At the limit: Quantum Computing

Classical computer:
- the information is stored in classical bits, values 0,1
- usual operations NOT, AND, OR
- general purpose device

Quantum computer:
- the information is stored in quantum bits **(qubits)**
- **unitary operations**, single- and two-qubit operations (XOR)
- powerful in calculating **specific tasks**

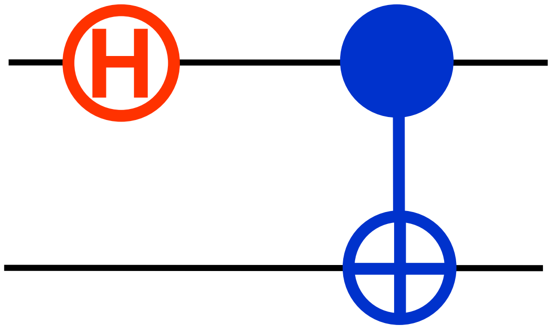
Algorithms:
- prime factorization (Shor)
- data base search (Grover)
- random number generator
- quantum simulation

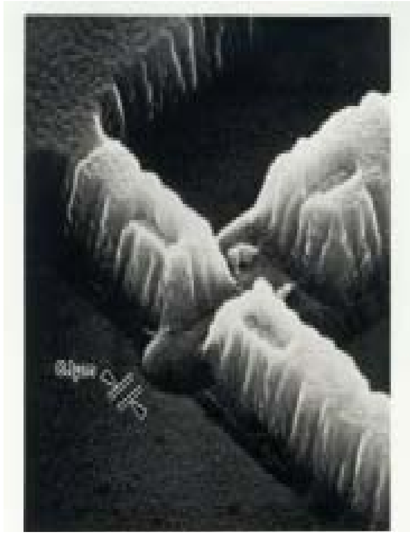
Quantum computation
is an interdisciplinary field,
with contributions from mathematics,
(theoretical) computer science,
physics, and chemistry.

Applications:
- quantum teleportation
- quantum cryptography

Implementations:
- Quantum optics
- **Solid state**
- NMR

Information meets Technology





Recent developments in

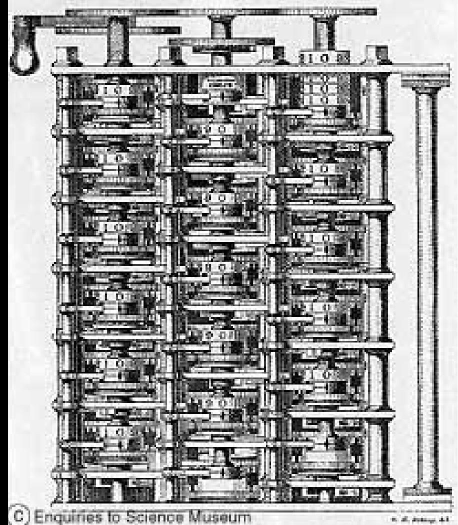
Information Science & **Fundamental/ Applied Physics**

merge to define a new common goal: the quantum computer

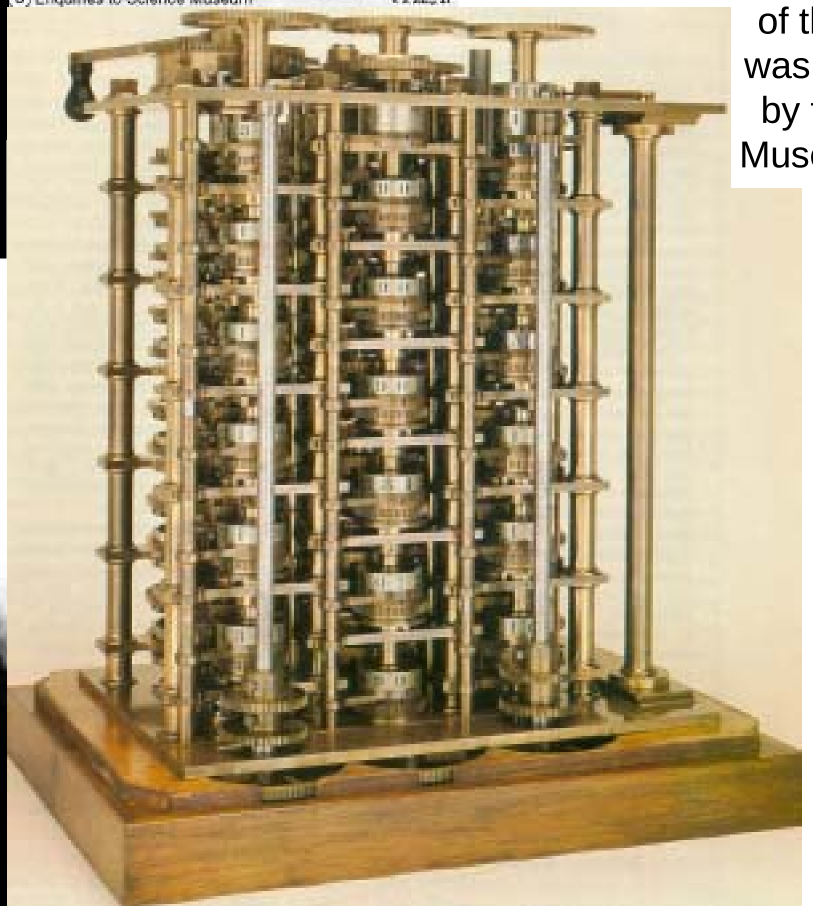
- **History:** from mechanics to nanoelectronics
- **Information Theory:** Turing machines & complexity
- **Quantum Mechanics:** superpositions & entanglement
- **Quantum Games:** no-cloning, cryptography, teleportation
- **Quantum Bits and Gates**
- **Quantum Algorithms:** Shor's period finder
- **Hardware:** superconducting phase qubits

Mechanics

Ada Byron,
Lady Lovelace
1815-1852



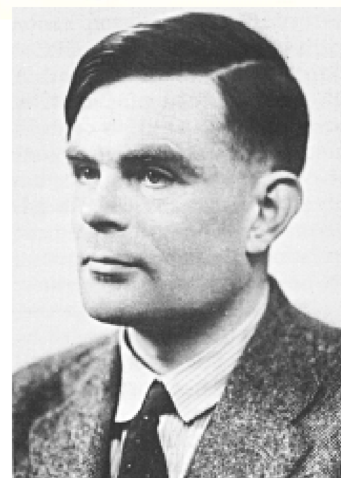
First `Programmer'
and
Inventor of the
Difference Engine
1834



The `full' version of this machine was built in 1991 by the Science Museum, London

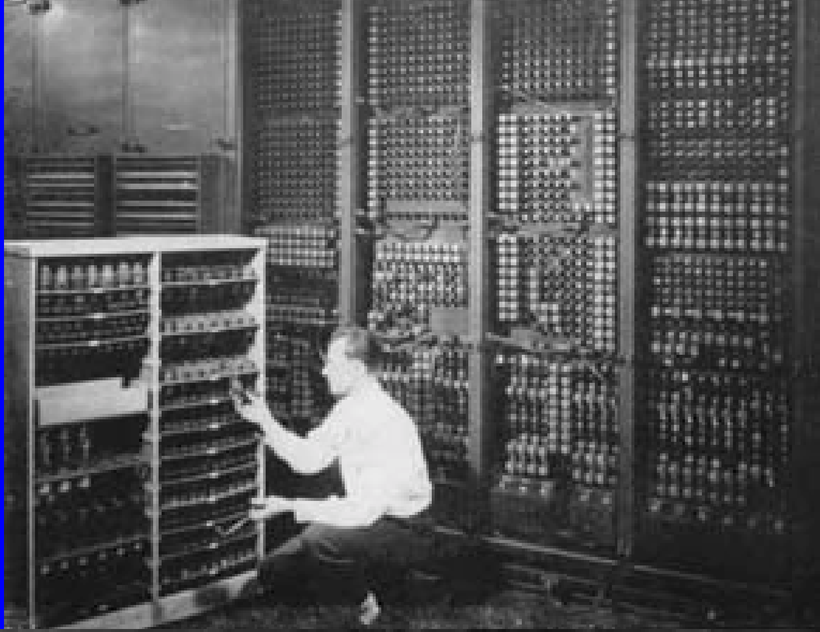
Charles Babbage
1791-1871

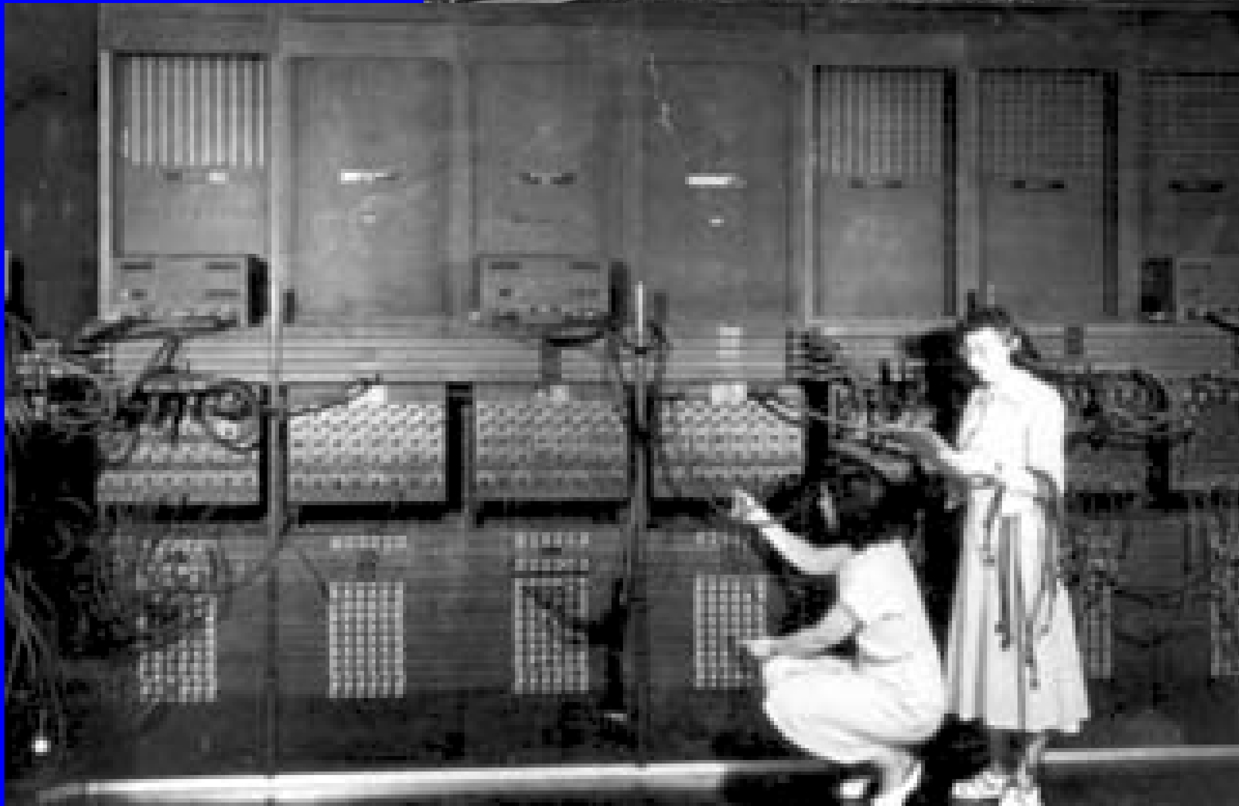
Enigma,
cracked by
Alan Turing
with help of
COLOSSUS



Electronics

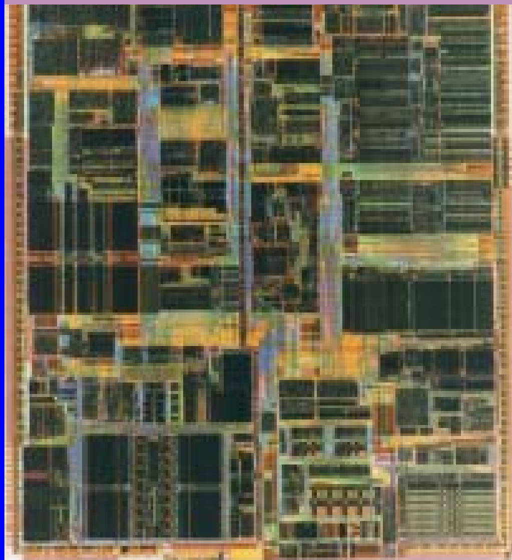
The ENIAC
(Electronic Numerical
Integrator and Computer)
computer
was built in 1946





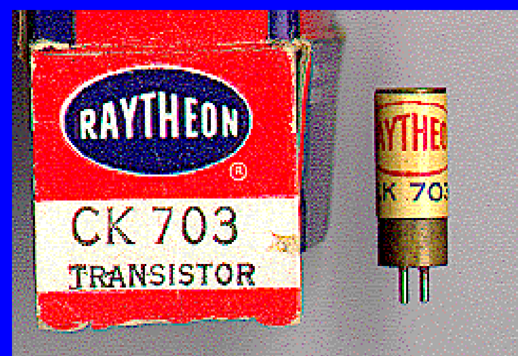
Built at University of Pennsylvania,
it included 18’000 tubes,
weighed 30 tons,
required 6 operators,
and 160 m^2 of space.

Pentium Processor,
1997, Intel



Transistors

First Transistor, 1947
Bell Laboratories
Bardeen, Brattain,
& Shockley

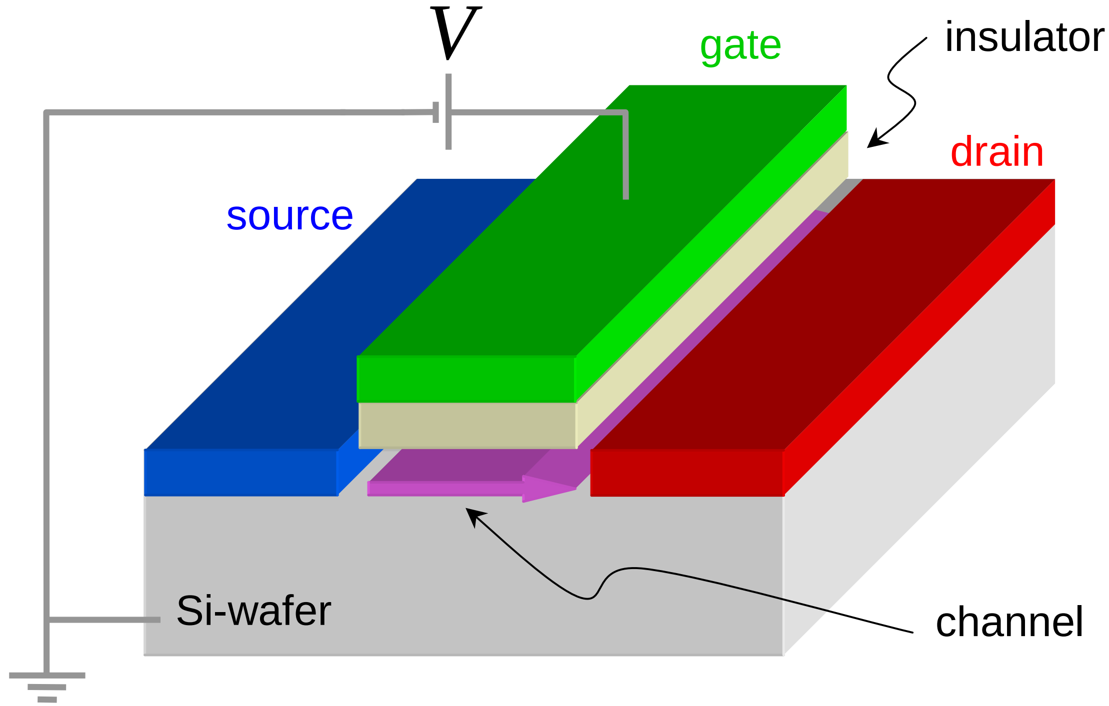


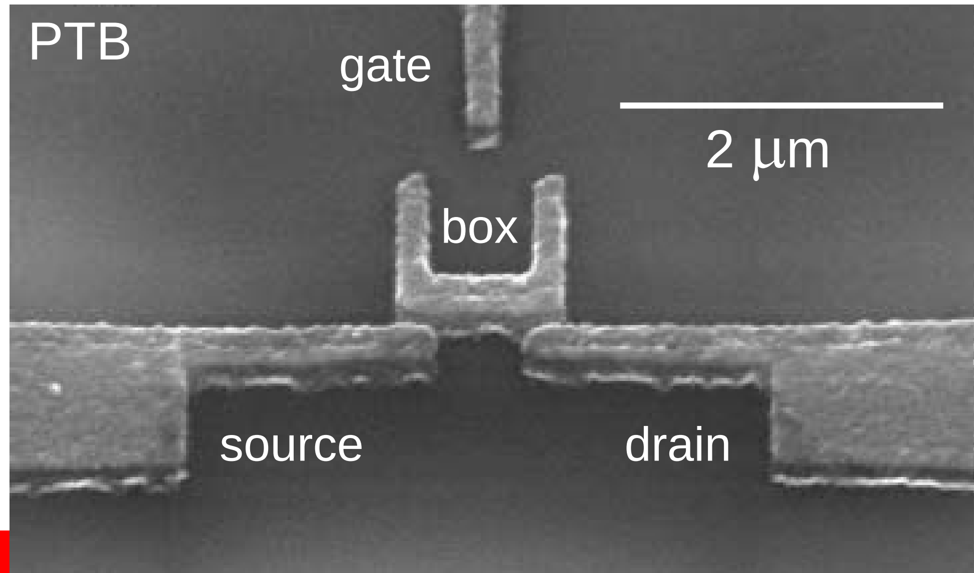
Packed Device

First Integrated Circuit, 1958
Jack Kilby, Texas Instruments

Nanoscale Technology

Ultra-short channel Si-MOSFET, IBM
0.5 µm wide, 0.1 µm channel





Single Electron Transistor (SET), Al–Technology

Switch a MOSFET with **1000** electrons,
while a SET requires only **one**!

