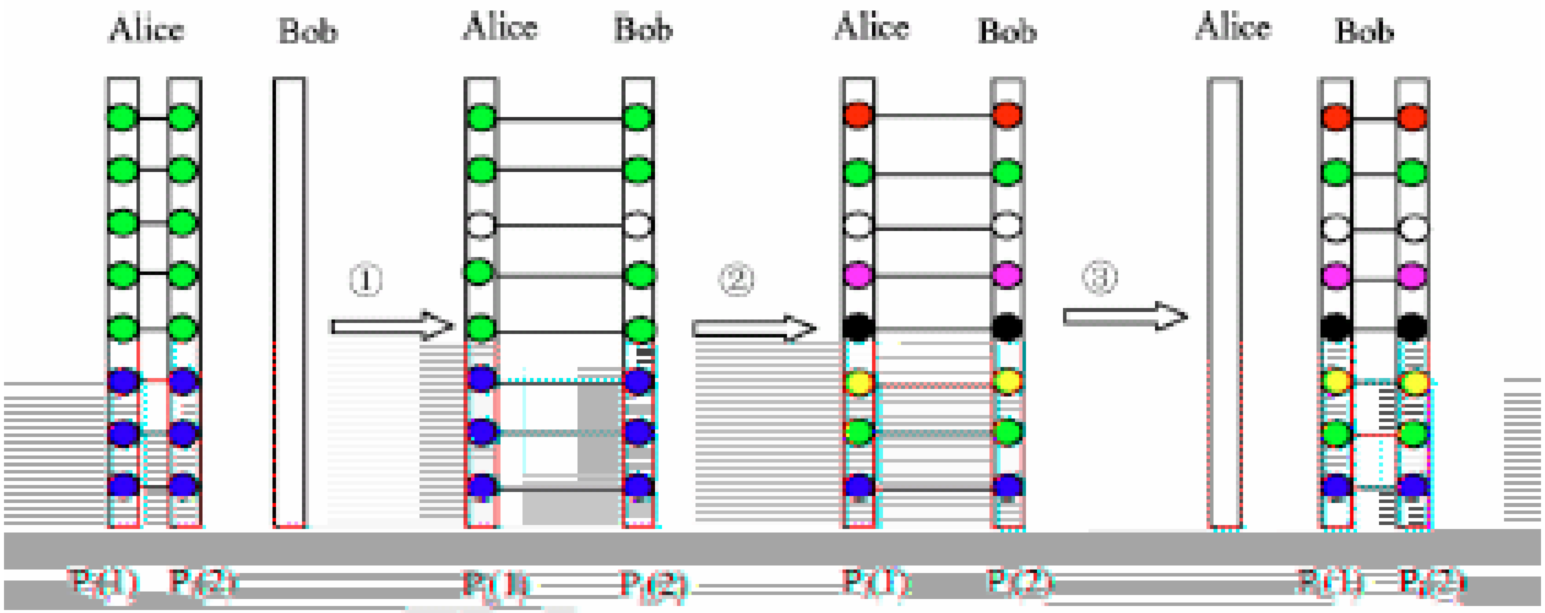


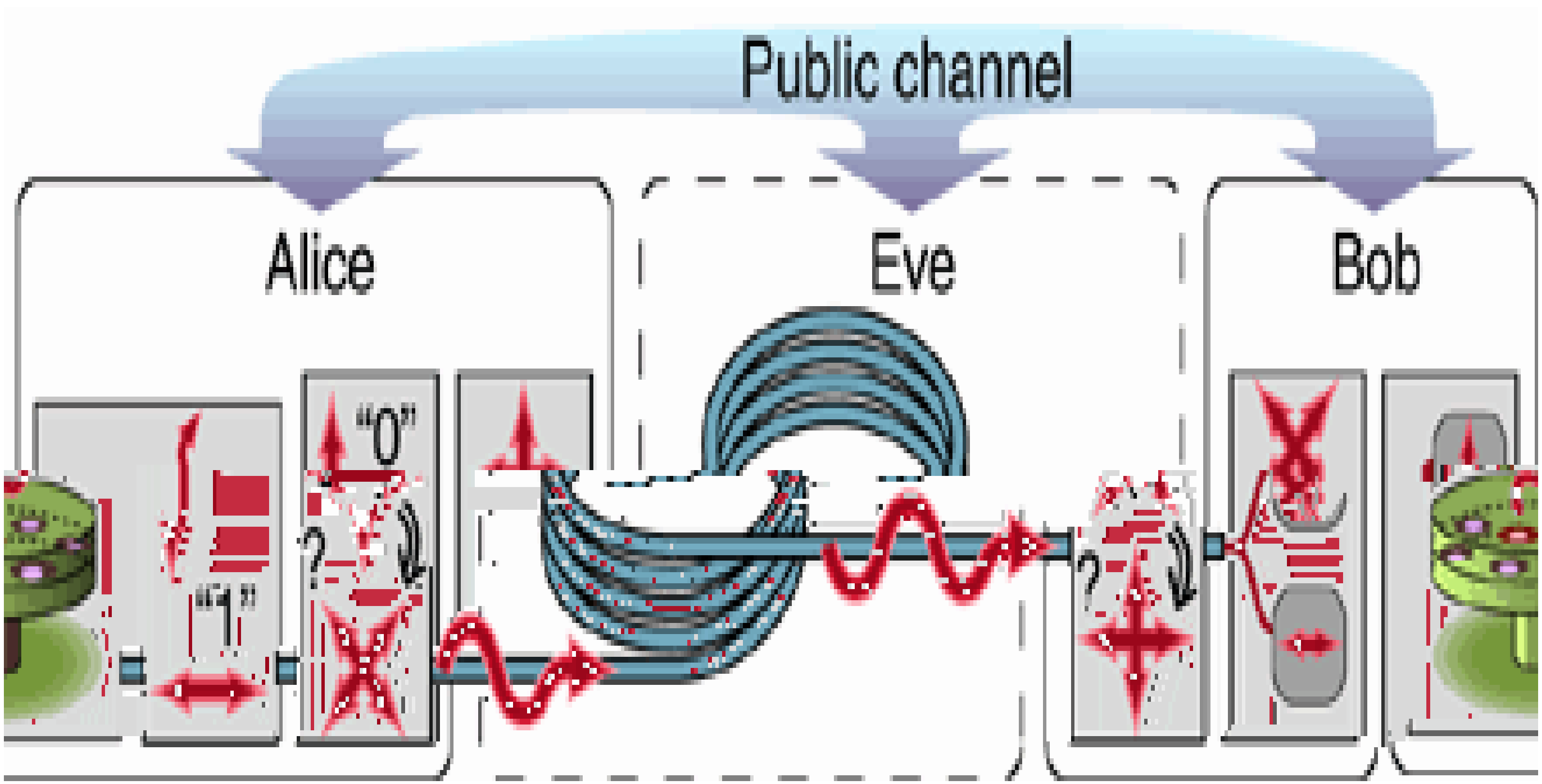
FIG. 1. Illustration of the QSDC protocol. Alice prepares the ordered N EPR pair in the same quantum states and divides them into two partner-particle sequences. She first sends one sequence to Bob for checking eavesdropping by choosing a fraction of particles to measure with randomly chosen measuring basis. If the quantum line is secure, Alice encodes the partner EPR pairs, using four unitary operations, the secret message and sends the encoded sequence to Bob.

