A Quiz before We Start (Related to today's topic)

- There is a country where thieves are in charge of the postal service. They open all the unlocked packages and steal what is inside, however, they would never touch the packages that have been locked. Bob and Alice are engaged, and Bob wishes to send Alice an engagement ring via the country's postal service. How does Bob send the ring safely to Alice?
- A sturdy locked box would keep the ring from being stolen though, Alice will not be able to open the package without a key. The lock can be obtained at any stores nearby but the key which goes to the lock remains where the sender is; the package receiver does not have the key in this case. If the lock itself is being sent in another package, it has to be locked again to prevent it from being stolen.
- Bob, at his wit's end, called Alice. She evidently came up with a very good idea, i.e., use a box that can have as many locks as possible attached. How did Alice eventually receive the ring safely from Bob?

December 5, 2005
University Lecture
Science of Material

Lecture 6 What is Condensed Matter Physics?

Lecture 7 Quantum Mechanics and Artificial Materials

-- High-tech and the State-of-the-art Physics

Lecture 8 Atom Control and Quantum Control

--Nano-science and Quantum Information

Lecture 9 Diverse Matter and Physical Properties

The University of Tokyo,
The Institute For Solid State Physics

Yasuhiro Iye

Lecture Review (1)

- Quantum mechanics
  - Wave functions, Schrodinger's equation, uncertainty principle, quantum probability.
  - Tunnel effect and quantum interference.
- Quantum interference
  - Young's double-slit experiment.
  - Electron interference experiment.
  - Aharonov-Bohm Effect.

Lecture Review (2)

- Artificial materials: mesoscopic system.
  - High-tech and micro-processing (super LSIs and hard disks).
  - Mesoscopic systems

    Artificial material making and micro-processing.
- Quantum conduction phenomena
  - Conduction electron and electrical conduction.
  - Quantum conductance: $e^2/h = (25.813\text{k}\Omega)^{-1}$

    Quantum point contact and quantum Hall effect.
  - Quantum interference and AB ring.
  - Mono-electron tunnels and quantum dots.

Today's Topics

- Observation and manipulation of atoms

  - STM, AFM and nanoscience
- Macroscopic quantum phenomena
  - Quantum statistics
  - Quantum liquid
  - Bose-Einstein condensation
- Quantum information processing
  - Cryptography
  - Quantum computers
  - Quantum ciphers (private key distribution)