Information Theory

Claude Shannon

Information Theory

Information: is a **general concept**,
similar to the concept of energy (appearing in many forms, e.g., mechanical, thermal, electrical,…).

Can be packed into **equivalent forms:**

$0, 1$ $\uparrow, \downarrow$ $\square, \blacksquare$

This text is difficult

Dieser Text ist schwierig

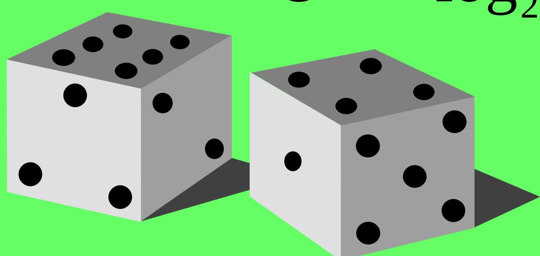
`Ce texte est difficile`

Can be **quantified:** The random variable X distributed according to $p(x)$ contains the information

$$S[p(x)] = -\sum_x p(x)\log_2 p(x)$$

E.g., in the process of throwing a dice one may gain the information

$$S = -\log_2(1/6)$$

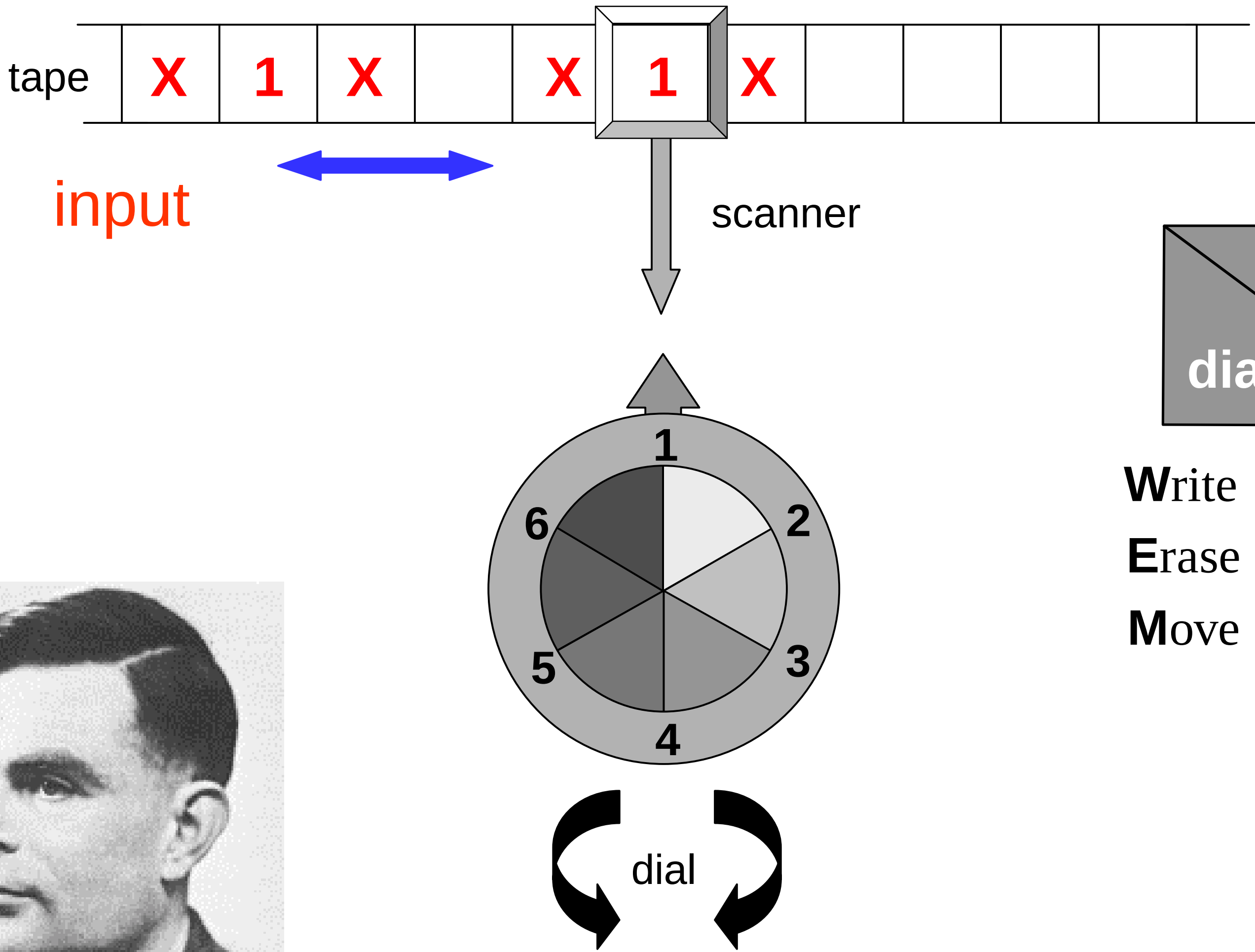


Information is physical (Landauer, 1991):
Need physical implementation to express and manipulate information; e.g.,
ink molecules on paper,
charges in capacitors,
currents in leads.

Rolf Landauer

Turing Machine (mid 1930)

machine



program

dial \ scanner		X	1
1	W_1 6	E 2	M_R 1
2	M_R 2	E 3	Error
3	M_R 3	E 4	E 5
4	M_L 4	Error	M_R 6
5	M_L 5	Error	M_R 1
6	W_X 6	Done	M_R 3

Write
Erase
Move

A Universal Computer

reproduces the action of any other computer :

Let **T** be a Turing machine acting on an input **x**.
There exists a universal machine **U** which takes **x**
and a (binary) description **d** [**T**] as an input and
reproduces the action of **T**, **U**(**d** [**T**], **x**) = **T**(**x**),
with polynomial effort in **d.**

Other models of computation,
e.g., the **network model of computing**,
are equivalent to the Turing model

concatenated logic gates
acting on n-bit symbols

Church-Turing Thesis (unproven)

Every function which would naturally be regarded
as computable can be computed by a
universal Turing machine.

This notion of universality allows us to
classify computational problems

Computational Complexity

An input **x** is quantified via its information content $\mathbf{L = \log_2 x}$.
A calculation is characterized by the number **s** of steps (logical gates) involved.

A problem is class **P** (efficiently solvable) if **s** is polynomial in **L**, $s \sim L^{\mu}$
A problem is deemed `hard' (not in P) if **s** scales exponentially in **L**, $s \sim \exp L^{\nu}$

A `classic' hard problem is that of **prime factorization**:
given a non-prime number **N**, find its factors;
the best known algorithm scales as $\mathbf{s \sim \exp\,(2\, L^{1/3}\,(\ln L)^{2/3})}$.

A modern computer can factor a 130-decimal-digits number (L = 300) in a few weeks – days;

1827365426354265930284950398726453672819048374987653426354857645283905612849667483920396069782635471628694637109586756325221365901

doubling L would take **millions of years** to carry out this calculation.

A quantum computer would do the job within minutes

Public Key Encryption

(Rivest, Shamir & Adleman, 1978)

M = message

$s,\ N = p \cdot q,$ (non-) public key

Encoding

$$E = M^{s} \bmod N$$

Decoding

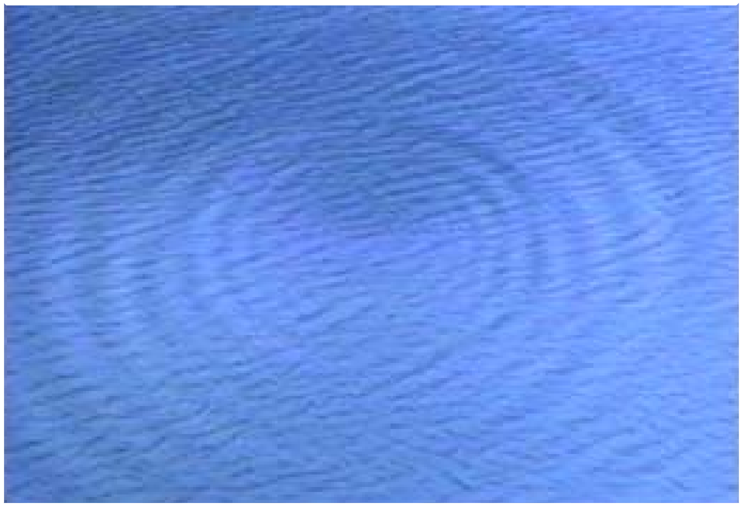
$$M = E^{t(s,p,q)} \bmod N$$

A quantum computer would crack this encryption scheme

Quantum Mechanics

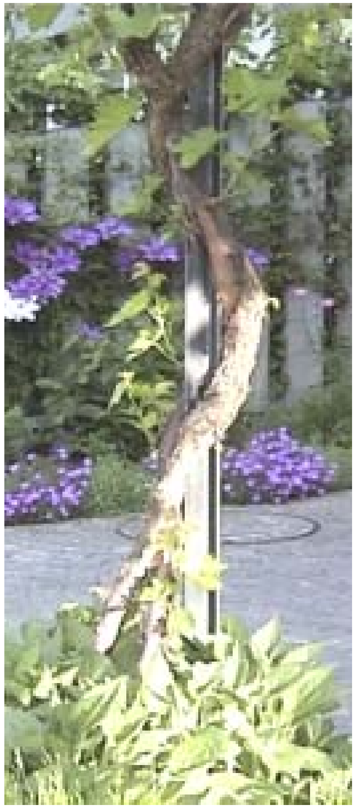
Quantum Mechanics

The following two elements of quantum mechanics are central to quantum computing



Superposition of states:

A quantum degree of freedom is described through a wave function.

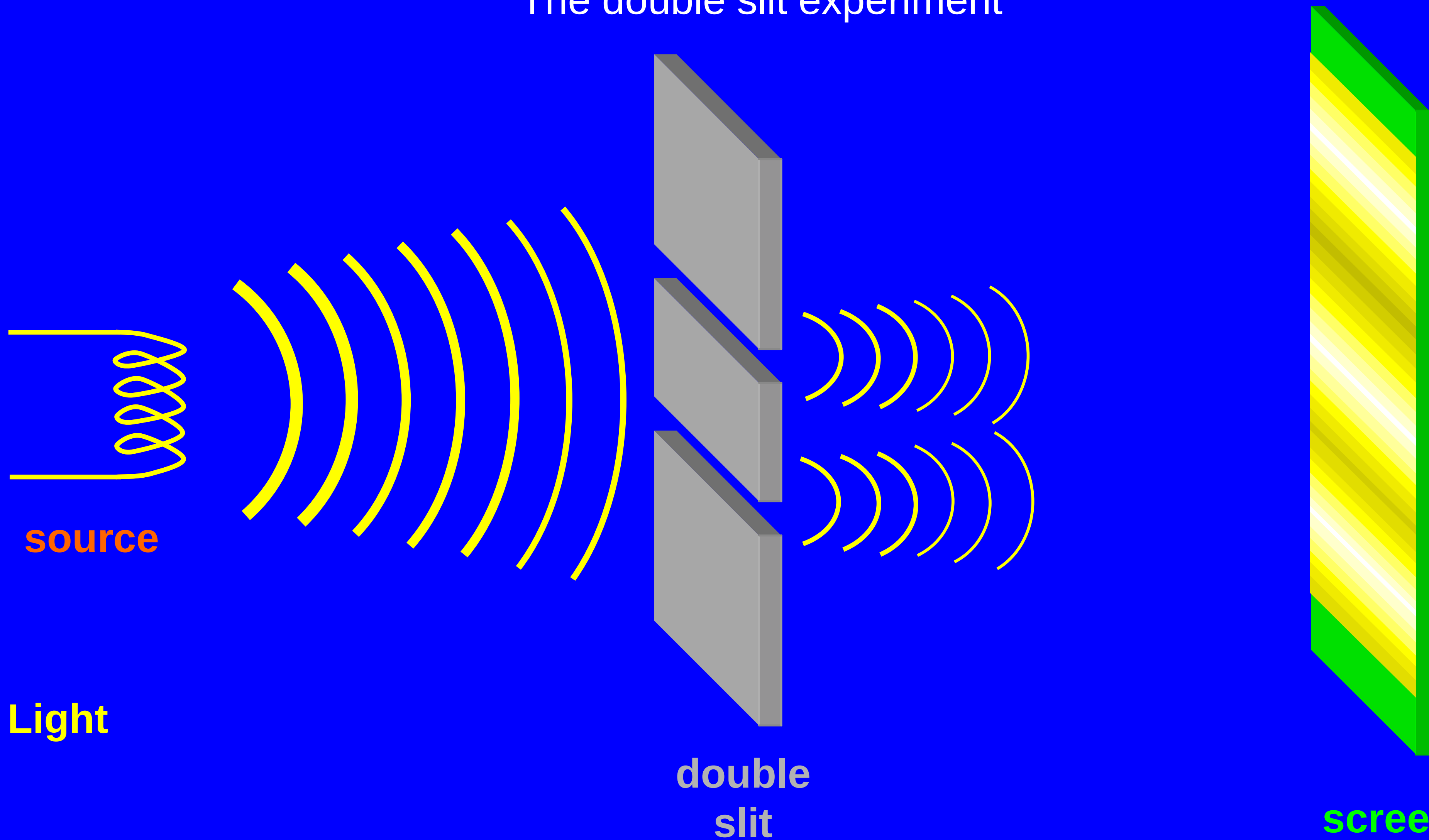


Entanglement of states:

Two quantum degrees of freedom can exhibit stronger correlations than any classical system.