:

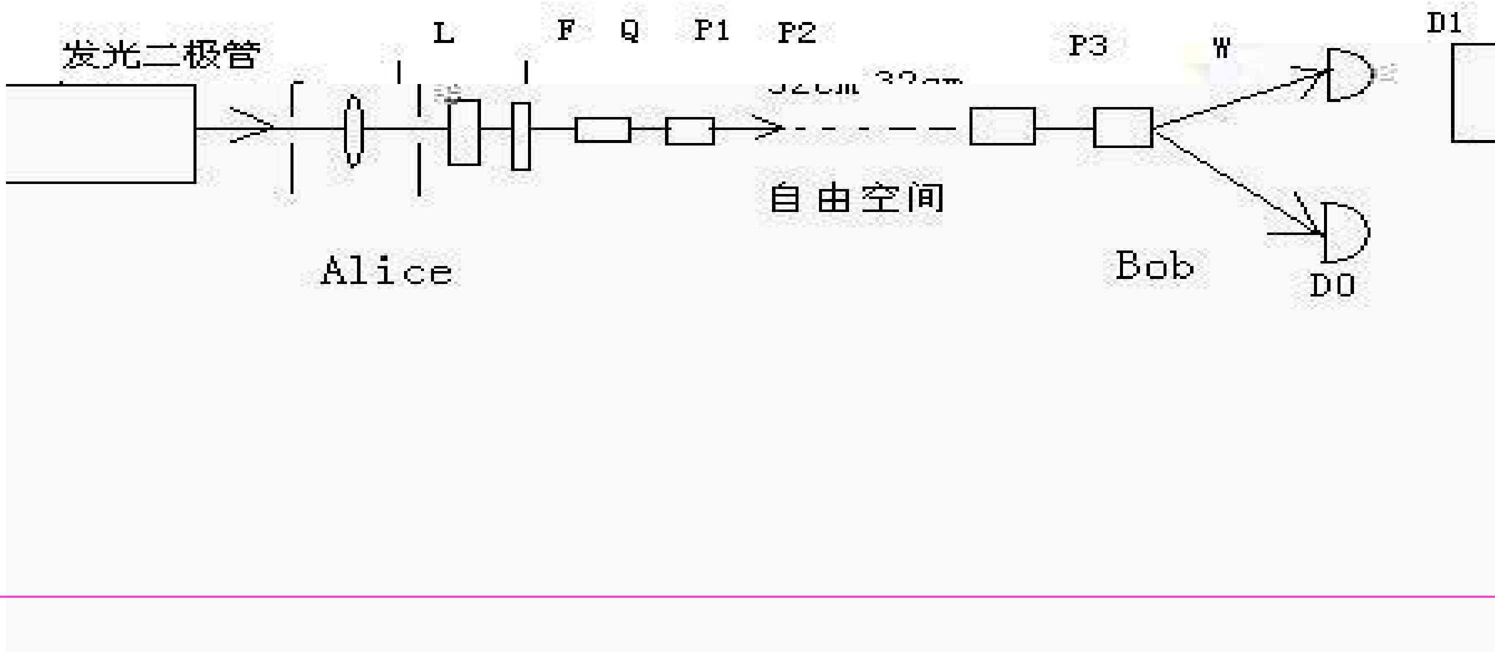
Efficient multiparty quantum-secret-sharing schemes, Li Xiao, Gui Lu Long, Fu-Guo Deng, and Jian-Wei Pan, PHYSICAL REVIEW A 69, 052307 (2004)

Secure direct communication with a quantum one-time pad, Fu-Guo Deng and Gui Lu Long, Physical Review A 69, 052319 (2004)

Bidirectional quantum key distribution protocol with practical faint laser pulses, F G Deng and G L Long, Phys. Rev. A70, 012311(2004)


Public channel
Alice
Eve
Bob
"0"
"1"
?
?