Observation and Manipulation of Atoms

Microscopic Universe

10^{-12} m 10^{-9} m 10^{-6} m 10^{-3} m 1 m

1 pm **Picometer**

1 nm **Nanometer**

1 μm **Micro-meter (Micron)**

1 mm **Millimeter**

Size of atomic nucleus

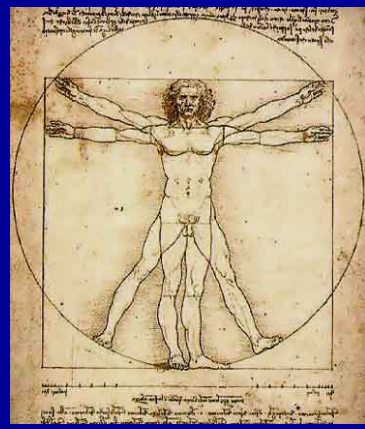
Size of atom

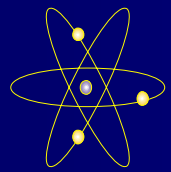
Virus

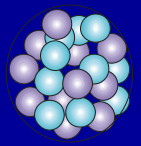
Wavelength of visible light

Bacteria

Needle hole and human hair





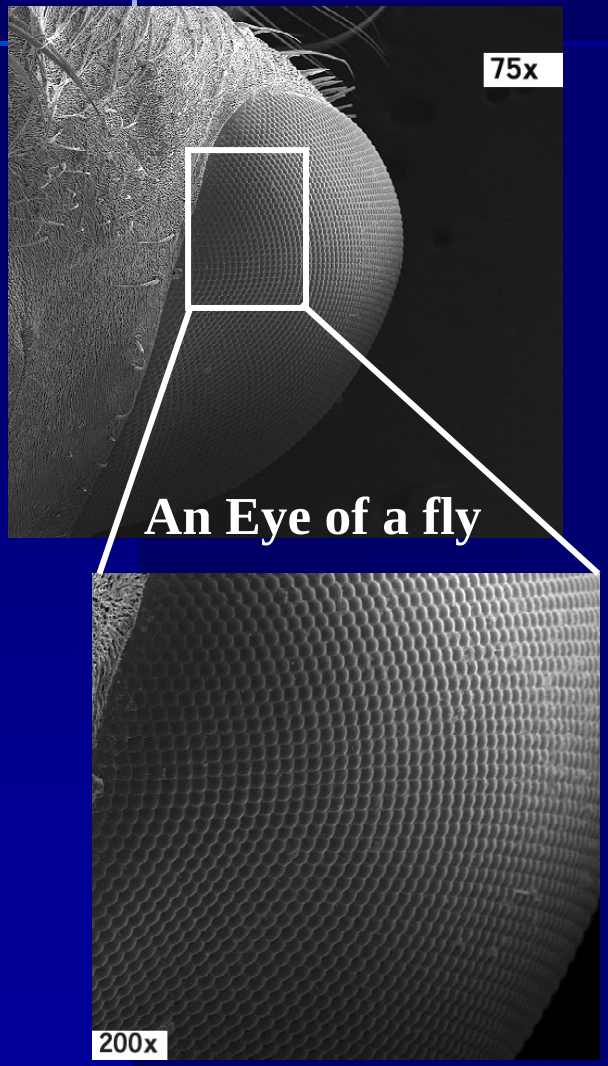


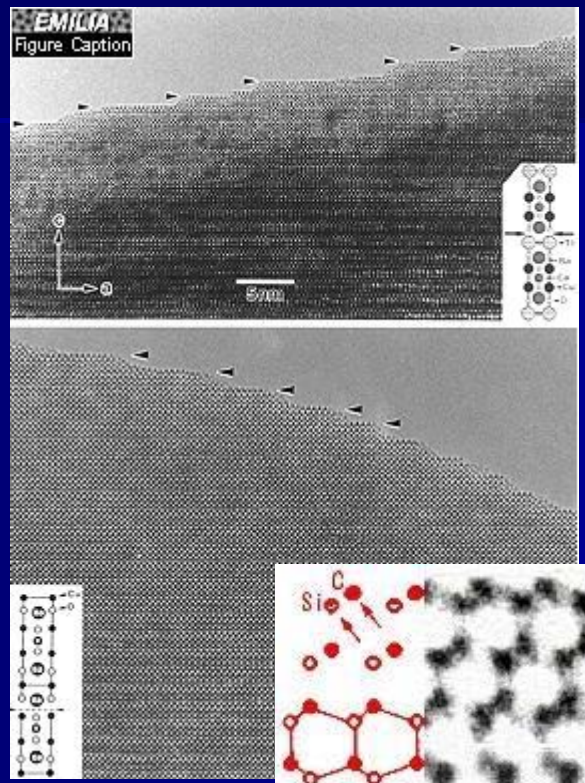
Optical microscope

Electron microscope

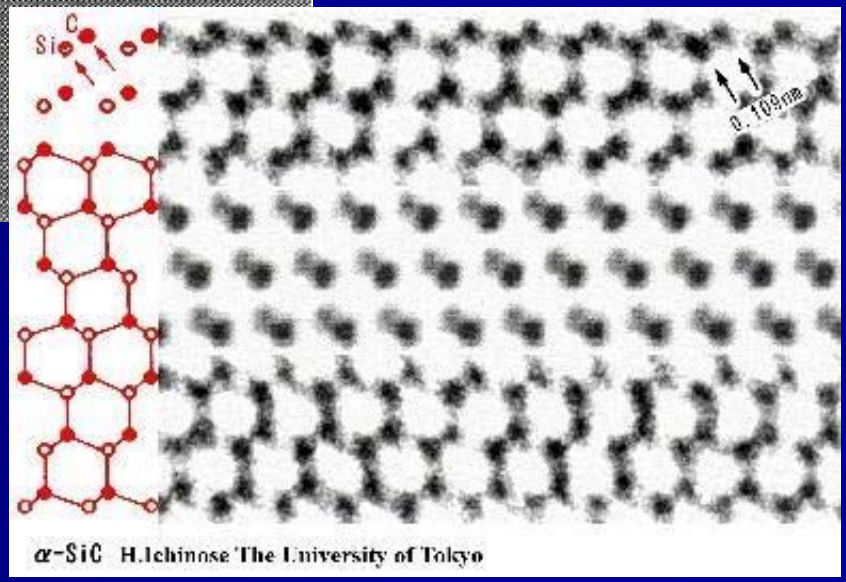
Scattering probe microscope