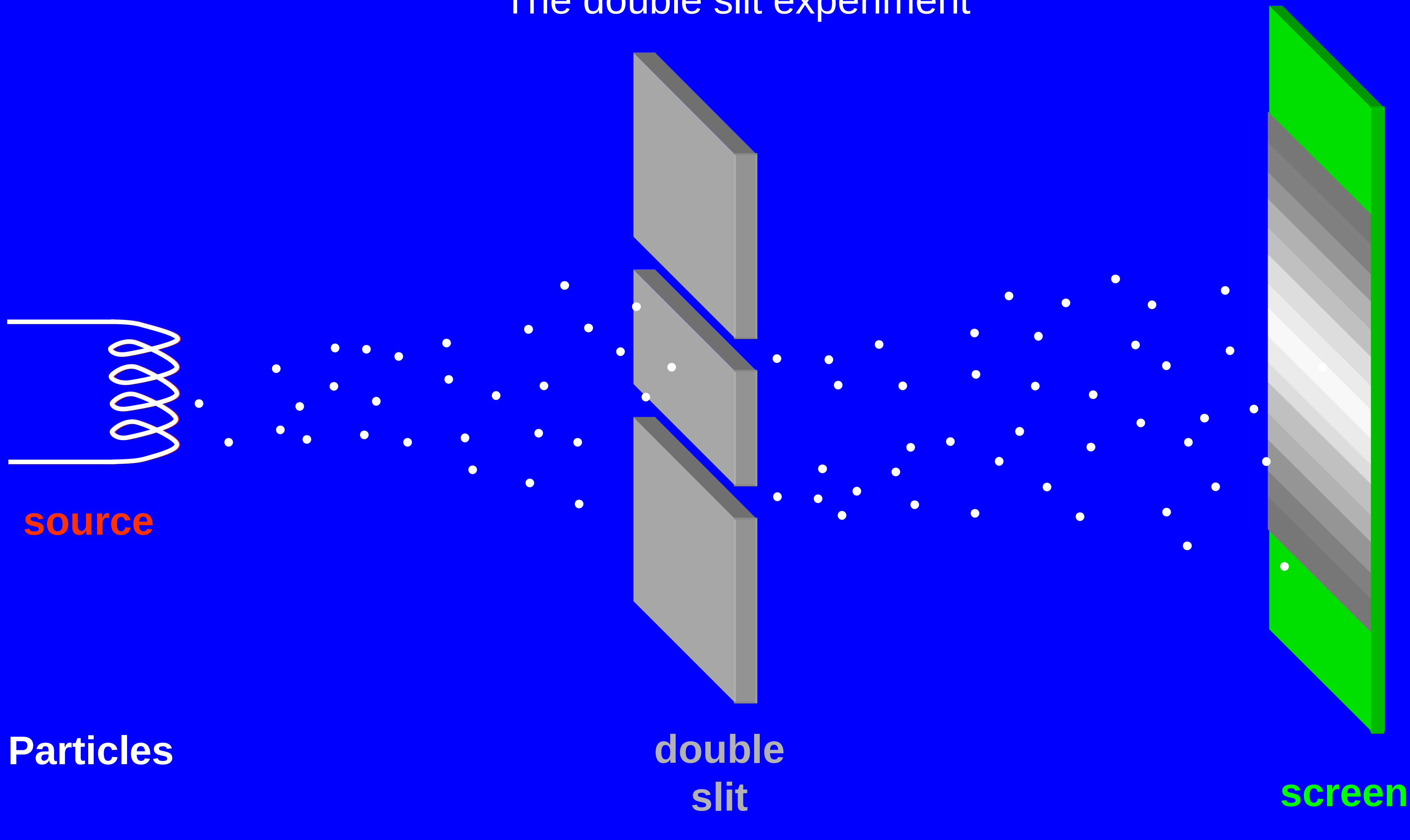
Waves

The double slit experiment

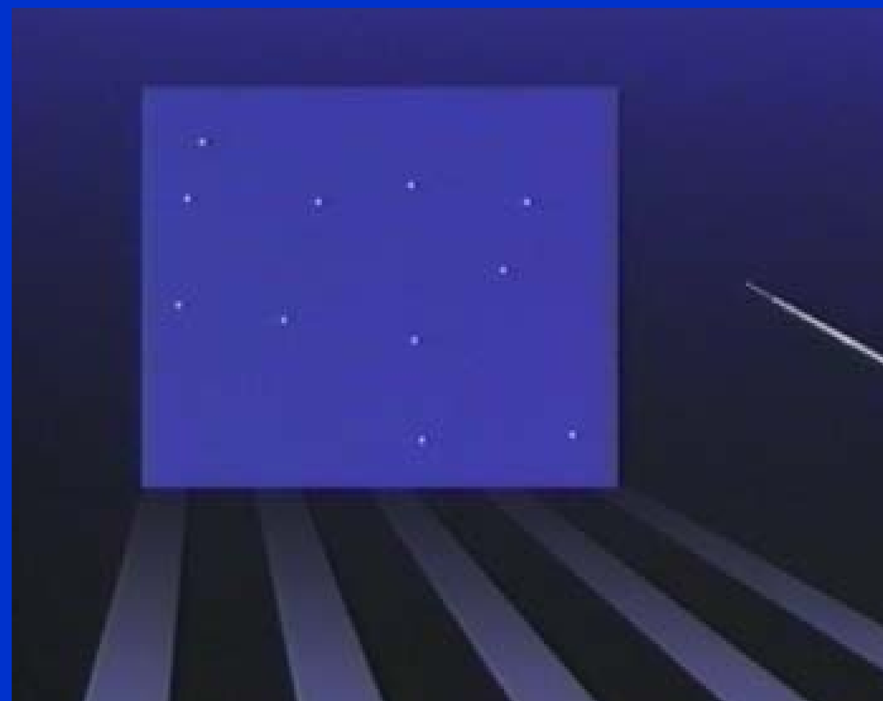


Waves

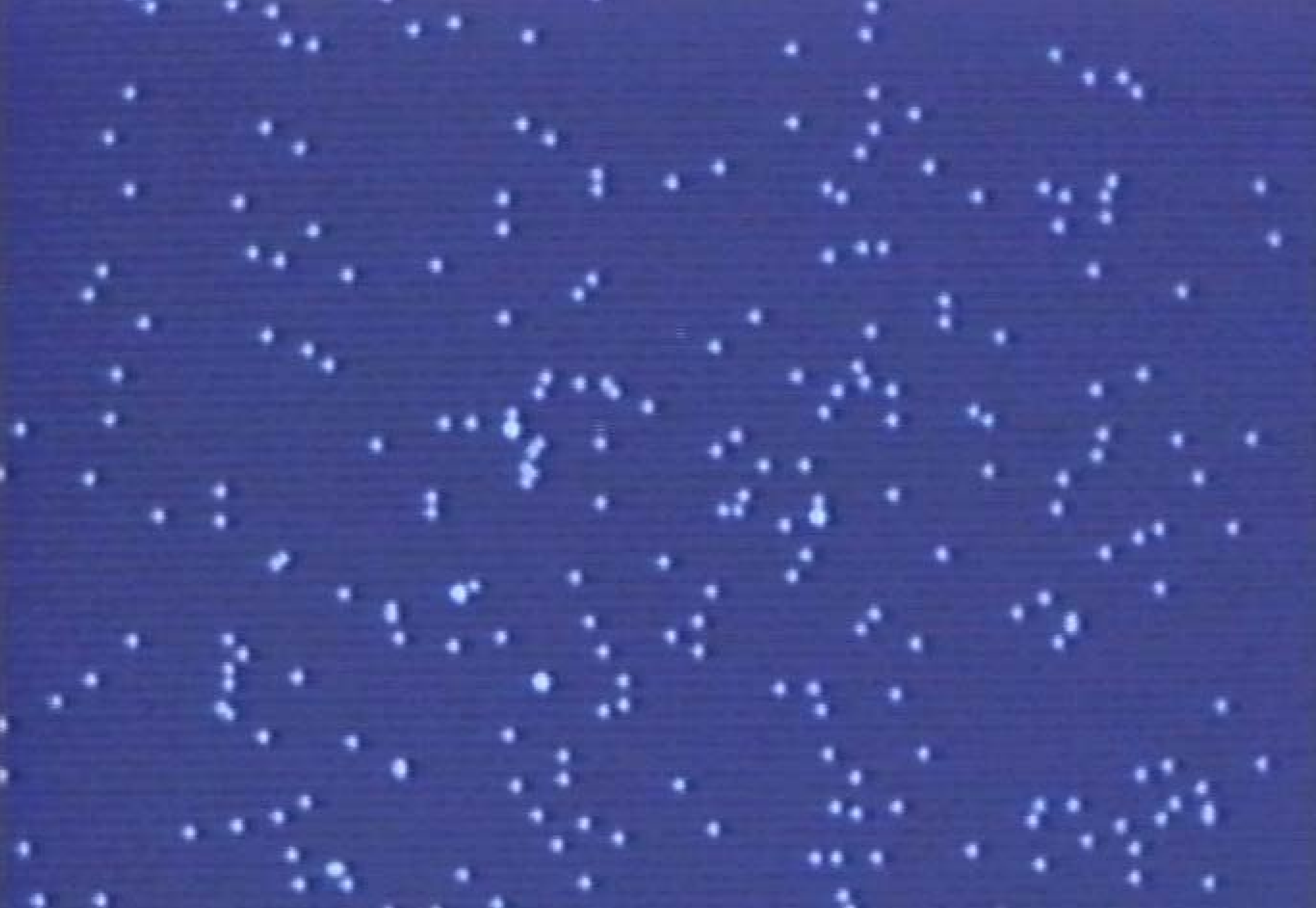
The double slit experiment



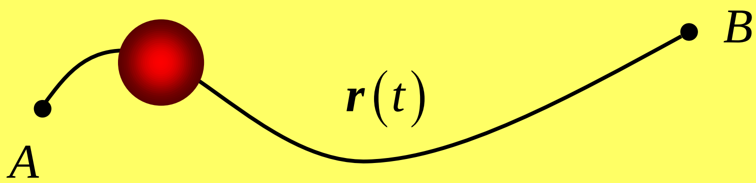
Particle-Wave Duality



- V = 50 kV electrons
- λ = 0.05 Å
- 10^3 electron / sec
- source–screen distance = 1.5 m
- average electron distance 150 km
- size of electronic wave packet 1 µm
- total exposure time 20 min

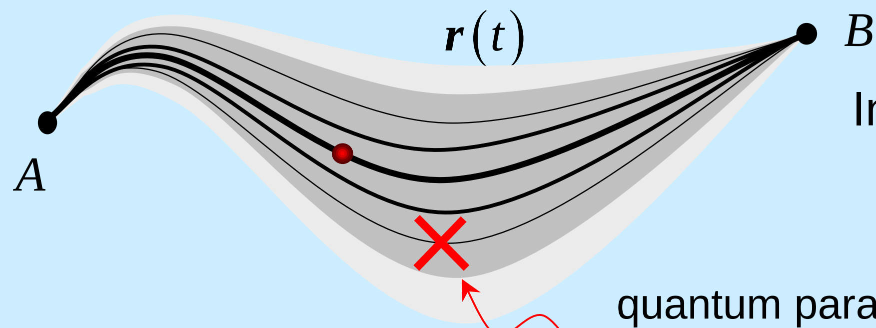


Classical vs quantum mechanics



A classical particle follows its trajectory $\boldsymbol{r}(t)$ from its initial starting point A to its final end point B.

A quantum particle probes all trajectories $\boldsymbol{r}(t)$ from its initial starting point A to its final end point B.

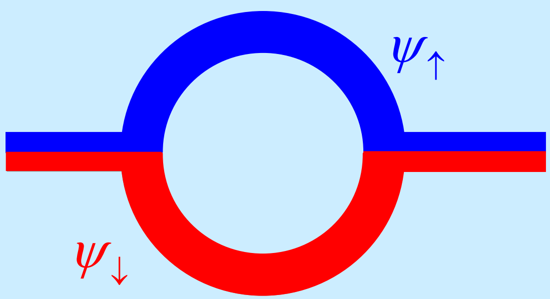


Intensity $\left|\psi_B\right|^2$

quantum parallelism is fragile: external perturbations easily destroy the quantum coherent state.

If we offer a particle only two paths then the wave function is the **superposition** of two amplitudes:

ψ_A



$$\psi_B = \psi_\uparrow + \psi_\downarrow$$

Its wave function is a sum over amplitudes over all paths,

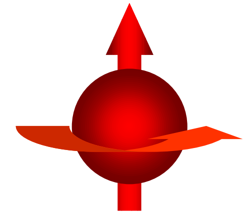
$$\psi_B = \sum_{\text{paths}} \exp\left[i\varphi_{\text{path}}\right]\psi_A$$

phase of the path, $\varphi_{\text{path}} = S_A^B(\text{path})$,

$$S_A^B = \frac{1}{\hbar}\int_{r_A,0}^{r_B,t} dt\left[m\frac{\dot{r}^2}{2} - V(r)\right].$$

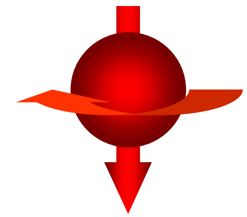
Spins

$$\psi_{\uparrow} = \left|\uparrow\right\rangle$$



Many elementary particles (such as electrons) carry a spin, an internal angular momentum taking on two values:

$$\psi_{\downarrow} = \left|\downarrow\right\rangle$$



A spin system is a generic two-level system which is the generalization of a **classical bit** to a **quantum bit** or **qubit**:

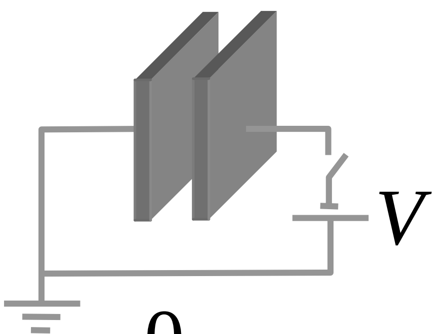
Classical bit

$$0,\ 1$$

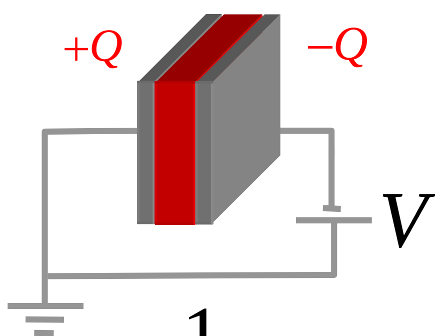
Quantum bit

$$\left|a,\varphi\right\rangle = \left[\left|0\right\rangle + a\, e^{i\varphi} \left|1\right\rangle\right] \Big/ \sqrt{1+a^{2}}$$

Physical realization via a charged/uncharged capacitor



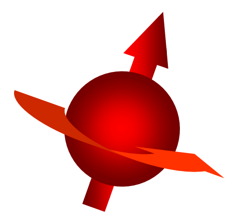
0



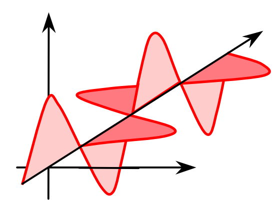
1

Physical realization via a two-level system

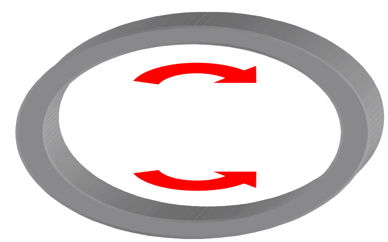
spin



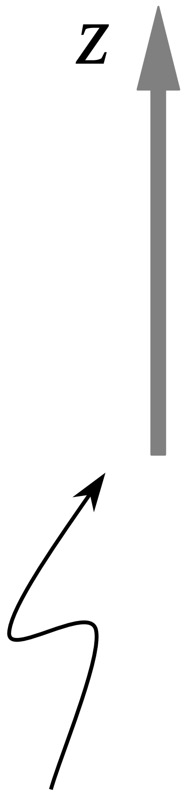
polarization



ring-current



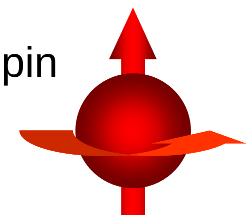
Quantization axis: preparing spins



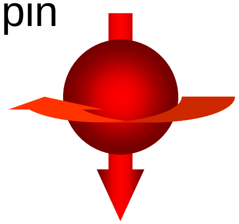
Choose an axis,
e.g., the z-axis,
and measure the spin,

we will find either

an up-spin



or a down-spin

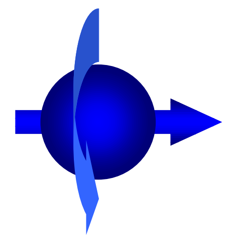


quantization axis

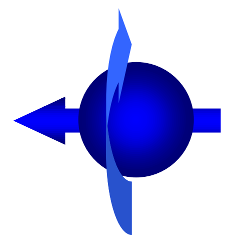
Let us assume we measured an up spin. We can re-measure the spin to check if it is still up and it will always be

But then, let us measure the spin along another axis, say the x-axis; we will find a new result, namely, half of the time the spin will point along

the positive direction



the negative direction

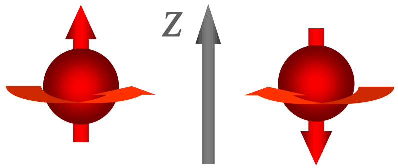


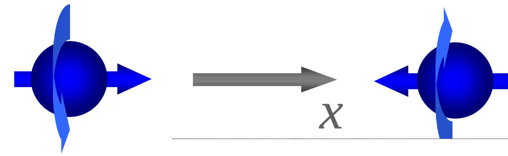
The reason is, that a spin prepared along a definite (quantization) axis, is a (50/50) superposition of states when viewed from another axis.

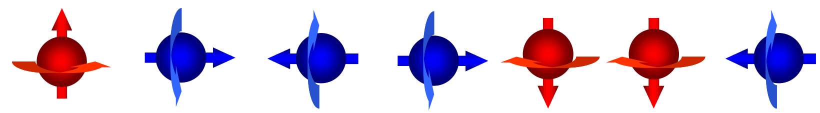
$$\left|\uparrow_z\right\rangle = \left[\left|{}_x\!\rightarrow\right\rangle + \left|\leftarrow_x\right\rangle\right]/\sqrt{2}$$

Cryptography

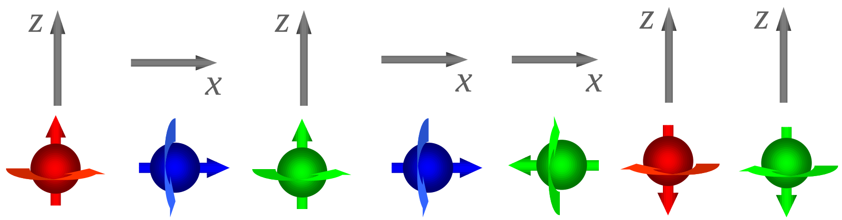
We can make use of spin / two-level systems for cryptography: Alice and Bob wish to exchange a secret key, a sequence of 0 and 1. In order to do so, Alice sends Bob a sequence of spins which she polarized either along the z- or x- axis.

$|\uparrow\rangle =$  $= |\downarrow\rangle$

$|+\rangle = [|\uparrow\rangle + |\downarrow\rangle]/\sqrt{2} =$  $|-\rangle = [|\uparrow\rangle - |\downarrow\rangle]/\sqrt{2}$

$\uparrow + - + \downarrow\downarrow - =$ 

Bob measures the spins he receives from Alice, choosing randomly among the x- and z- axis



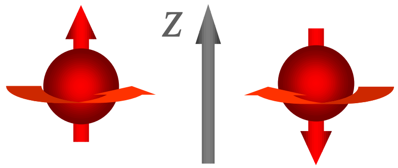
$= \uparrow + \uparrow + - \downarrow\downarrow$

When Alice publicly announces along which axes she has prepared the individual spins, Bob can identify the bad spins and inform Alice – in the end they possess a `good' key made from $|\uparrow\rangle, |+\rangle \Rightarrow 0$ and $|\downarrow\rangle, |-\rangle \Rightarrow 1.$

Cryptography

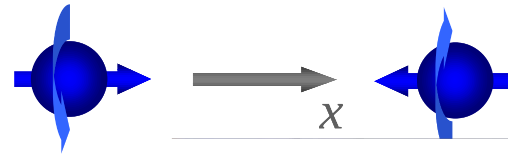
We can make use of spin / two-level systems for cryptography: Alice and Bob wish to exchange a secret key, a sequence of 0 and 1. In order to do so, Alice sends Bob a sequence of spins which she polarized either along the z- or x- axis.