- 1989 Bennett Brassard



1) 1993

1.3micro-m 10km

2) 1995
10km(1.5%) 30km(4%)
700 260

3) 1993 1.1km
1.3 micro-m ,
0.54%

( )

4 1995, 23km
, 3.4
5) Johns Hopkins: 1995, 1km , 0.4% 1996, 200m
, 2 , 1k
6 LANL:
1995, 1.3 B92 , 205m ;
2000, 500m , 48km ;
2000, 1.6km
7) 5
70km

Daylight Quantum Key Distribution over 1.6 km

W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson
University of California, Los Alamos National Laboratory, Los Alamos, New Mexico 87545
(Received 14 January 2000)

Quantum key distribution (QKD) has been demonstrated over a point-to-point 1.6-km atmospheric [illegible] optical path [illegible] satellite and other long-distance applications.

PACS numbers: 03.67.Dd, 03.65.Bz, 42.50.Ar, 42.79.Sz

Quantum cryptography was introduced in the mid-1980s [1] as a new method for generating the shared, secret random number sequences, known as cryptographic keys, that are used in crypto-systems to provide communications security (for a review, see [2]). The appeal of quantum cryptography (or more accurately, quantum key distribution, QKD) is that its security is based on laws of nature and information-theoretically secure techniques, in contrast to existing methods of key distribution that derive their security from the perceived intractability of certain problems in number theory, or from the physical security of the distribution process.

Several groups have demonstrated QKD over multikilometer distances of optical fiber [3], but there are many key distribution problems for which QKD over line-of-sight atmospheric paths would be advantageous (for example, it is impractical to send a courier to a satellite). Free-space

bit in the sequence, Alice prepares and transmits a single photon to the recipient, "Bob," who measures each arriving photon and attempts to identify the bit value Alice has transmitted. Alice's photon state preparations and Bob's measurements are chosen from sets of nonorthogonal possibilities. For example, using the B92 protocol [11] Alice agrees with Bob (through public discussion) that she will transmit a **45°** polarized photon state $|45\rangle$, for each "0" in her sequence, and a vertical polarized photon state $|v\rangle$, for each "1" in her sequence. Bob agrees with Alice to randomly test the polarization of each arriving photon with **−45°** polarization, $|-45\rangle$, to reveal "1s," or horizontal polarization, $|h\rangle$, to reveal "0s." In this scheme Bob will never detect a photon for which he and Alice have used a preparation/measurement pair that corresponds to different bit values, such as $|h\rangle$ and $|v\rangle$, which happens for 50% of the bits in Alice's sequence. However, for the other

BS output ports is used to monitor the average photon number $\bar{n}$ of the dim pulses as follows: (1) a calibration photon-number measurement is made from the rate at which a calibrated single-photon counting module (SPCM) [20] fires at the transmitter's SM transmission-fiber output with a given input, (2) next the transmitter's SPD count rate is calibrated to the SPCM firing rate with the same input to determine the SPD efficiency, which is then (3) used with the experimental SPD count rates to measure the transmitted $\bar{n}$ in key generation mode.

(LST) under cloudless New Mexico skies. By 11:30 LST turbulence induced beam-spreading hindered our ability to efficiently acquire data at low bit-error rates (BER), ϵ (where BER, ϵ, is defined as the ratio of the number of bits received in error to the total number of bits received). The system efficiency, η_{sys}, which accounts for losses between the transmitter and MM fibers at the receiver, and the receiver's SPDs efficiencies had an average value of $\langle\eta_{sys}\rangle \sim 0.13$ with a standard deviation of $\sigma = 0.04$. Fluctuations in η_{sys} were caused by turbulence induced

am At the QKD receiver (Bob) light pulses are collected by a 8.9-cm diameter Cassegrain telescope and directed

beam spreading and beam wander; the typical bea

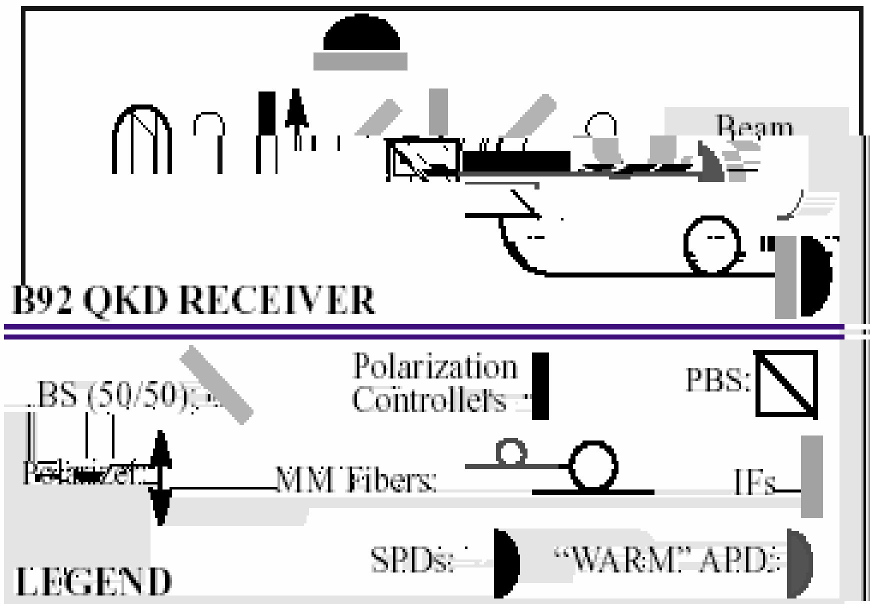


FIG. 2. Free-Space QKD Receiver (Bob): The legend describes the basic components; SPD MM-fibers are longer than the "warm" APD MM-fiber to delay the dim pulse 50 ns relative to the bright timing-pulse. See text for details.