Observation of Small Structures : Electron Microscopes



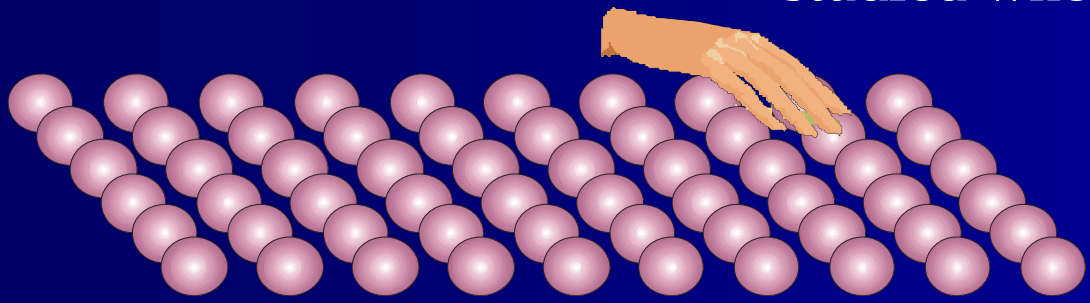


The arrangement of atoms observed by high resolution electron microscope.



Arrangement of Atoms on Solid Body Surfaces

Macroscopic structure can be studied when touched directly by i



Is the same observation possible for structures on an atomic scale?

⇒ "Impossible" may be the likely answer.

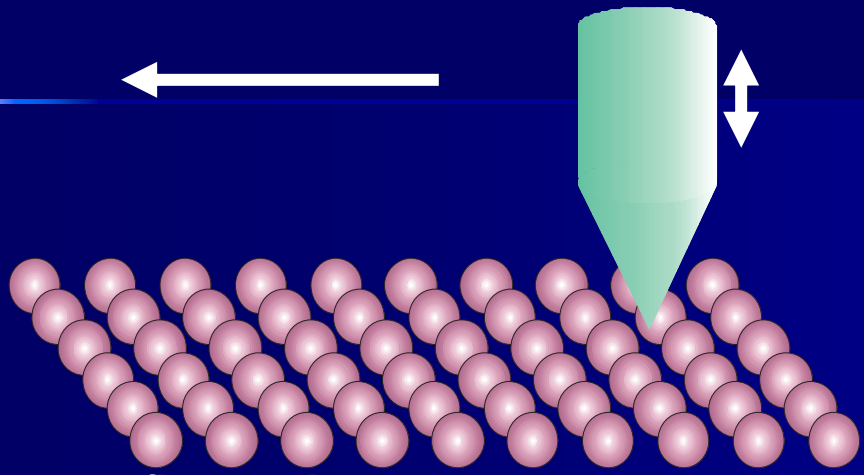
Scanning tunnel microscope

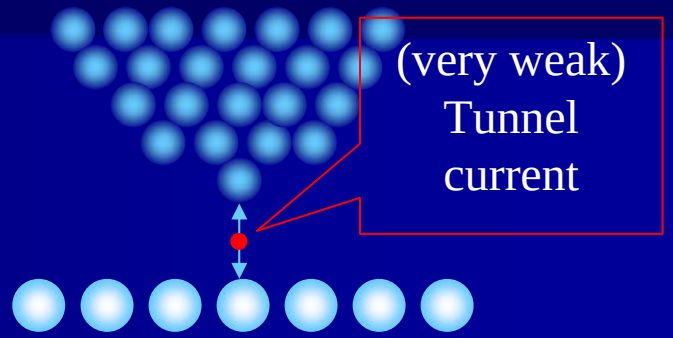
Binning and Rohrer, 1984.

The first image of atomic arrangement on a silicon crystal surface.