$|\uparrow\rangle =$



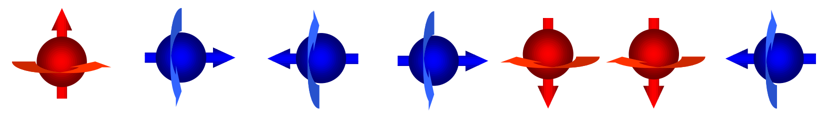
$= |\downarrow\rangle$

$|+\rangle = [|\uparrow\rangle + |\downarrow\rangle]/\sqrt{2} =$

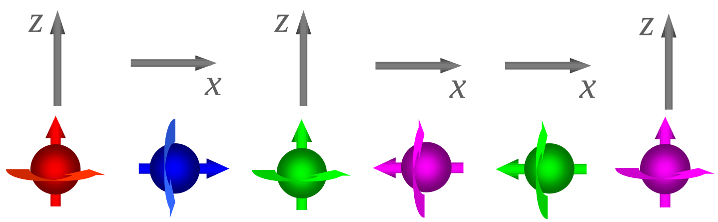


$|-\rangle = [|\uparrow\rangle - |\downarrow\rangle]/\sqrt{2}$

$\uparrow + - + \downarrow\downarrow - =$



Bob measures the spin he receives from Alice, choosing randomly among the x- and z- axis



Alice and Bob share a probabilistically secure key

And when Eve interferes to learn about Alice’s and Bob’s secret key, she will spoil the sequence such that Bob and Alice can detect her presence.

Classical & quantum gates I

The possibilities to manipulate a classical bit are quite limited:
The NOT-gate simply interchanges the two values 0 and 1 of the classical bit.

i	f
0	*1*
1	*0*

On the other hand, manipulation of a quantum bit is much richer!

Classical & quantum gates I

A single qubit is manipulated via **unitary transformations** $U(t)$,
which is just the usual **time evolution of quantum mechanics:**

Schrödinger equation

$$i\hbar\partial_t\psi(t) = H\,\psi(t), \quad H = H^{\dagger},$$

Hamiltonian

$$\psi(t) = \underbrace{\exp\left[-iH\,t/\hbar\right]}_{U(t)}\,\psi(0)$$

For a spin / two-level system we can perform rotations around the x -, y -, and z - axis;
placing the spin $\boldsymbol{S}$ (with magnetic moment μ) into a magnetic field $\boldsymbol{H}$, the Hamiltonian

$$H = -\mu \boldsymbol{S}\cdot\boldsymbol{H}$$

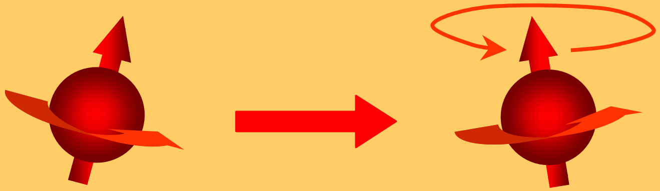
produces the desired rotation. E.g., with

$H = H_z$ we obtain the time evolution

$$U = \begin{pmatrix} e^{-i\mu H_z t/2} & 0 \\ 0 & e^{i\mu H_z t/2} \end{pmatrix},$$

phase shifter

$$|\psi(t)\rangle = \left[e^{-i\mu H_z t/2}|\uparrow\rangle + a\,e^{i\mu H_z t/2}|\downarrow\rangle\right]\Big/\sqrt{1+a^2}\,.$$

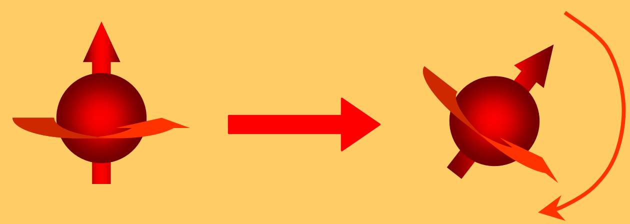


$H = H_x$ we obtain the time evolution

$$U = \begin{pmatrix} \cos\mu H_x t & i\sin\mu H_x t \\ i\sin\mu H_x t & \cos\mu H_x t \end{pmatrix},$$

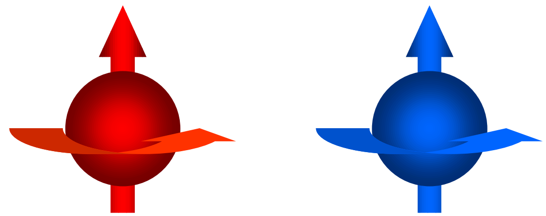
amplitude shifter ($a = 0$)

$$|\psi(t)\rangle = \cos\mu H_x t\,\left[|\uparrow\rangle + i\tan\mu H_x t\,|\downarrow\rangle\right].$$



Entanglement

Consider two spins:



They can appear in a superposition of four states

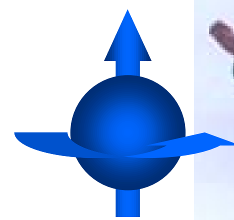
$$|\uparrow\uparrow\rangle,\ |\uparrow\downarrow\rangle,\ |\downarrow\uparrow\rangle,\ |\downarrow\downarrow\rangle$$

The singlet state
is an entangled state
with astonishing properties:

$$|00\rangle = [|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle]/\sqrt{2}$$

After preparation of the singlet state (through having the two spins interact with one another) let us separate the two spins and give Alice and Bob each one of the two spins:

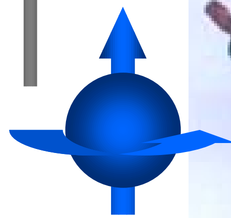
Alice and Bob now can experiment with their spins, e.g., measure their direction along the *x*-, *y*,-, or *z*- axis, and they will find a few astonishing results!

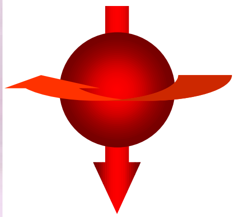


Einstein-Podolsky-Rosen

Have Alice measure her spin along an axis, say the z-axis. She has a fifty-fifty chance to measure a spin up – assume she really finds her spin pointing up.

z





Next, have Bob measure his spin; although he may be arbitrarily far away from Alice, he will find his spin point down. This is the **EPR–Paradox: quantum mechanics is non-local**.

The repetition of this experiment always gives the same result – the two entangled spins are fully correlated. A more careful analysis shows, that whenever Alice and Bob measure their spins along the directions θ_A and θ_B they will find them correlated to a degree $\sin^2[(\theta_A - \theta_B)/2]$ – there is no classical process which will deliver such a high degree of correlations – here is a process which a classical computer cannot simulate!

No-Cloning

The ability to copy a classical bit is widely exploited in computers and algorithms.

C → C C

There are no quantum copying machines: a qubit cannot be copied (cloned).

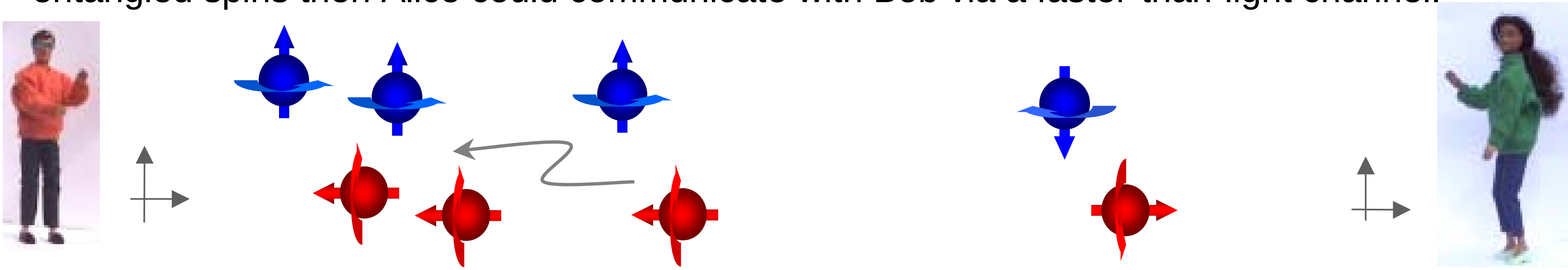
Assume the contrary, then there exists a unitary operator U independent of $|\alpha\rangle$ and $|\beta\rangle$ which produces copies of $|\alpha\rangle$ and $|\beta\rangle$,

$$U|\alpha 0\rangle = |\alpha\alpha\rangle \quad \text{and} \quad U|\beta 0\rangle = |\beta\beta\rangle.$$

But when we try to copy $|\gamma\rangle = [|\alpha\rangle + |\beta\rangle]/\sqrt{2}$ our quantum copying machine U fails,

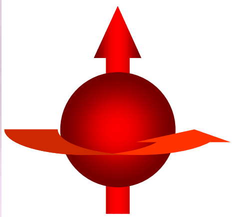
$$U|\gamma 0\rangle = \left[|\alpha\alpha\rangle + |\beta\beta\rangle\right]/\sqrt{2} \neq |\gamma\gamma\rangle.$$

The combination of the EPR Paradox and the No-Cloning Theorem rescues the consistency between quantum mechanics and special relativity: For, if Bob could draw copies of entangled spins then Alice could communicate with Bob via a faster-than-light channel.

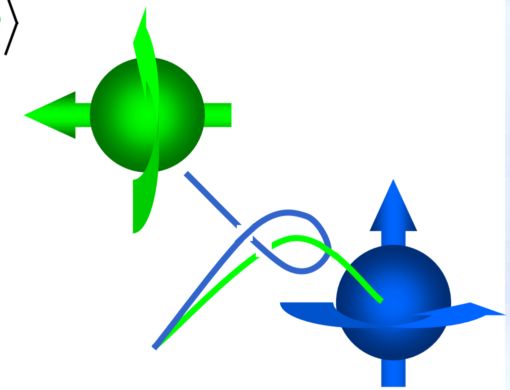


Teleportation

Though a qubit $|\phi\rangle = a|\uparrow\rangle + b|\downarrow\rangle$ cannot be copied, it can be teleported, i.e., it can be made to vanish at one place and reappear at another place. In order to do so, Alice and Bob share an entangled state $[|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle]/\sqrt{2}$.



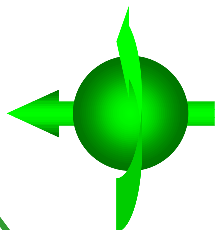
Next, Alice entangles her spin $\uparrow$ with the unknown state $|\phi\rangle$ and then measures what state her two spins are in.

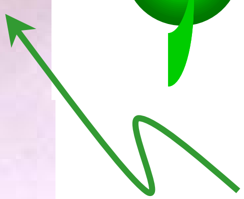


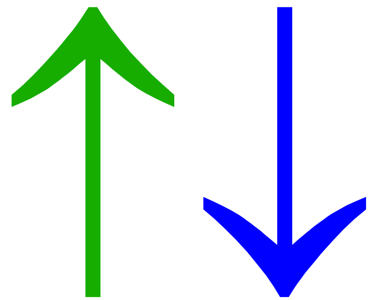
Teleportation

Though a qubit $|\phi\rangle = a|\uparrow\rangle + b|\downarrow\rangle$ cannot be copied, it can be teleported, i.e., it can be made to vanish at one place and reappear at another place. In order to do so, Alice and Bob share an entangled state $[|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle]/\sqrt{2}$.

Next, Alice entangles her spin $\uparrow$ with the unknown state $|\phi\rangle$ and then measures what state her two spins are in.







She tells Bob, which of the four possible results $\uparrow\uparrow, \uparrow\downarrow, \downarrow\uparrow, \downarrow\downarrow$ she has found and Bob carries out the appropriate rotation of his spin $\uparrow$ by π around the 1, x-, z- , or y-axis.

As a result, Bob ends up with his spin in the state $|\phi\rangle = a|\uparrow\rangle + b|\downarrow\rangle$.

Classical & quantum gates II

irreversible

NOT

i	f
0	*1*
1	*0*

AND

i	i	f
0	*0*	*0*
0	*1*	*0*
1	*0*	*0*
1	*1*	*1*

OR

i	i	f
0	*0*	*0*
0	*1*	*1*
1	*0*	*1*
1	*1*	*1*

The combination of the classical gates allows us to construct all manipulations on classical bits.

Is there a set of universal quantum gates ?
How does such a set look like ?

Single–qubit gates:
Rotations

$$U = \begin{pmatrix} \cos(\theta/2) & -ie^{-i\phi}\sin(\theta/2) \\ -ie^{i\phi}\sin(\theta/2) & \cos(\theta/2) \end{pmatrix},$$

amplitude shifter

phase shifter

$$|\psi\rangle = \left[|0\rangle + a\, e^{i\varphi}\, |1\rangle\right] \Big/ \sqrt{1+a^2}\,.$$

Hadamard (basis change):

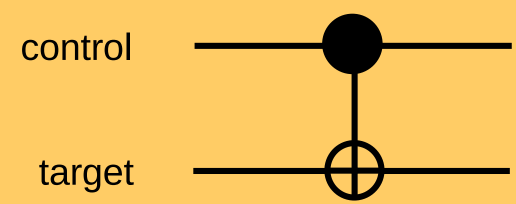
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}: \quad \left.\begin{matrix} |0\rangle \\ |1\rangle \end{matrix}\right\} \Leftrightarrow \left\{\begin{matrix} |+\rangle = \left[|0\rangle + |1\rangle\right]/\sqrt{2}, \\ |-\rangle = \left[|0\rangle - |1\rangle\right]/\sqrt{2}. \end{matrix}\right.$$

Two–qubit gate:
XOR (CNOT)

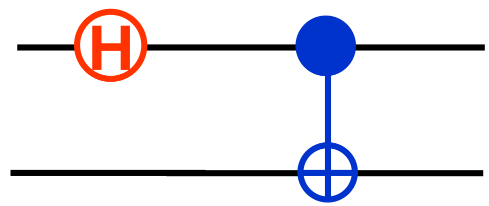
The target flips if the control is on 1

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

i	i	f
0	*0*	*0*
0	*1*	*1*
1	*0*	*1*
1	*1*	*0*



Entangling two qubits



$$\mathbf{H}|00\rangle = \left[|00\rangle + |10\rangle\right]/\sqrt{2}$$

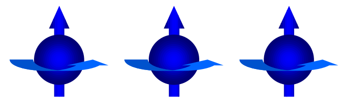
$$\mathbf{XOR}\left(\mathbf{H}|00\rangle\right) = \left[|00\rangle + |11\rangle\right]/\sqrt{2}$$

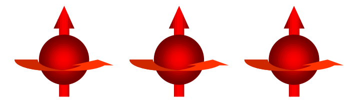
Quantum Algorithms

Quantum algorithms

Find the period of the function
$f(x) = 1 + \cos(\pi x)$ (Shor)

We work with two registers, X and Y:

X : 

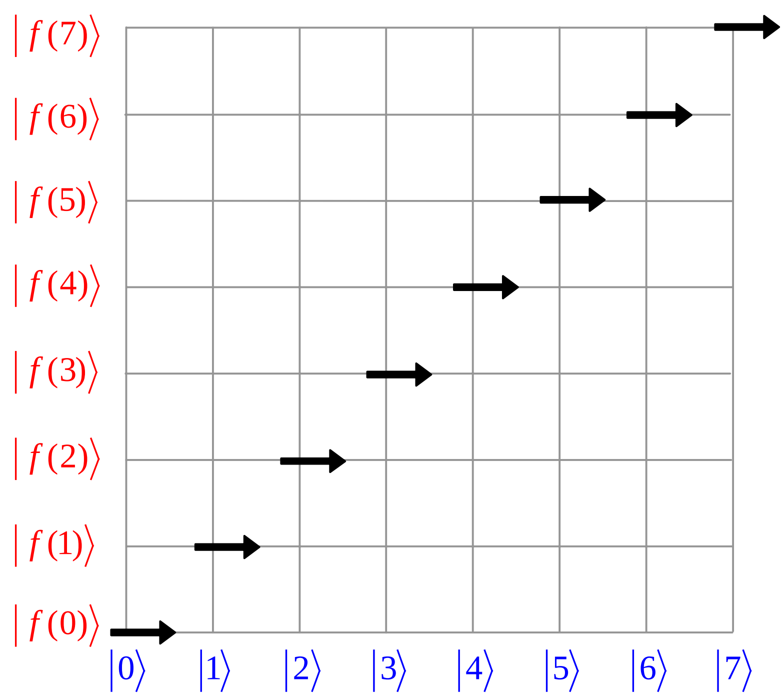
Y : 