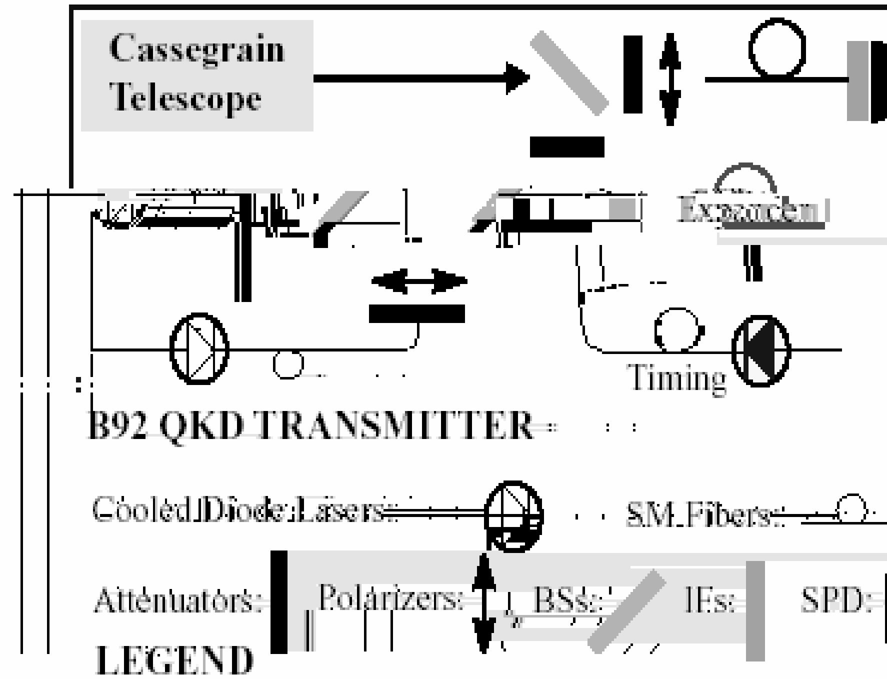
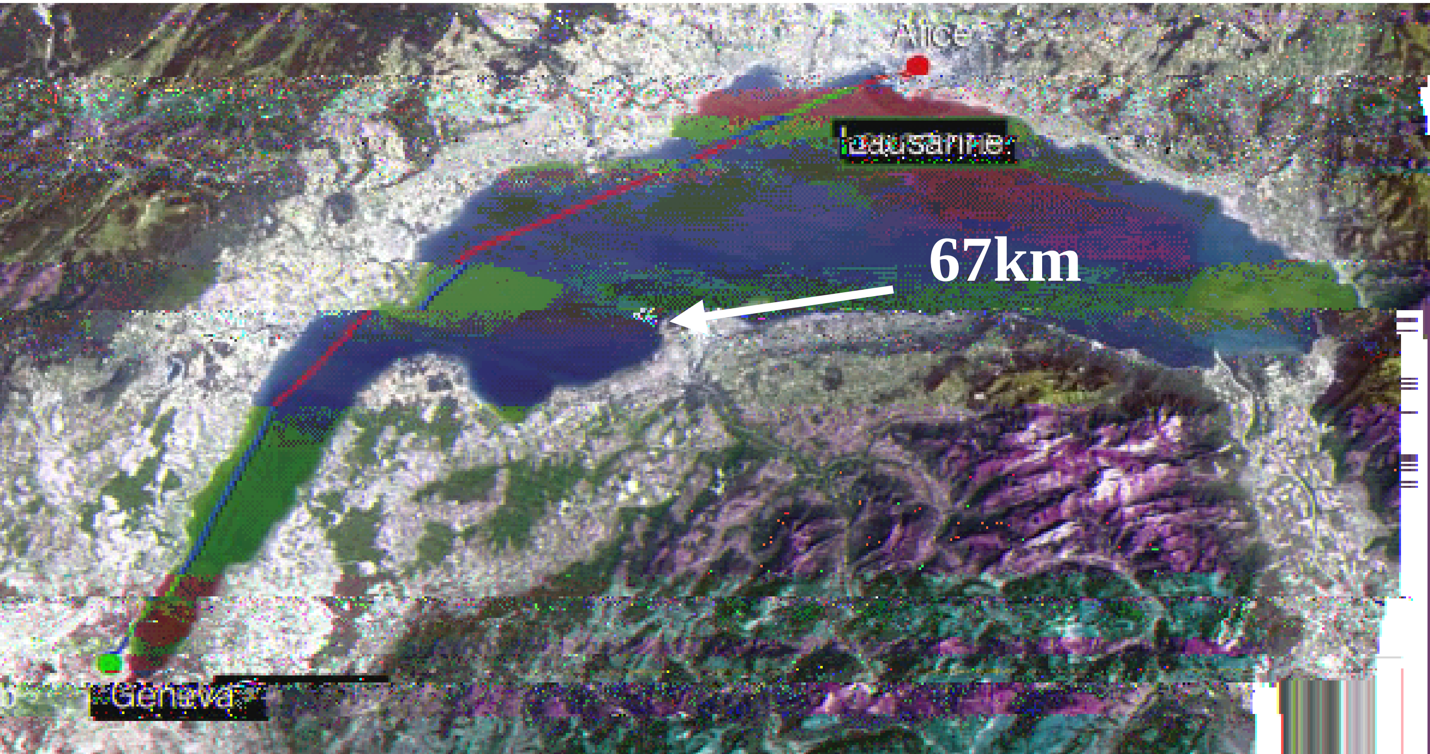


FIG. 1. Free-Space QKD Transmitter (Alice): The legend describes the basic components; cooled data lasers (or ... pulsed 5 ns prior to the timing laser. See text for details

Light work: keys encoded using polarized photons have been sent between Alice and Bob (left) through 67 km of fibre-optic cable under Lake Geneva.