Place the X register into a superposition of all states, Y into the state 0 :

$$|\psi_X\rangle = \left[|000\rangle + |100\rangle + |010\rangle + |001\rangle + |011\rangle + |101\rangle + |110\rangle + |111\rangle\right]/\sqrt{8}$$
$$= \left[|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle\right]/\sqrt{8},$$
$$|\psi_Y\rangle = |000\rangle = |0\rangle.$$

Next, we entangle the X and Y registers, evaluating all function values $f(x)$ in one go

$$\psi = \tfrac{1}{8}\sum_x |x, f(x)\rangle,$$



Quantum algorithms, cont.

and then carry out a discrete Fourier transform on the X register,

$$|x\rangle \Rightarrow \frac{1}{\sqrt{8}} \sum_{k=0}^{7} e^{2\pi i k x/8} |k\rangle,$$

producing the superposition

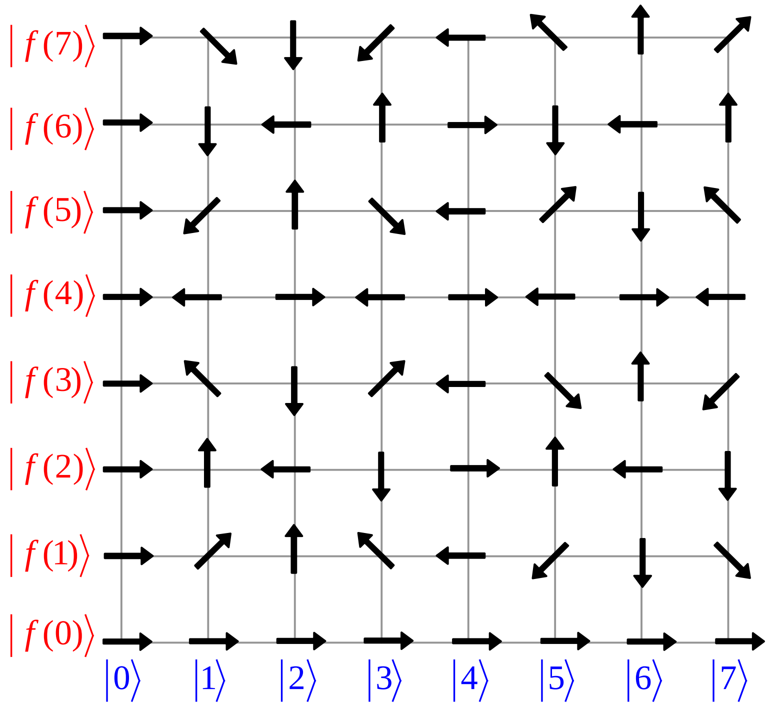
$$|\psi\rangle = \tfrac{1}{8} \sum_{x,k=0}^{7} e^{2\pi i k x/8} \left| k, f(x) \right\rangle$$

$$= \tfrac{1}{8}|0\rangle \left[|f(0)\rangle + \quad |f(1)\rangle + \ldots + \quad |f(6)\rangle + \quad |f(7)\rangle \right]$$

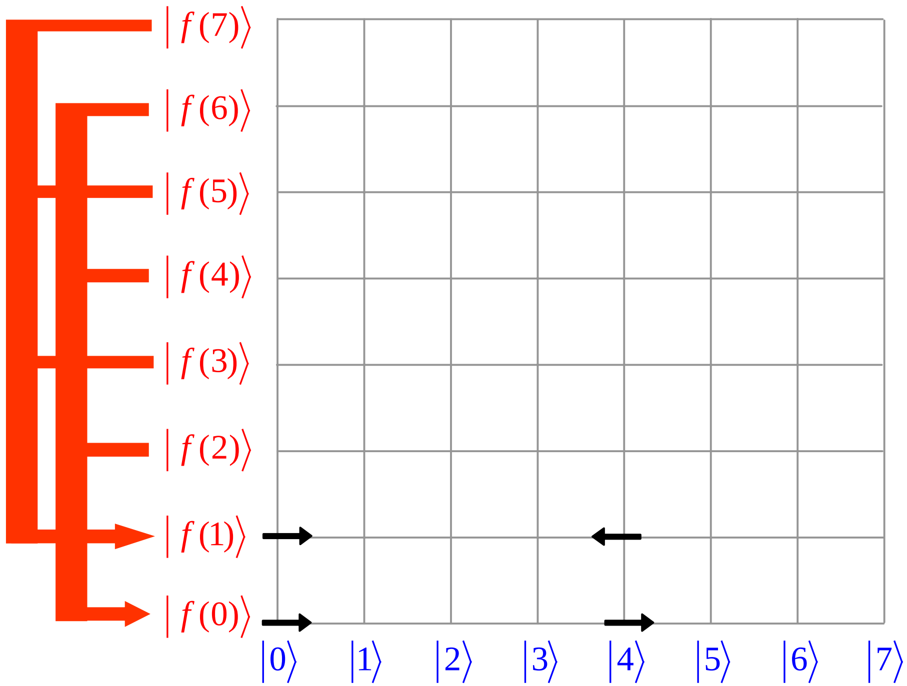
$$+ \tfrac{1}{8}|1\rangle \left[|f(0)\rangle + e^{2\pi i/8} |f(1)\rangle + \ldots + e^{12\pi i/8} |f(6)\rangle + e^{14\pi i/8} |f(7)\rangle \right]$$

$$+ \tfrac{1}{8}|2\rangle \left[|f(0)\rangle + e^{4\pi i/8} |f(1)\rangle + \ldots + e^{24\pi i/8} |f(6)\rangle + e^{28\pi i/8} |f(7)\rangle \right]$$

$$+ \ldots \quad .$$



Quantum algorithms, cont.



Finally, assume that $f(x)$ has period 2,

$$f(0) = f(2) = f(4) = f(6),$$

$$f(1) = f(3) = f(5) = f(7);$$

then most amplitudes add up to zero:

$$
\begin{aligned}
|\psi\rangle = \tfrac{1}{2}|0\rangle\Big[|f(0)\rangle & + |f(1)\rangle\Big] \\
+ \tfrac{1}{8}|1\rangle\Big[|f(0)\rangle\left[1 + e^{4\pi i/8} + e^{8\pi i/8} + e^{12\pi i/8}\right] & + |f(1)\rangle\left[e^{2\pi i/8} + e^{6\pi i/8} + e^{10\pi i/8} + e^{14\pi i/8}\right]\Big] \\
+ \tfrac{1}{8}|2\rangle\Big[|f(0)\rangle\left[1 + e^{8\pi i/8} + e^{16\pi i/8} + e^{24\pi i/8}\right] & + |f(1)\rangle\left[e^{4\pi i/8} + e^{12\pi i/8} + e^{20\pi i/8} + e^{28\pi i/8}\right]\Big] \\
+ \ldots & \\
+ \tfrac{1}{8}|4\rangle\Big[|f(0)\rangle\left[1 + e^{16\pi i/8} + e^{32\pi i/8} + e^{48\pi i/8}\right] & + |f(1)\rangle\left[e^{8\pi i/8} + e^{24\pi i/8} + e^{40\pi i/8} + e^{56\pi i/8}\right]\Big] \\
+ \ldots \quad . &
\end{aligned}
$$

Quantum algorithms, cont.

In the end we obtain the state

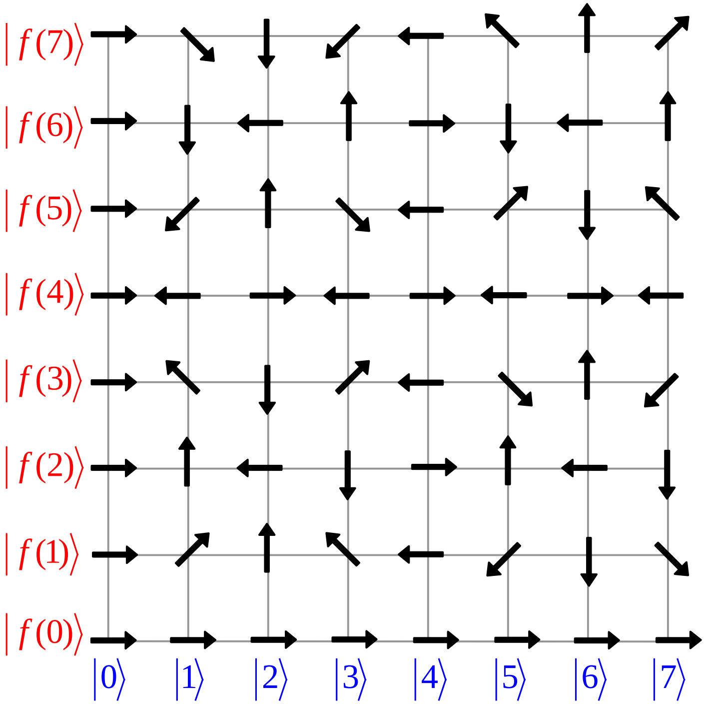
$$|\psi\rangle = \tfrac{1}{2}\left[|0, f(0)\rangle + |0, f(1)\rangle + |4, f(0)\rangle - |4, f(1)\rangle\right]$$

and a measurement of the ***X*** register always delivers a result $k = 0$ or $k = 4$, each with probability 1/2. The period p of the function f then is given by

$$p = \text{maximal numerator}\left[\text{red}\left(\frac{2^3}{k}\right)\right] = 2.$$

Once we know how to calculate the period of a function a few more steps are needed to factorize a number (Shor's algorithm, using **Euclid's algorithm** for finding the greatest common divisor of two numbers).

Note, there is no quantum speed-up in adding numbers! Classical computers do a great job on that.



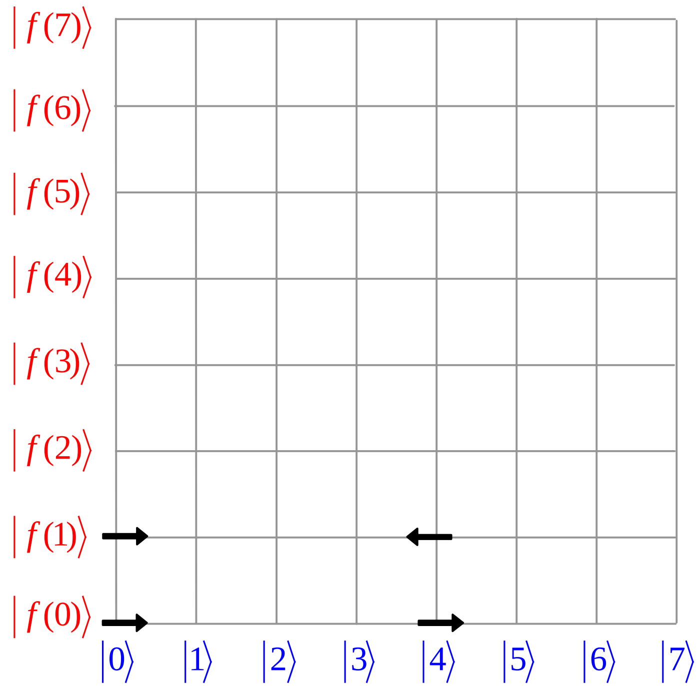
Parallel evolution

Evaluate all function *f(x)* in one go

$$\psi = \tfrac{1}{8}\sum_{x} \left| x, f(x) \right\rangle$$

`Cleanup'

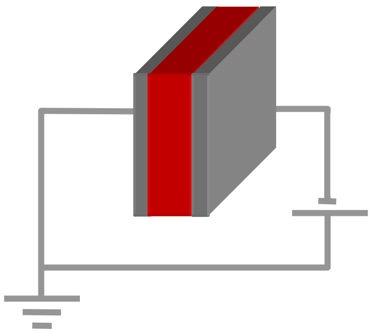
due to interference



Hardware

Hardware

Classical computer



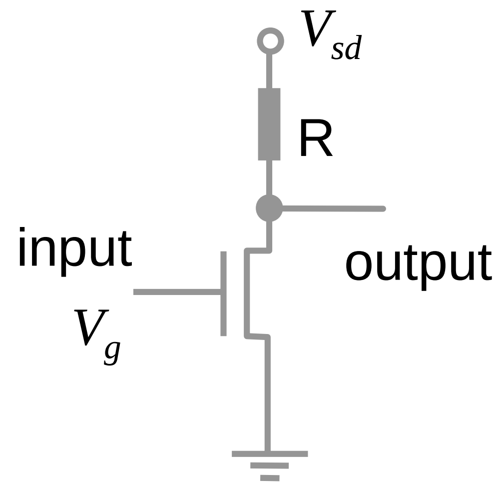
Capacitors:

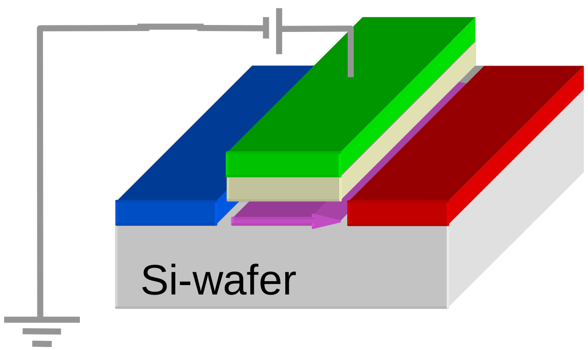
Bits

$$0: \quad V = 0,$$

$$1: \quad V > 0.$$

1-bit gate: NOT





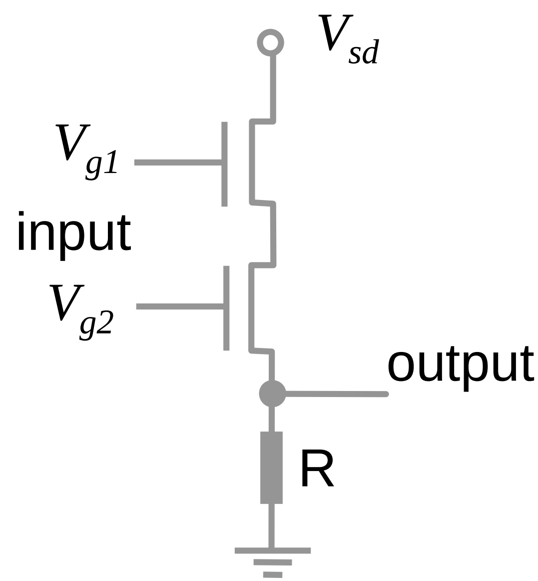
Transistors:

Gates

$V_g = 0$, closed,

$V_g > 0$, open.

2-bit gate: AND



Network model of quantum computing

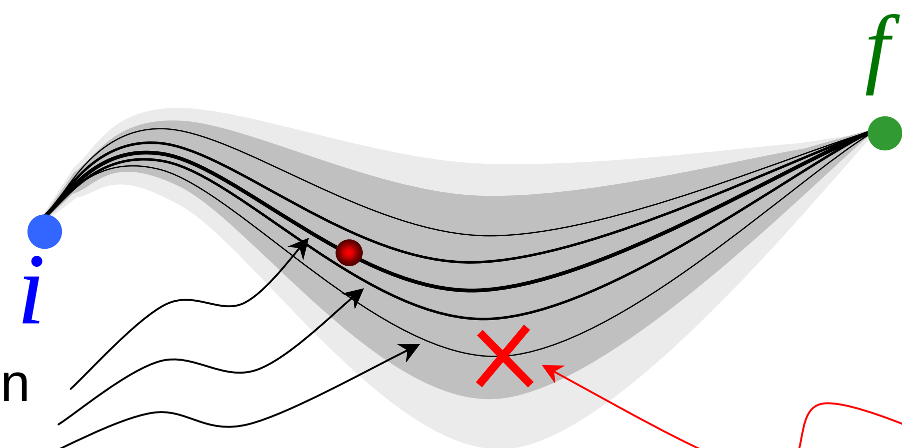
(David Deutsch, 1985)

initial state

- each qubit can be **prepared** in some known state, $|00000\ldots0000\rangle$.
- each qubit can be **measured** in a basis, $|01100\ldots1010\rangle$.

final state

- the qubits can be **manipulated** through quantum gates
- the qubits are **protected** from decoherence



Parallel evolution providing the quantum speedup.

Perturbations from the environment destroy the parallel evolution of the computation

Physical implementations

Quantum optics, NMR-schemes

Good decoupling & precision:

- trapped atoms (Cirac & Zoller)
- photons in QED cavities (Monroe ea, Turchette ea)
- molecular NMR (Gershenfeld & Chuang)
- ^{31}P in silicon (Kane)

Solid state implementations

Good scalability & variability:

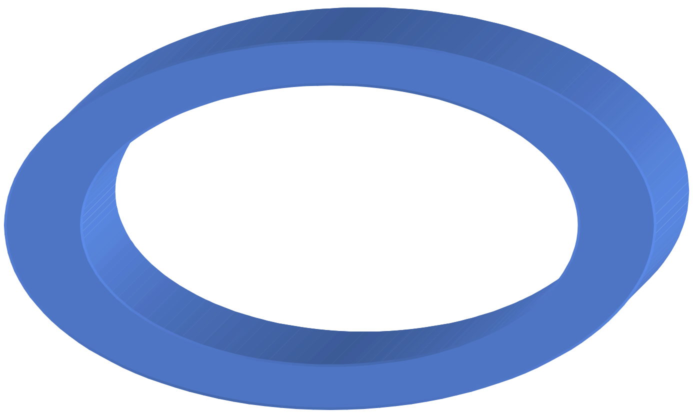
- spins on quantum dots (Loss & DiVincenzo)
- ^{31}P in silicon (Kane)
- Josephson junctions, charge (Schön ea, Averin)
  phase (Bocko ea, Mooij ea)

All hardware implementations of quantum computers have to deal with the conflicting requirements of **controllability** while minimizing the coupling to the environment in order to **avoid decoherence**.