S. RIBORDY/UNIV.



:

Shor

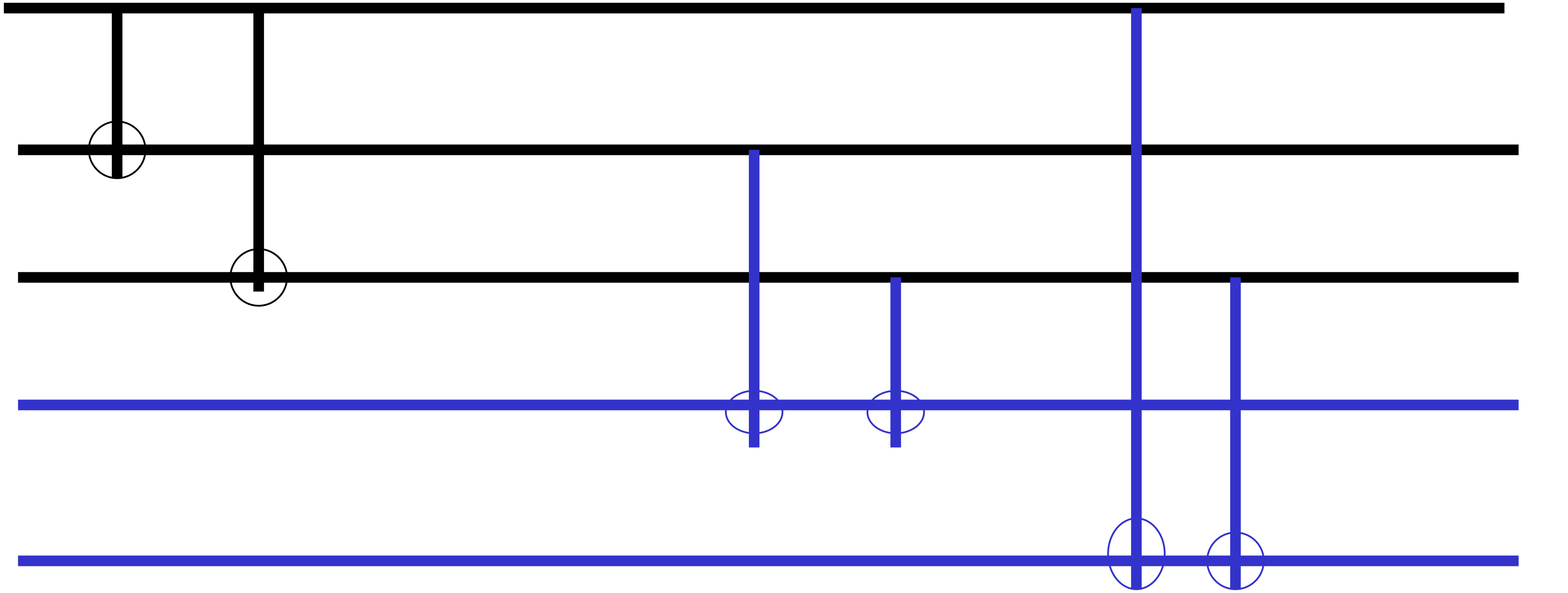
$$(a|000\rangle + b|111\rangle)|00\rangle \to (a|000\rangle + b|111\rangle)|00\rangle$$

$$(a|001\rangle + b|110\rangle)|00\rangle \to (a|001\rangle + b|110\rangle)|01\rangle$$

$$(a|010\rangle + b|101\rangle)|00\rangle \to (a|010\rangle + b|101\rangle)|10\rangle$$

$$(a|100\rangle + b|011\rangle)|00\rangle \to (a|100\rangle + b|011\rangle)|11\rangle$$

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



$$(a\,|000\rangle + b\,|111\rangle)\,|00\rangle + \varepsilon(a\,|001\rangle + b\,|110\rangle)\,|00\rangle$$
$$\Downarrow$$
$$(a\,|000\rangle + b\,|111\rangle)\,|00\rangle + \varepsilon(a\,|001\rangle + b\,|110\rangle)\,|01\rangle$$

For small error, with large probability to obtain (0,0) and small probability to obtain (0,1)

1 Shor

2 Bennett, Preskill 10^{-6}

3 Knill: 2005.3.3 3%

10

<1%

Quantum Teleportation

- For a 2 qubit system there a 4 bell states
- The 4 states are orthogonal → They can be represented as a Unitry Transform.
- The Propery that make BELL STATES so remarkable is that

Teleportation

Of One qubit ➔ $|0\rangle$ Or $|1\rangle$

Entangled State

Superposition

$$|\psi\rangle_{123} = |\psi\rangle_1 \otimes |\psi^-\rangle_{23}$$

$$|\psi^-\rangle_{23} = \frac{1}{\sqrt{2}}\left(|0\rangle_2 |1\rangle_3 - |1\rangle_2 |0\rangle_3\right)$$