Have to deal with individual atoms, photons, spins,…… Problems with control, interconnections, measurements.

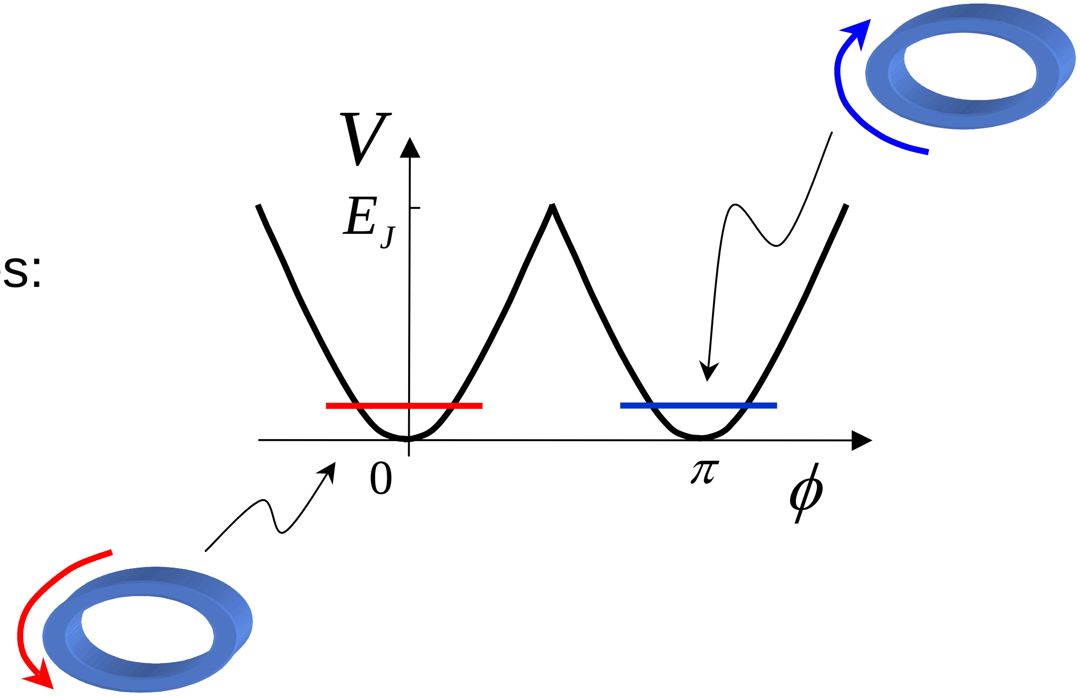
Have to deal with many degrees of freedom. Problems with decoherence.

Superconducting Phase Qubits

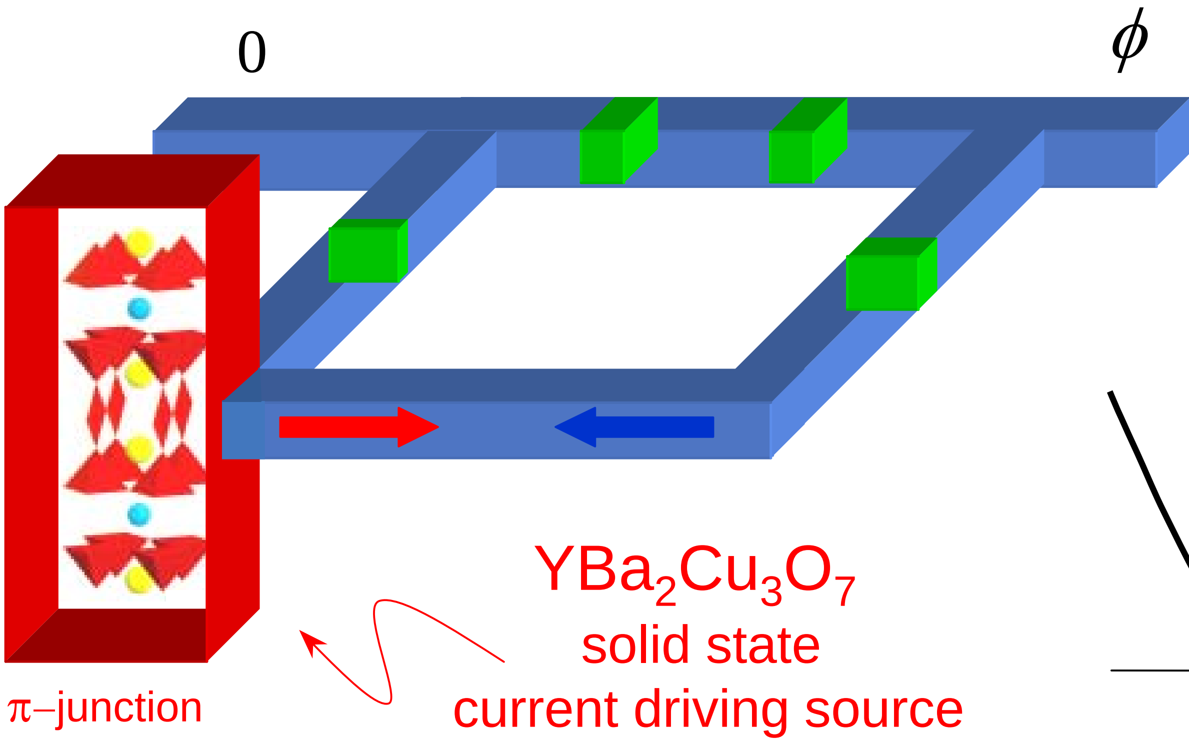


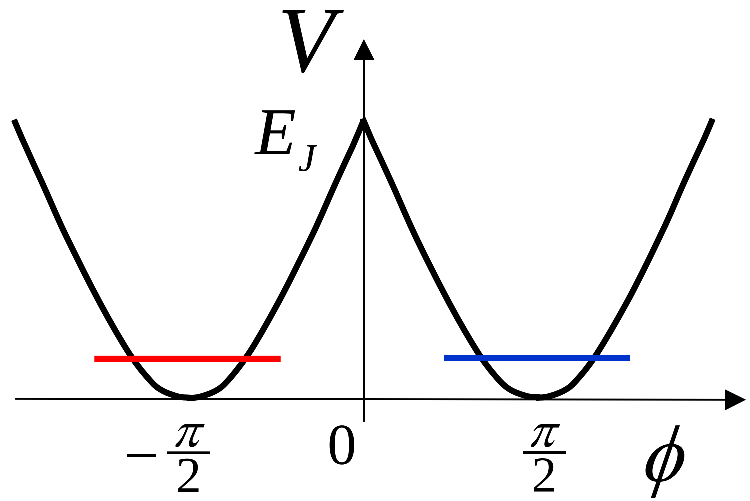
In a superconducting ring, currents do not decay: persistent current states.

Construct a qubit with 2 persistent current states:

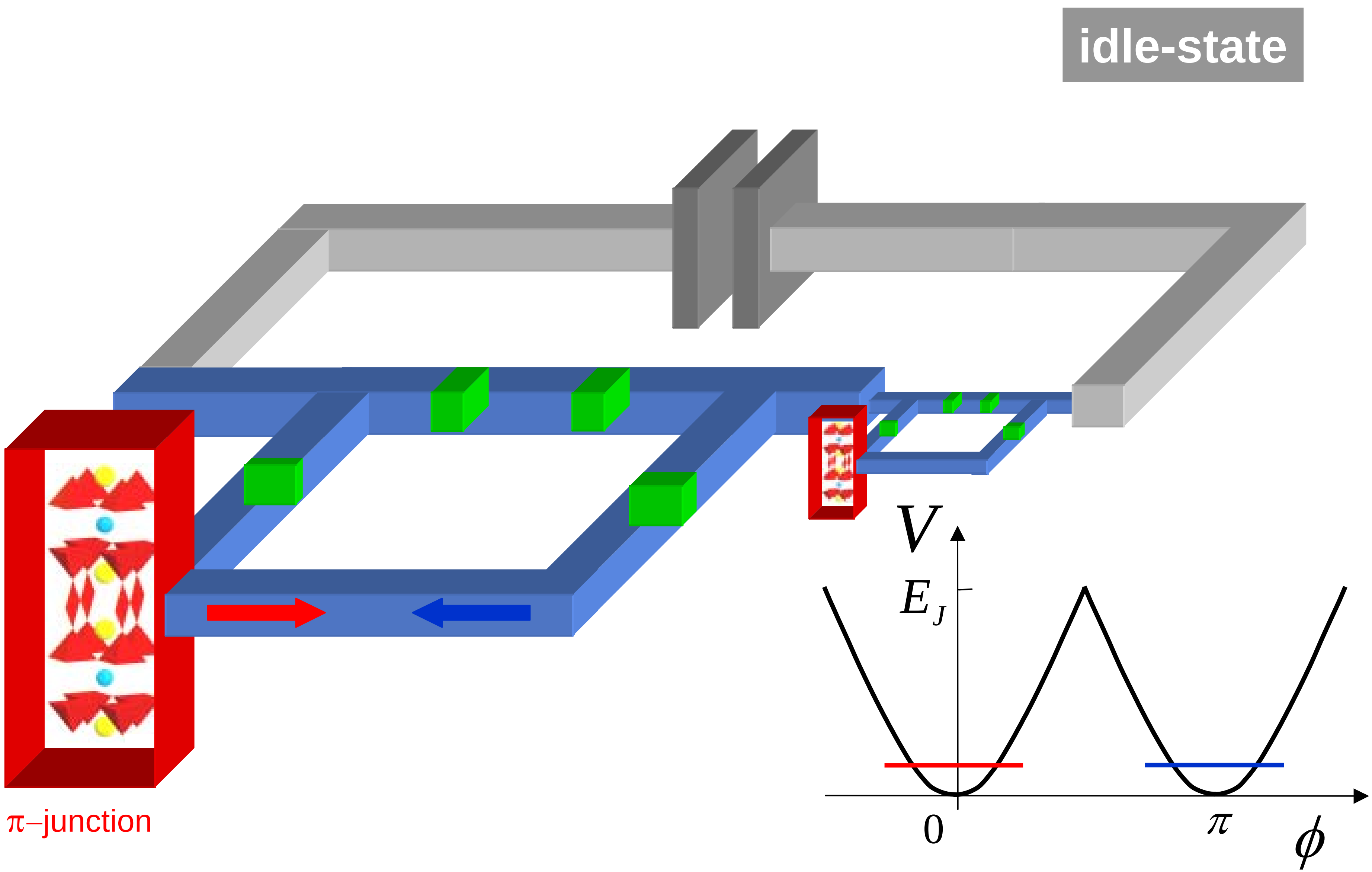


Superconducting Phase Qubits

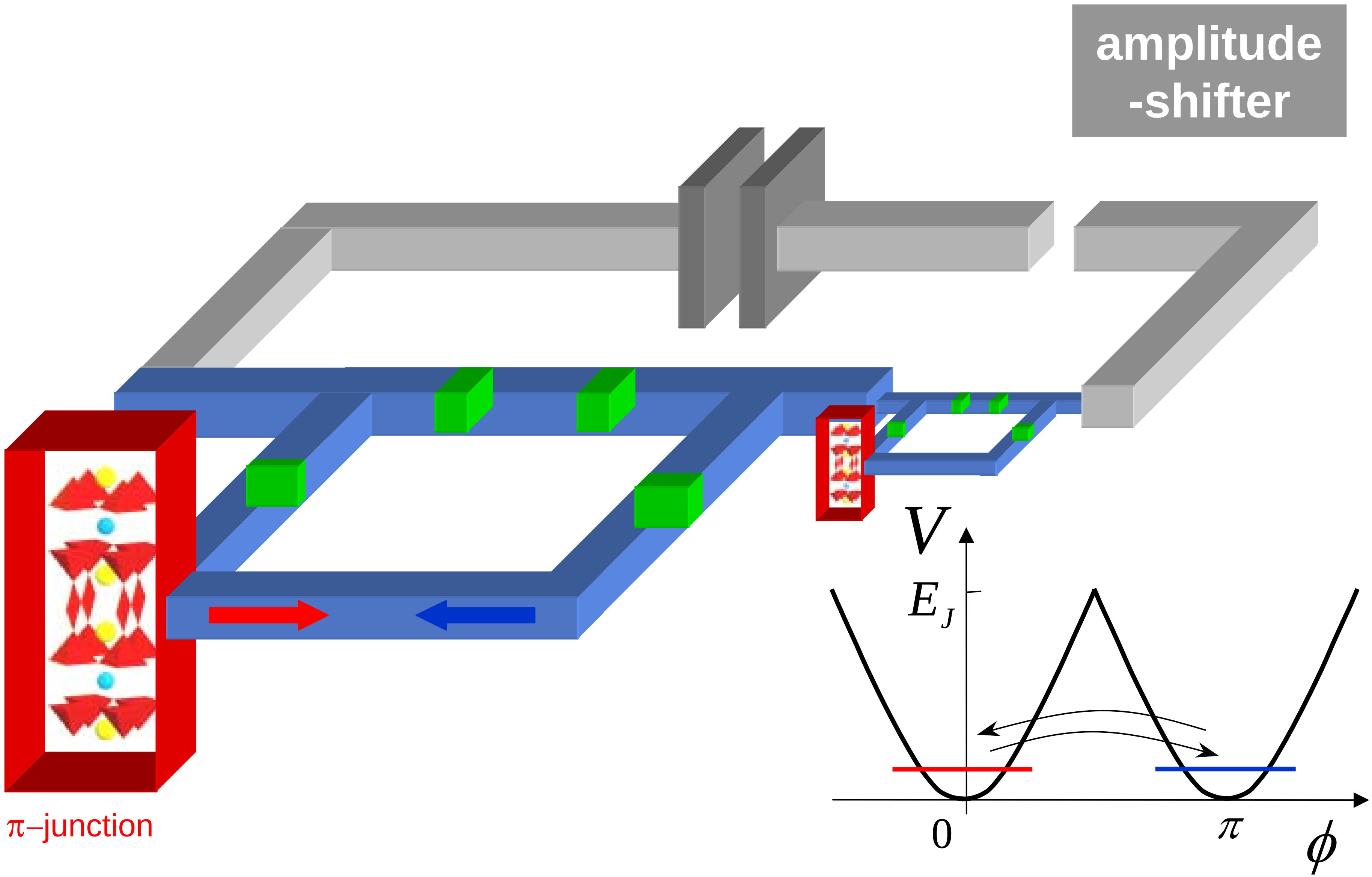




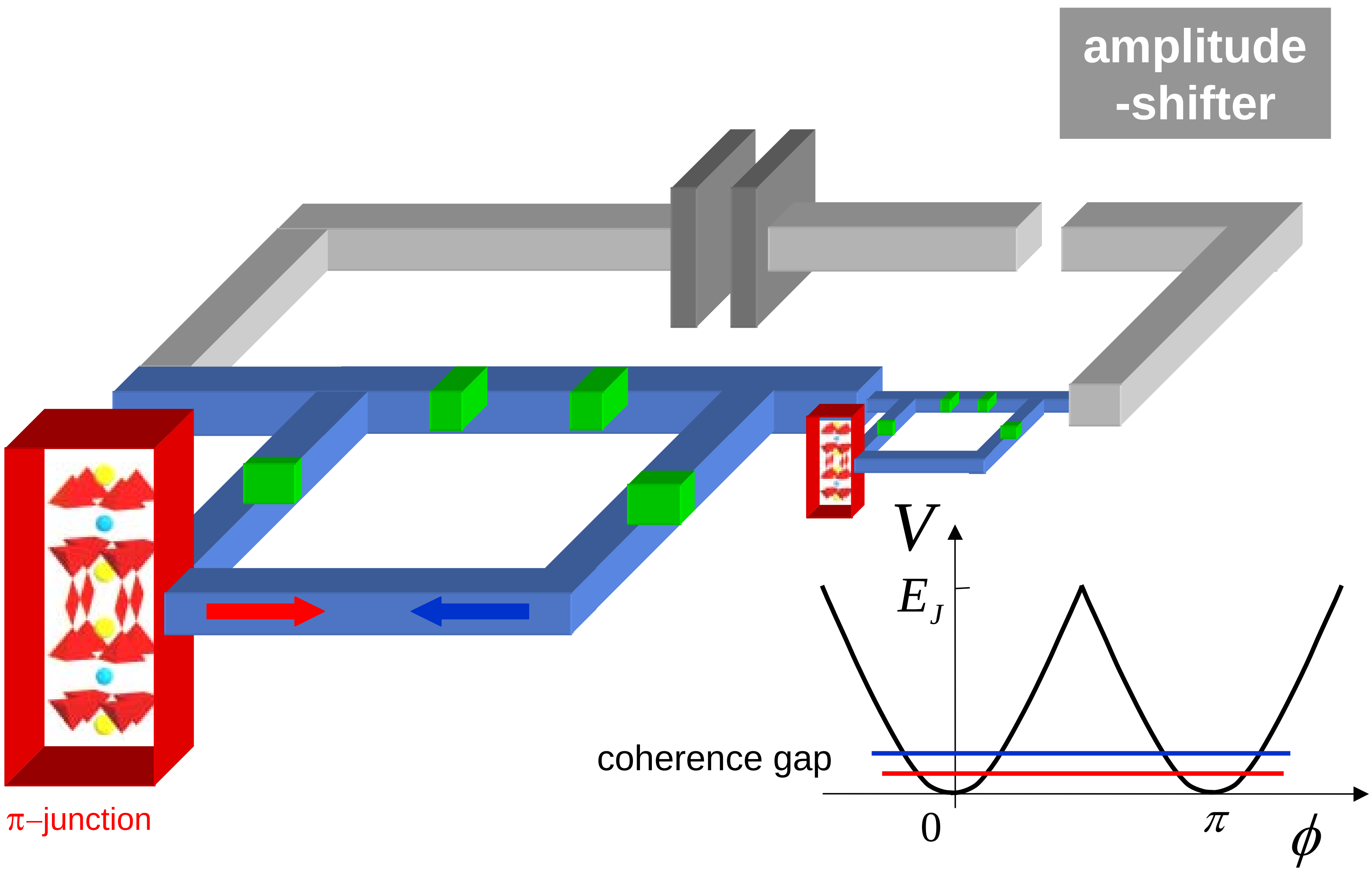
Superconducting Phase Qubits



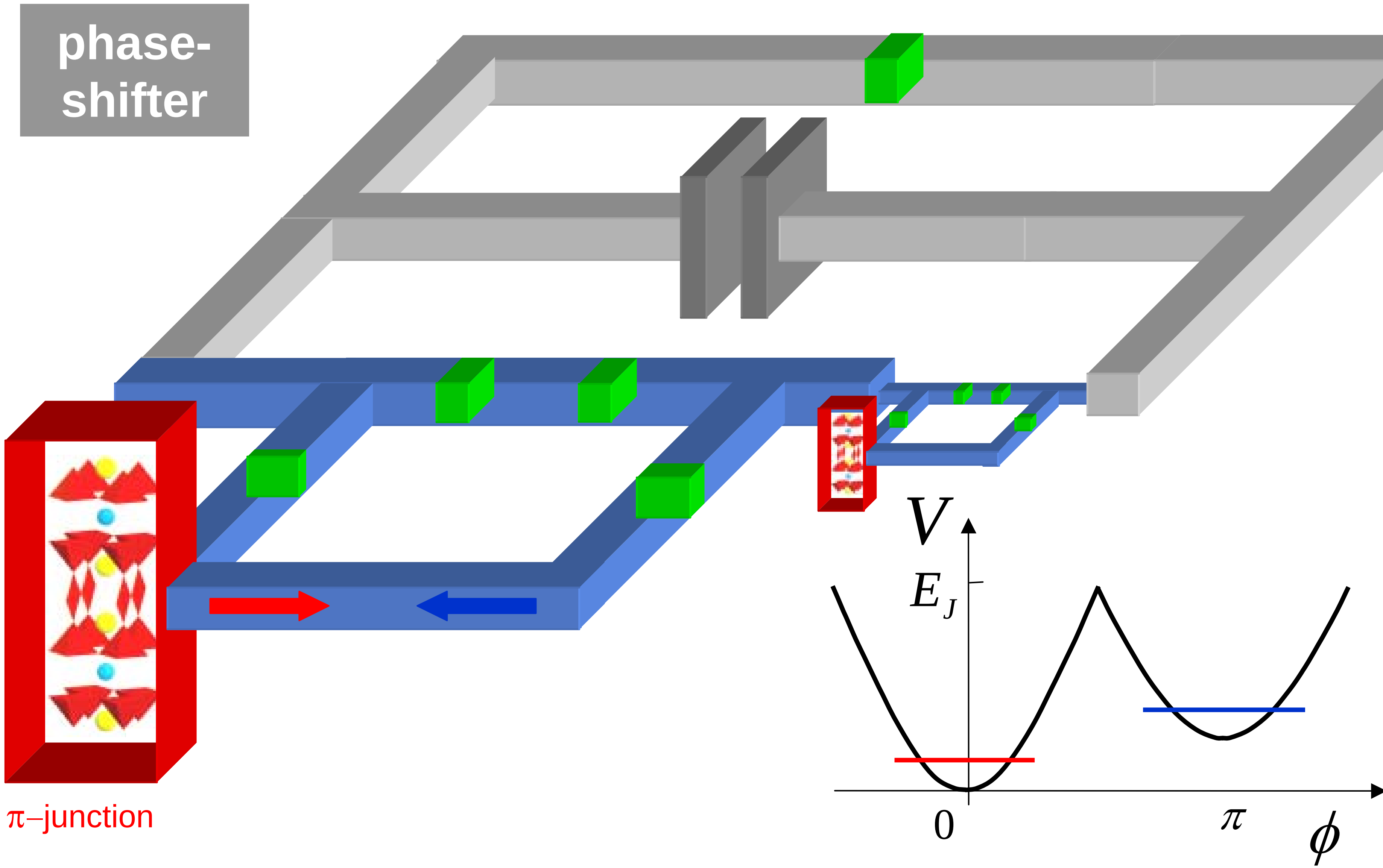
Superconducting Phase Qubits

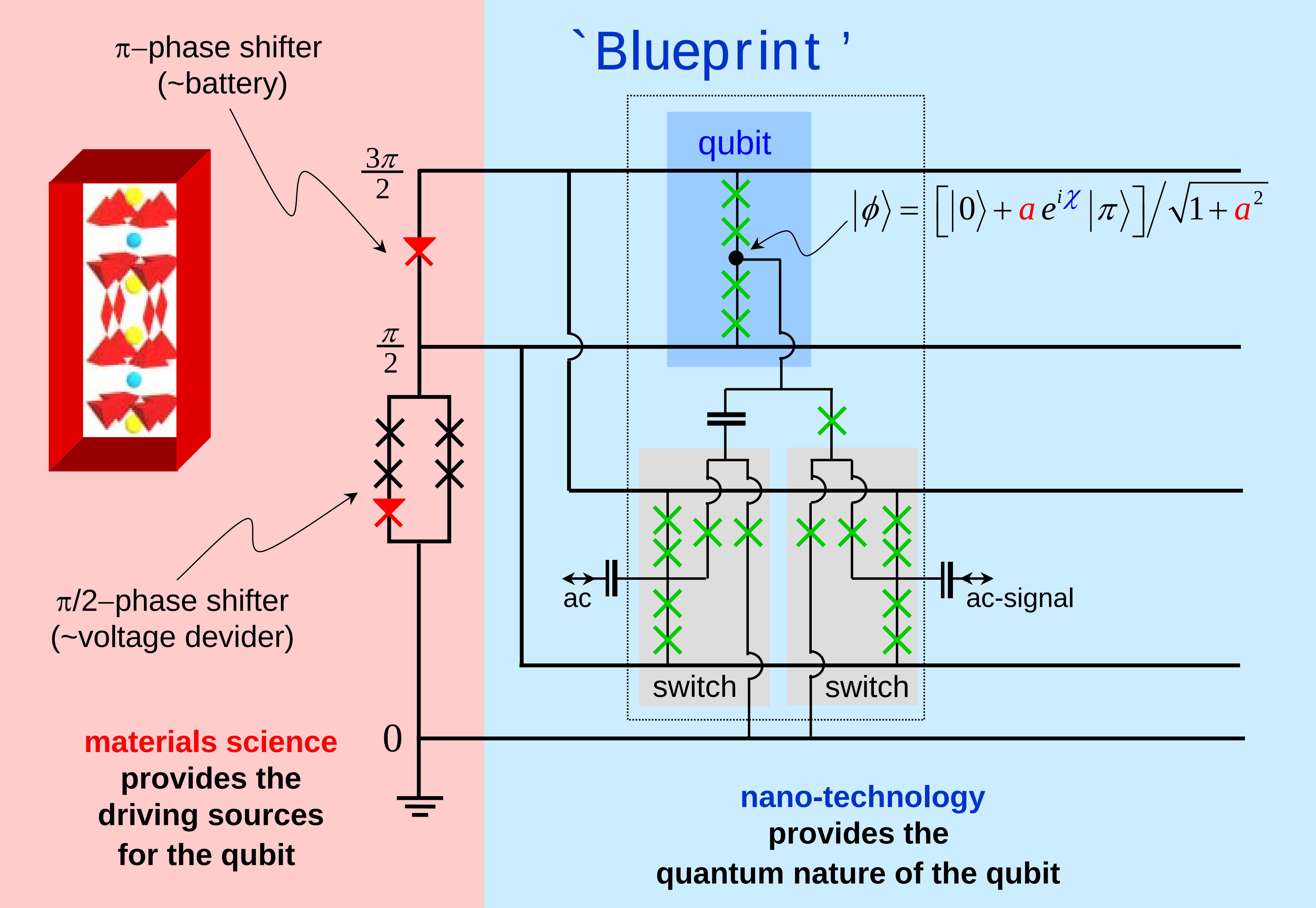


Superconducting Phase Qubits



Superconducting Phase Qubits




`Blueprint '
π–phase shifter
(~battery)
$\frac{3\pi}{2}$
$\frac{\pi}{2}$
0
qubit
$|\phi\rangle = \left[|0\rangle + a\, e^{i\chi}\, |\pi\rangle\right] / \sqrt{1+a^2}$
π/2–phase shifter
(~voltage devider)
ac
ac-signal
switch
switch
materials science
provides the
driving sources
for the qubit
nano-technology
provides the
quantum nature of the qubit

Quantum Computation

Classical computer:

- the information is stored in classical bits, values 0,1
- usual operations NOT, AND, OR
- general purpose device

Quantum computer:

- the information is stored in quantum two-level systems, **qubits**
- **unitary operations**, single- and two-qubit operations (XOR)
- powerful in calculating **specific tasks**

Algorithms:
- prime factorization (Shor)
- data base search (Grover)
- random number generator
- quantum simulation

Applications:
- quantum teleportation
- quantum cryptography

Quantum computation is an interdisciplinary field, with contributions from mathematics, (theoretical) computer science, physics, and chemistry

Implementations:
- Quantum optics
- **Solid state**
- NMR

- **History:** from mechanics to nanoelectronics
- **Information Theory:** Turing machines & complexity
- **Quantum Mechanics:** superpositions & entanglement
- **Quantum Games:** no-cloning, cryptography, teleportation
- **Quantum Bits and Gates**
- **Quantum Algorithms:** Shor’s period finder
- **Hardware:** superconducting phase qubits

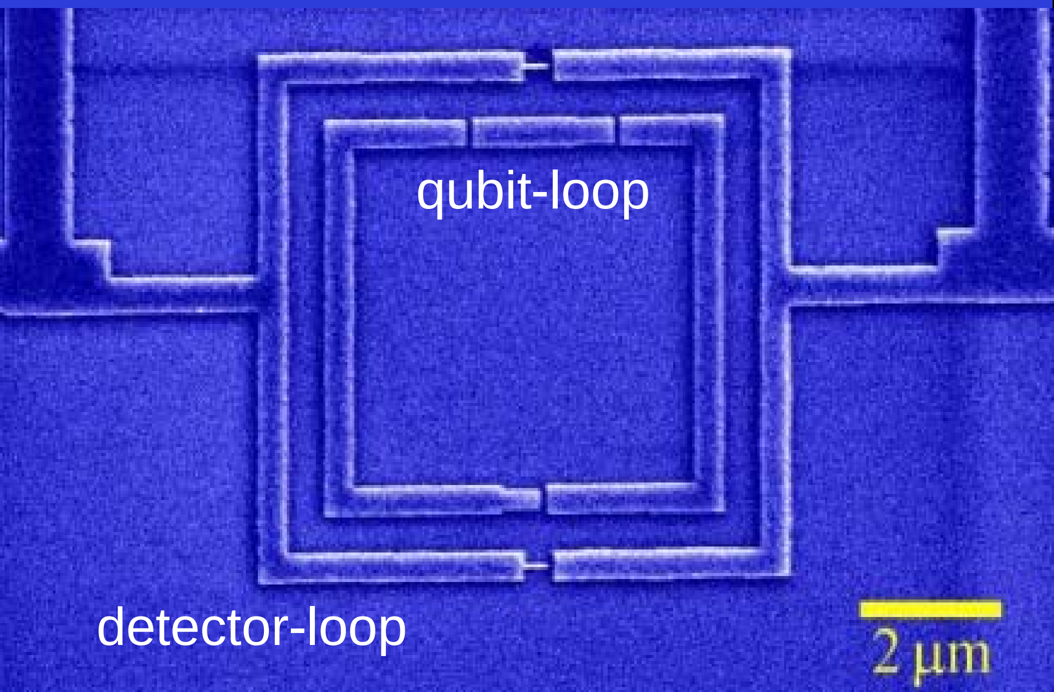
Thanks to

Vadim Geshkenbein
Lev Ioffe
Alban Fauchere
Mikhail Feigel’man
Oskar Hallatschek

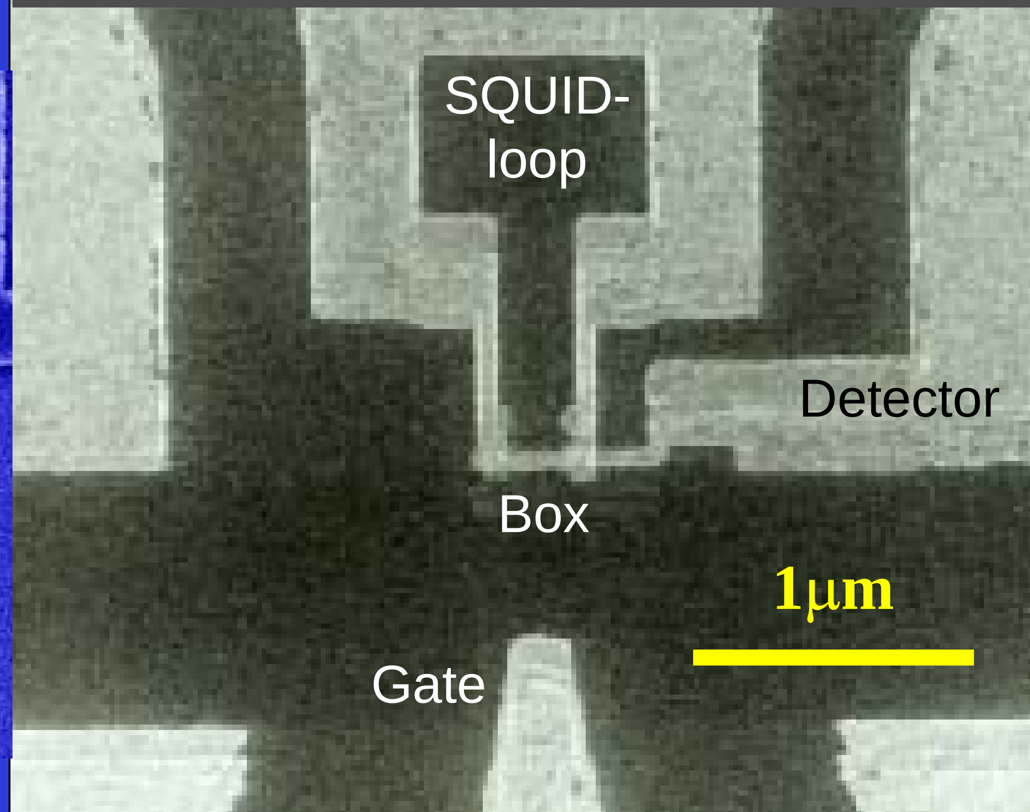
Akira Tonomura
Ulrich Helg
Hanni Hediger
Elmar Heeb

Solid State Qubits: Recent Achievements

Superconducting Phase Qubit
Al–technology,
observation of coherence gap
via *rf*-absorption;
Hans Mooij *et al.*, TU-Delft