Bell States

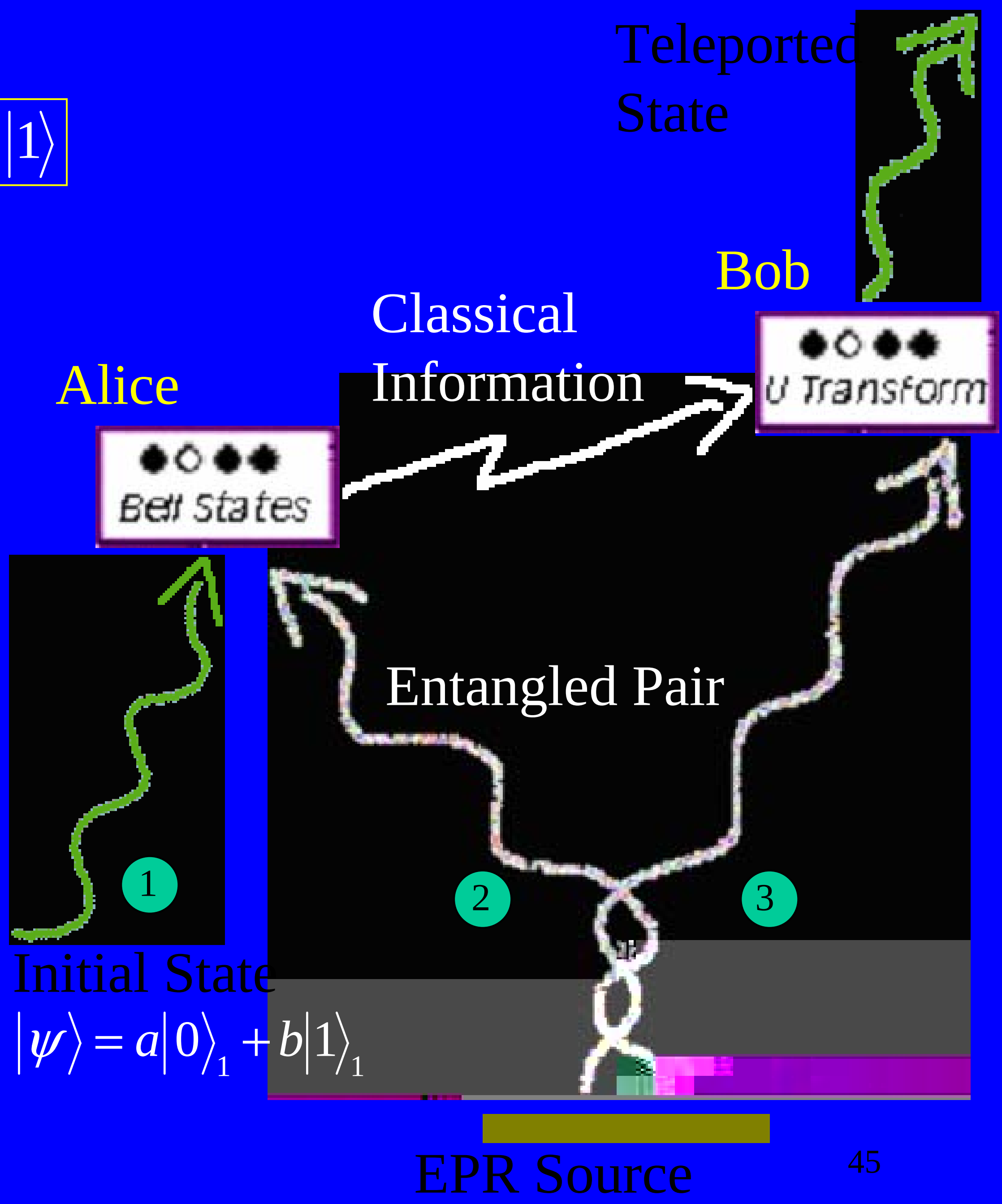
$$|\psi^+\rangle_{12} = \frac{1}{\sqrt{2}}\left(|0\rangle_1 |1\rangle_2 + |1\rangle_1 |0\rangle_2\right)$$

$$|\psi^-\rangle_{12} = \frac{1}{\sqrt{2}}\left(|0\rangle_1 |1\rangle_2 - |1\rangle_1 |0\rangle_2\right)$$

$$|\phi^+\rangle_{12} = \frac{1}{\sqrt{2}}\left(|0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2\right)$$

$$|\phi^-\rangle_{12} = \frac{1}{\sqrt{2}}\left(|0\rangle_1 |0\rangle_2 - |1\rangle_1 |1\rangle_2\right)$$

$$\frac{1}{2}\Big[\,|\psi^-\rangle_{12}\left(-a|0\rangle_3 - b|1\rangle_3\right) + |\psi^+\rangle_{12}\left(-a|0\rangle_3 + b|1\rangle_3\right) + |\phi^-\rangle_{12}\left(a|1\rangle_3 + b|0\rangle_3\right) + |\phi^+\rangle_{12}\left(a|1\rangle_3 - b|0\rangle_3\right)\Big]$$



Superdense Coding

Super Dense Coding

- Alice & Bob have the long distance feeling
- Goal: to transmit some CLASSICAL information from Alice to Bob.
- Alice is in possession of two classical bits of information which she wishes to send to Bob but can only send one qubit to Bob.
- Can she achieve her goal?

Super Dense Coding

- Super Dense Coding says YES!

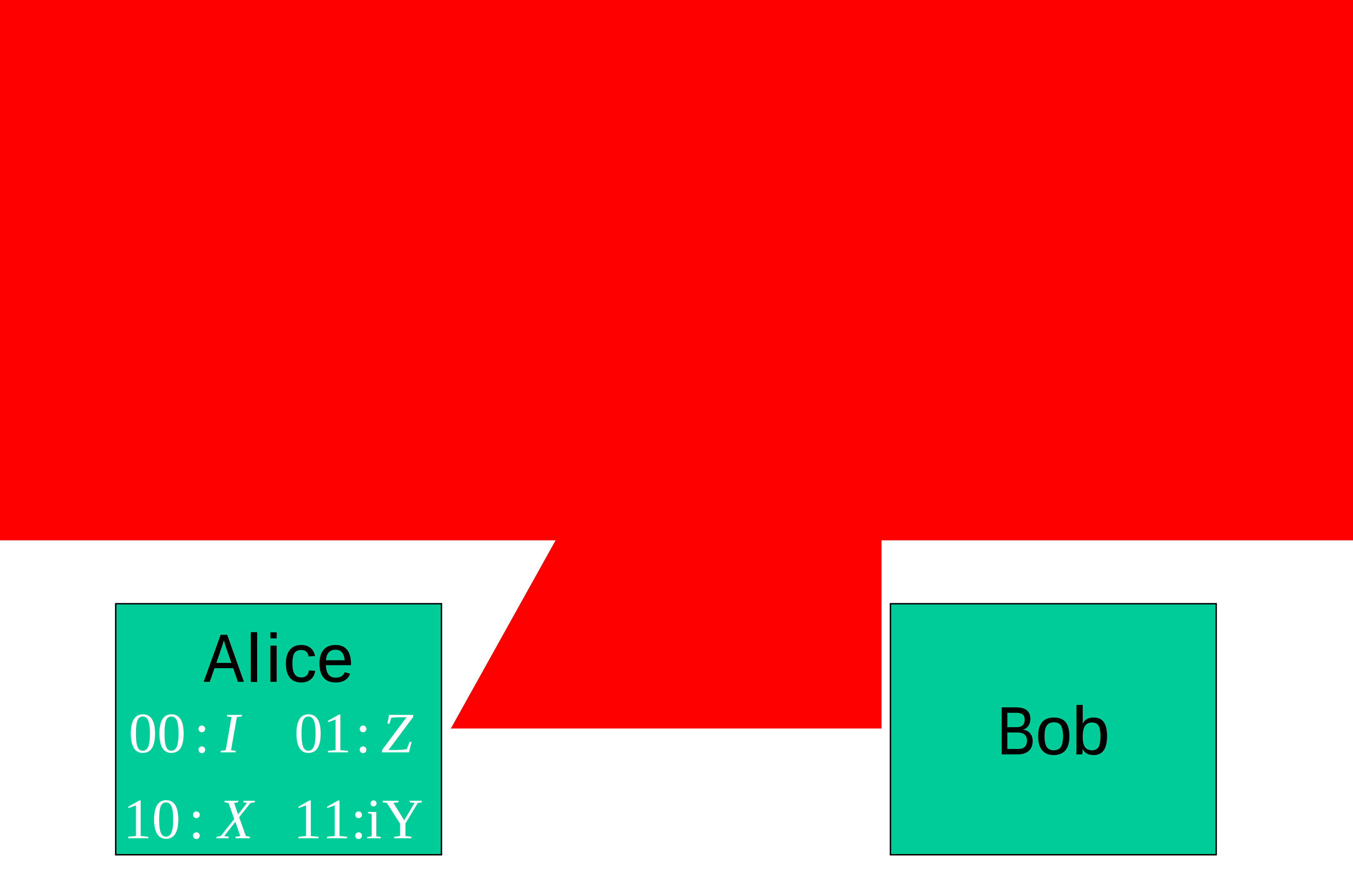
  - They both initially share a pair of qubits in the entangled state.

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

  - Alice initially has the first qubit and Bob has the second qubit.

  - Note the qubit is prepared ahead of time by a third party who then sends one to Alice and one to Bob

  - By sending a single qubit to Bob, Alice can communicate two bits of classical information


Alice
00 : I
01 : Z
10 : X
11:iY
Bob

Super Dense Coding

- Procedure:
  - If Alice wants to send…

00	She does nothing
01	She applies the phase flip Z to her qubit
10	She applies quantum NOT gate X
11	She applies the iY gate

- Then Bob applies an appropriate measurement operator

Super Dense Coding

- Four Resulting States

$$00: |\psi\rangle \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$01: |\psi\rangle \rightarrow \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$10: |\psi\rangle \rightarrow \frac{|10\rangle + |01\rangle}{\sqrt{2}}$$

$$11: |\psi\rangle \rightarrow \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Bell States

Super Dense Coding

- Notice that the Bell States…

Form an orthonormal basis

eg:

$$\frac{\langle 00| + \langle 11|}{\sqrt{2}} \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$= \frac{1}{2}\left(\langle 00|00\rangle + \langle 00|11\rangle + \langle 11|00\rangle + \langle 11|11\rangle\right)$$

$$= \frac{1}{2}(2) = 1$$

…therefore can be distinguished by an appropriate quantum measurement. Example:

$$P_{ij} = |b_{ij}\rangle\langle b_{ij}|$$

PHYSICAL REVIEW A, VOLUME 65, 022304

General scheme for superdense coding between multiparties

X. S. Liu,[1,2] G. L. Long,[1,2,3,4,5] D. M. Tong,[2] and Feng Li[6]
[1]Department of Physics, Tsinghua University, Beijing 100084, China
[2]Department of Physics, Shandong Normal University, Jinan 250014, China
[3]Key Laboratory for Quantum Information and Measurement, Beijing 100084, China
[4]Institute of Theoretical Physics, Chinese Academy of Sciences, Beijing 100080, People's Republic of China
[5]Center for Atomic, Molecular and NanoSciences, Tsinghua University, Beijing 100084, People's Republic of China
[6]Basic Education Section, Captial University of Economics and Business, Beijing 100026, People's Republic of China

(Received 25 July 2001; published 4 January 2002)

Dense coding or superdense coding in the case of high-dimension quantum sta tes between two parties and multiparties is studied in this paper. ... single-body unitary operations corresponding to the basis chosen, and the r ules for selecting the one-body unitary operations in a multiparty case.

DOI: 10.1103/PhysRevA.65.022304 PACS number(s): 03.67.−a, 89.70.+c

Quantum dense coding or superdense coding [1] is one of the important branches of quantum-information theory. It has been widely studied both in theory and in experiment [1,2]. ... mechanics allows one to encode information in the quan tum states that is denser than classical coding. Bell-basis sta tes

$$|\Psi^+\rangle=(|00\rangle+|11\rangle)/\sqrt{2},$$

$$|\Psi^-\rangle=(|00\rangle-|11\rangle)/\sqrt{2},$$

To present our scheme more clearly, let us first begin with dense coding between two parties in three dimensions. The general Bell basis of the Hilbert space of two particles with ...