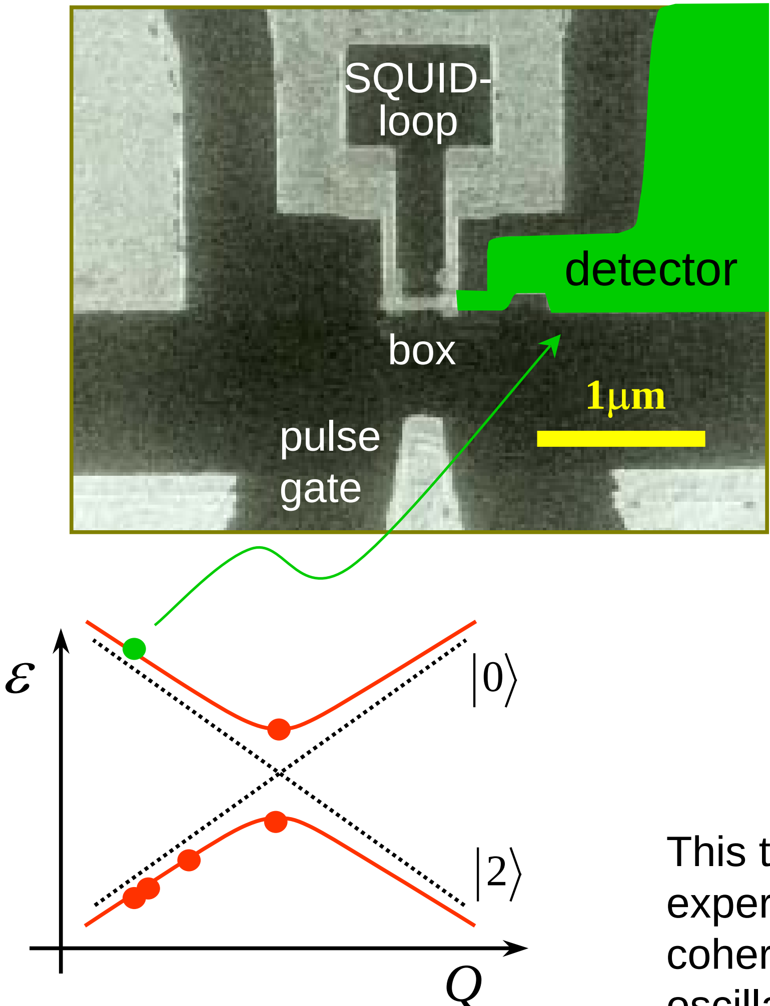


Superconducting Charge Qubit
Al–technology,
observation of coherence gap
via *rf*-absorption and via a
real time experiment;
J. Tsai *et al.*, *NEC* Tsukuba

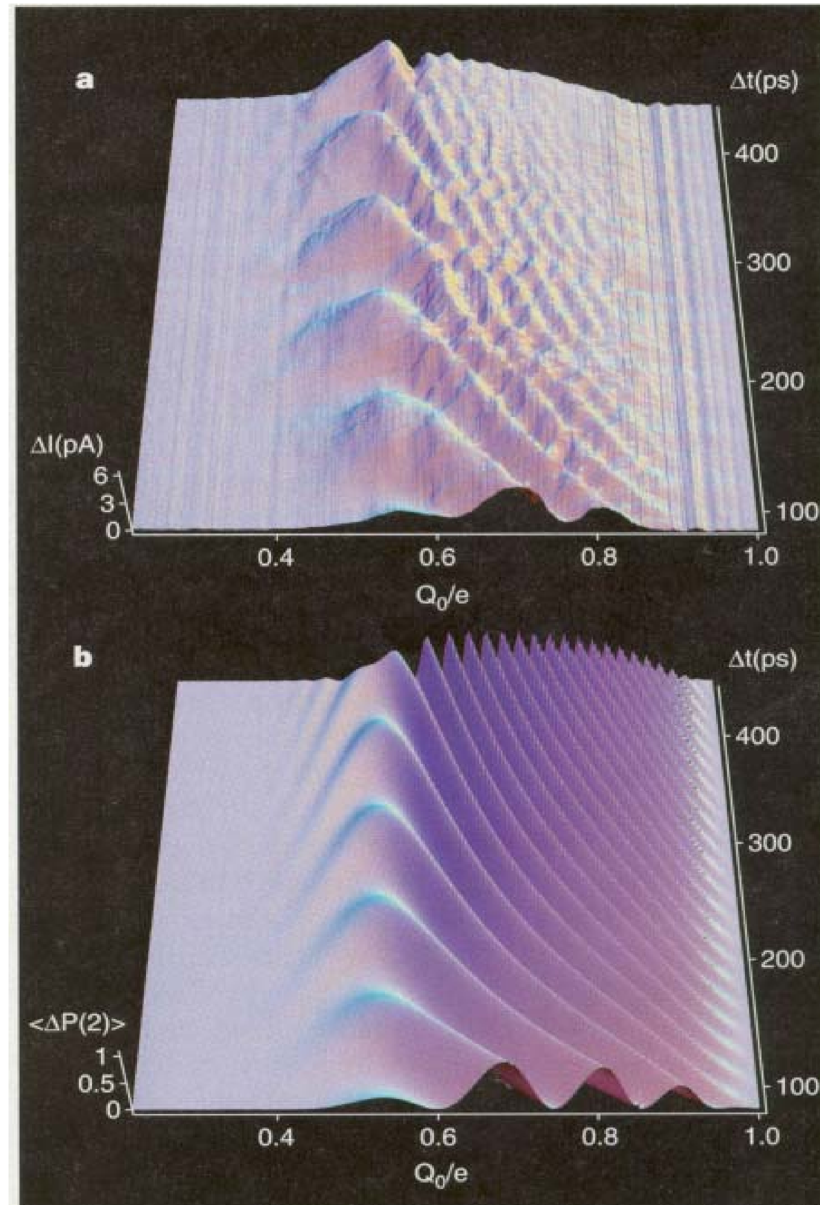


Coherent devices

Charge (Nakamura *et al.*, 1999)

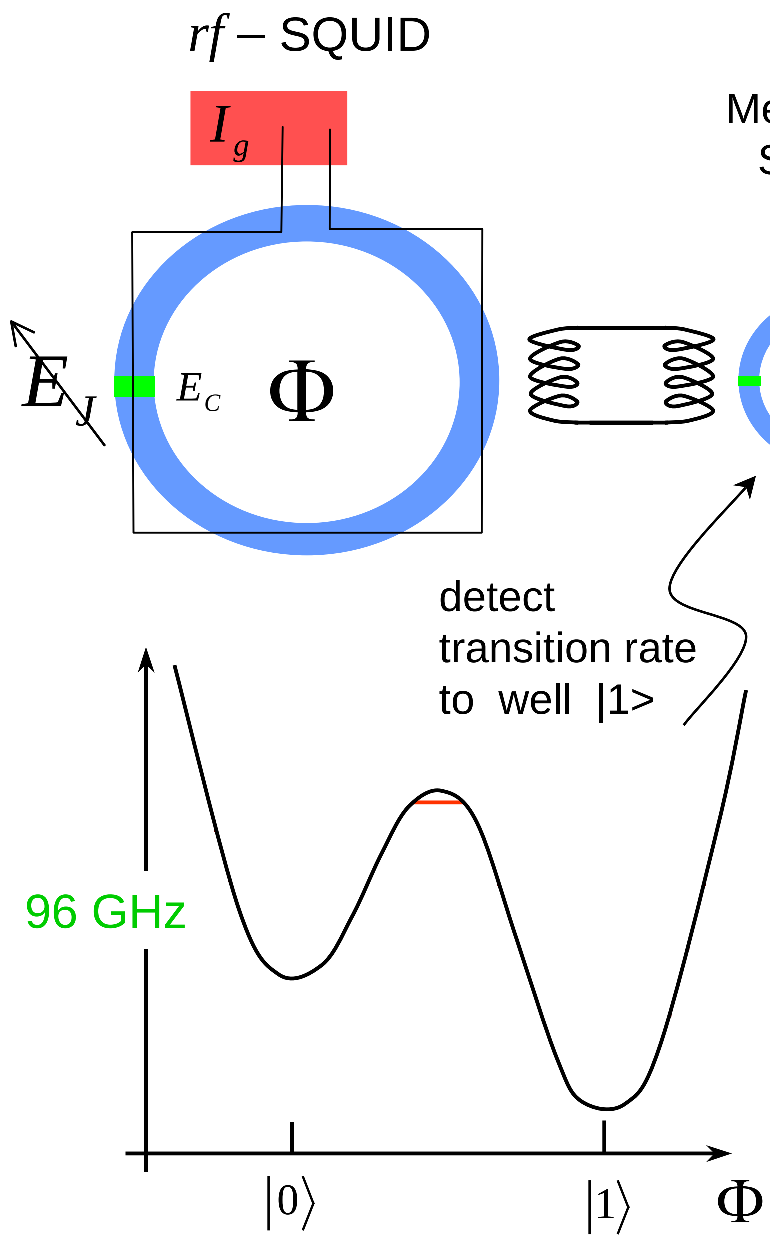


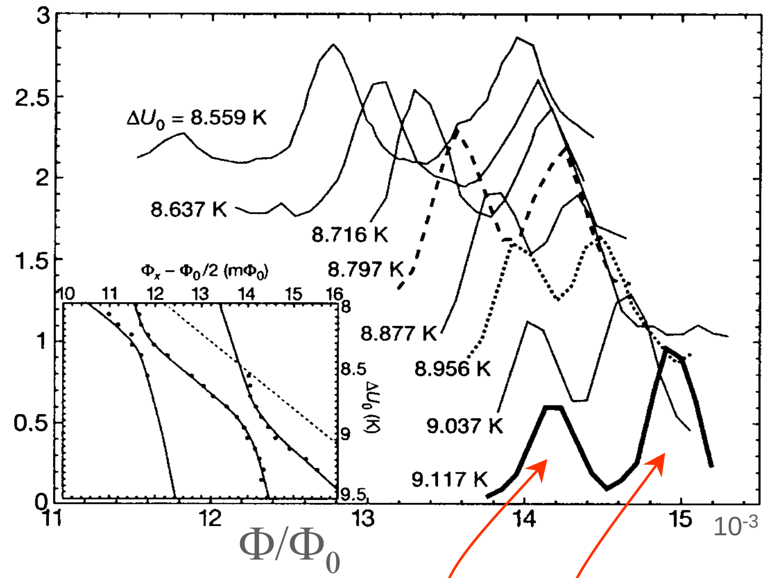
This time domain experiment shows coherent charge oscillations of **50 – 100 ps** duration during a total coherence time of **2 ns**.

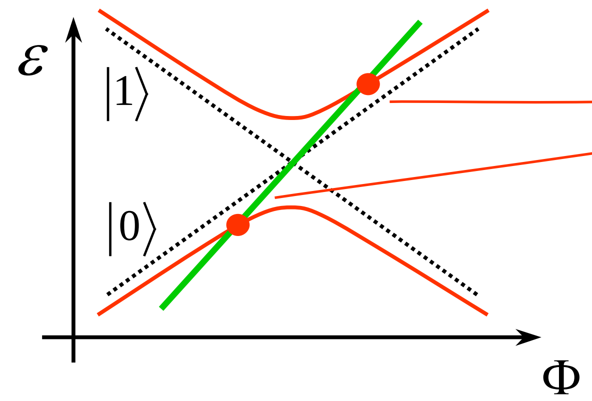


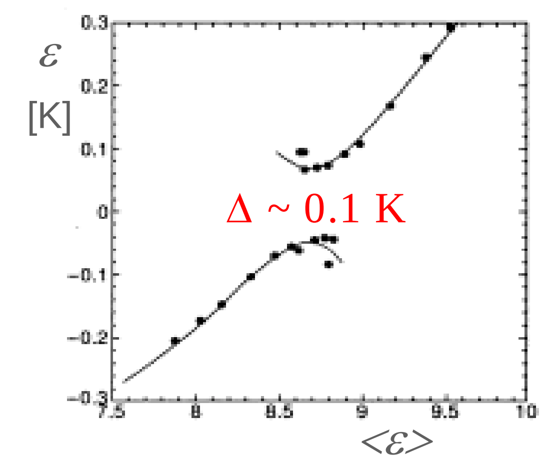
Coherent devices

Flux (Friedman *et al.*, 2000)





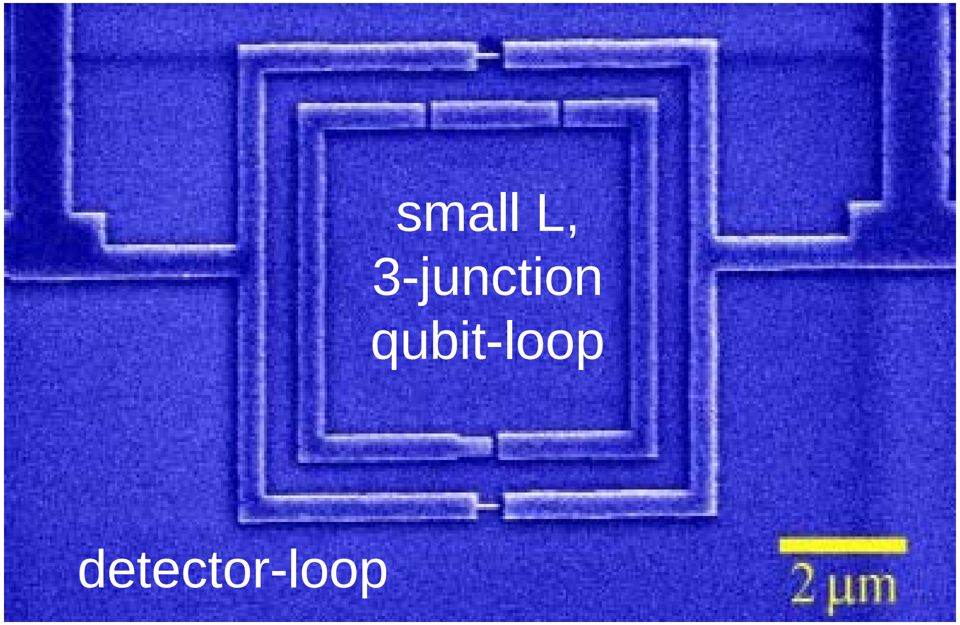




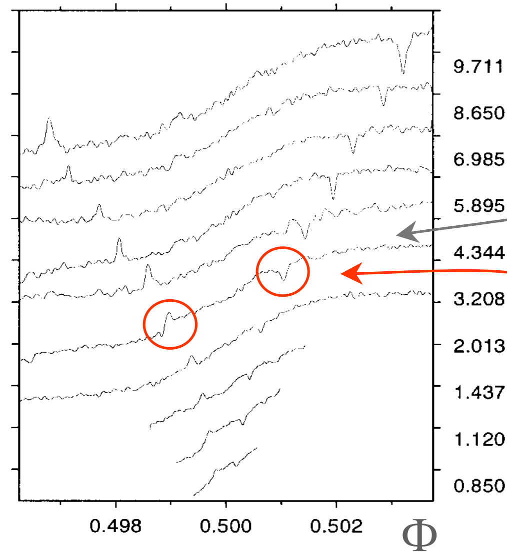
This experiment demonstrates the coherent current oscillation of ~10^9 Cooper pairs producing an oscillating moment of size ~10^{10} μ_B.

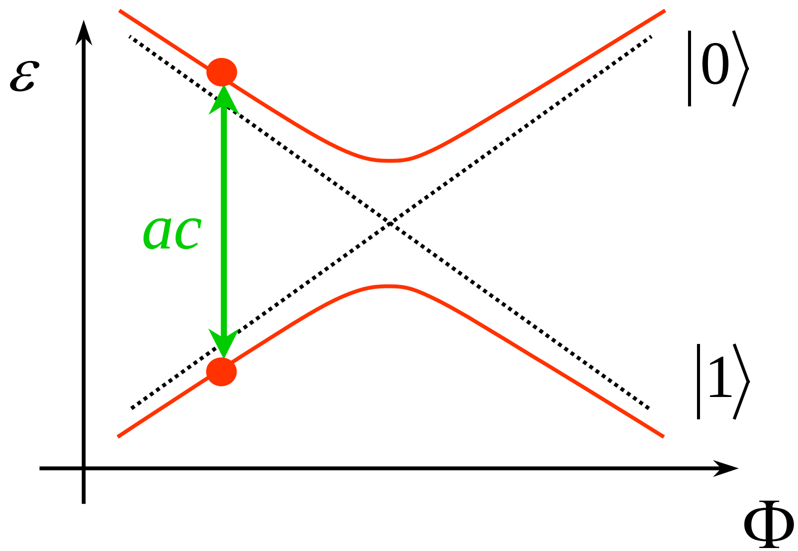
Coherent devices

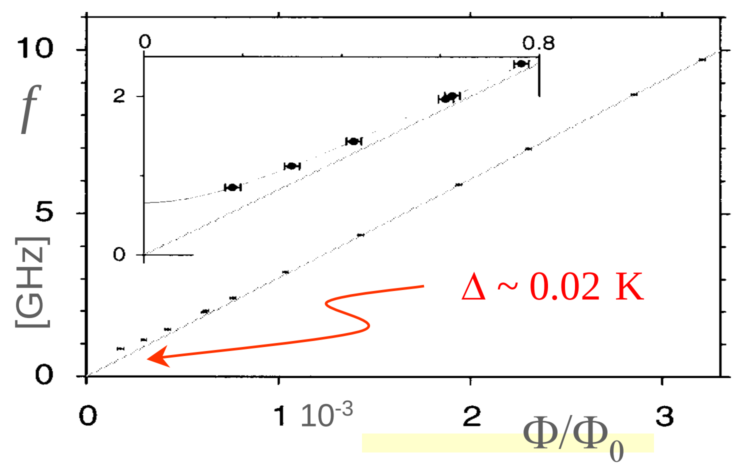
Phase (Mooij *et al.*, 2000)



Scanning flux Φ at different microwave frequencies f







This experiment measures coherent current (0.5 μA) oscillations over ~ 5 cycles.