$$|\Psi_{nm}\rangle=\sum_j e^{2\pi ijn/3}|j\rangle\otimes|j+m \bmod 3\rangle/\sqrt{3}, \qquad (2)$$

where $n,m,j=0,1,2$. Explicitly,

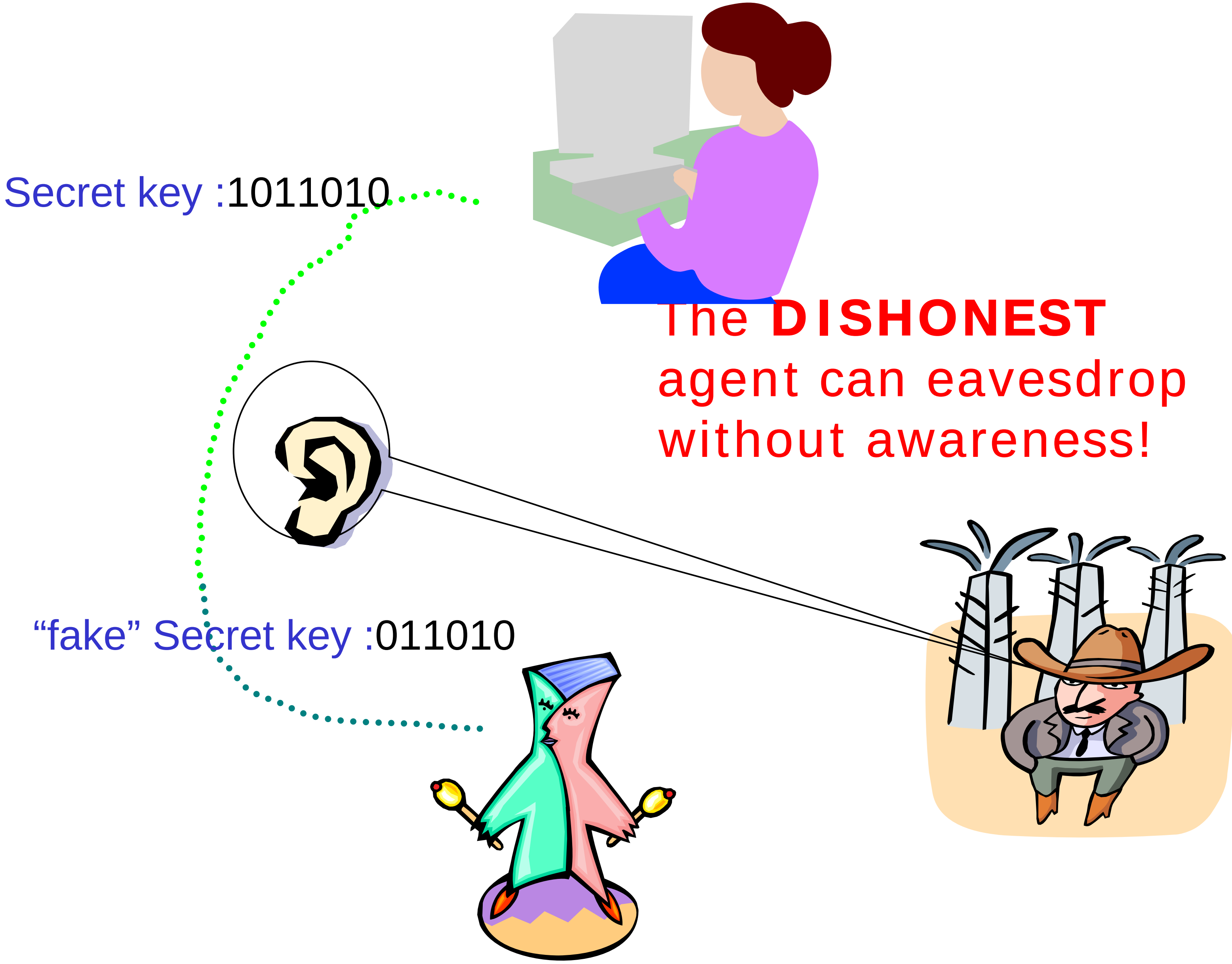
$$|\Psi_{00}\rangle=(|00\rangle+|11\rangle+|22\rangle)/\sqrt{3},$$

Quantum Secret Sharing

A

ge: K : 0101001

Secret key :1011010



Agent Bob Agent Charlie

Alice

x x x

Bob

	+x	-x	+y	-y
+x	+x	-x	-y	+y
-x	-x	+x	+y	-y
+y	-y	+y	-x	+x
-y	+y	-y	+x	-x

Entry : Charlie x

$$\pm x = \frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right) \qquad \pm y = \frac{1}{\sqrt{2}}\left(|0\rangle \pm i|1\rangle\right)$$

$$
\left|GHZ\right\rangle = \frac{1}{\sqrt{2}}\left(\left|000\right\rangle + \left|111\right\rangle\right)
$$

$$
= \underline{\frac{1}{\sqrt{2}}\left|+x\right\rangle \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right)} + \underline{\frac{1}{\sqrt{2}}\left|-x\right\rangle \frac{1}{\sqrt{2}}\left(\left|00\right\rangle - \left|11\right\rangle\right)}
$$

$$
= \underline{\frac{1}{\sqrt{2}}\left(\left|+y\right\rangle + \left|-y\right\rangle\right) \boxed{\frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right)}}
$$

$$
\underline{+ \frac{-i}{\sqrt{2}}\left(\left|+y\right\rangle - \left|-y\right\rangle\right) \frac{1}{\sqrt{2}}\left(\left|00\right\rangle - \left|11\right\rangle\right)}
$$

$$
\boxed{\begin{aligned} &\frac{1}{2}\Big[e^{\frac{-i\pi}{4}}\left(\left|+x\right\rangle\left|+y\right\rangle + \left|-x\right\rangle\left|-y\right\rangle\right) \\ &+ e^{\frac{i\pi}{4}}\left(\left|+x\right\rangle\left|-y\right\rangle + \left|-x\right\rangle\left|+y\right\rangle\right)\Big] \end{aligned}}
$$

Bob	Alice: +y
+x	-y
-x	+y
+y	-x
-y	+x

Charlie

1946 2 14

ENIAC

2007 2 13 D-wave

ORION

D-wave

2007 32

2008 1024