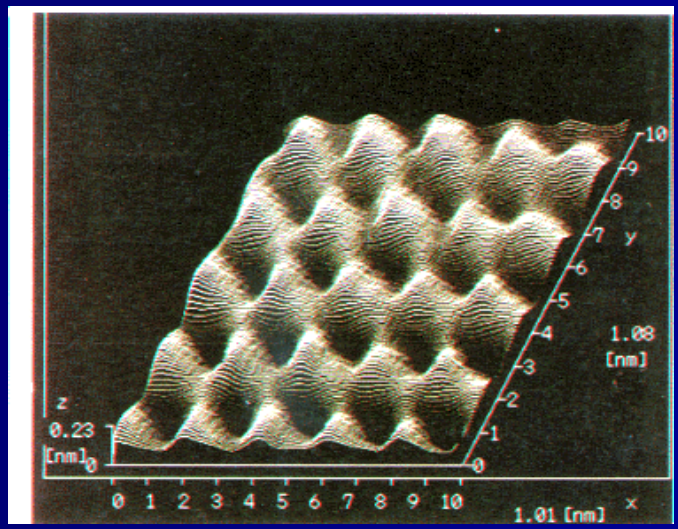
Figure removed due to copyright restrictions.
http://scholar.lib.vt.edu/ejournals/SPT/v8n2/images/hen_lg_fig3.jpg

Scanning Tunnel Microscope (STM)





Tunnel current flows when atoms in the needle tip are brought close to the atoms on the surface by roughly 1nm.
Irregularity of the surface on an atomic scale can be observed by moving the needle vertically while moving it horizontally at the same time to adjust the tunnel current to stay constant.

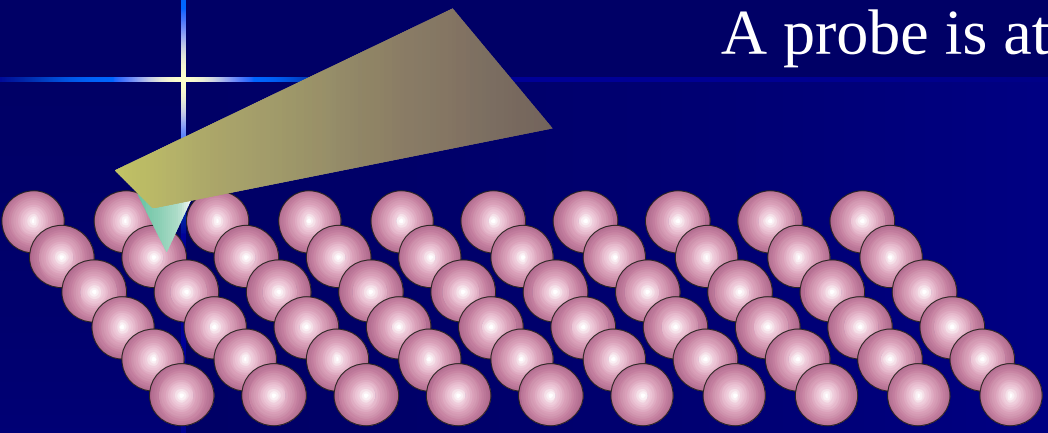


Stability problem
Mechanical vibra
Electrical noise

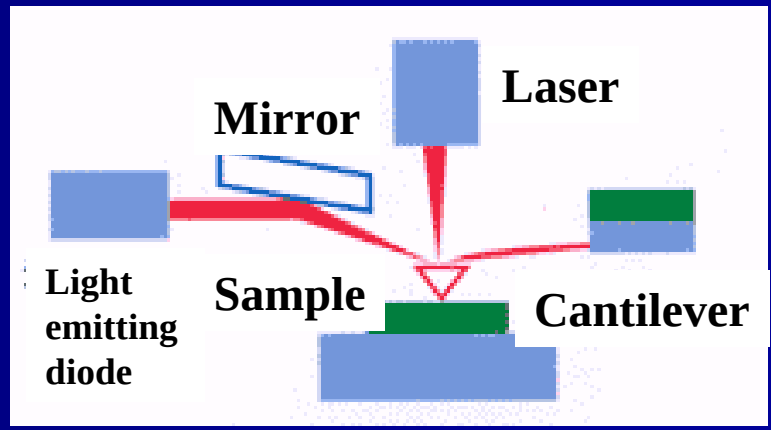
Aoyama Laboratory, The University of Electro-Communications
& Iwata Laboratory, Shizuoka University ‡

Atomic Force Microscope (AFM)

A probe is attached to the tip of a cantilever.

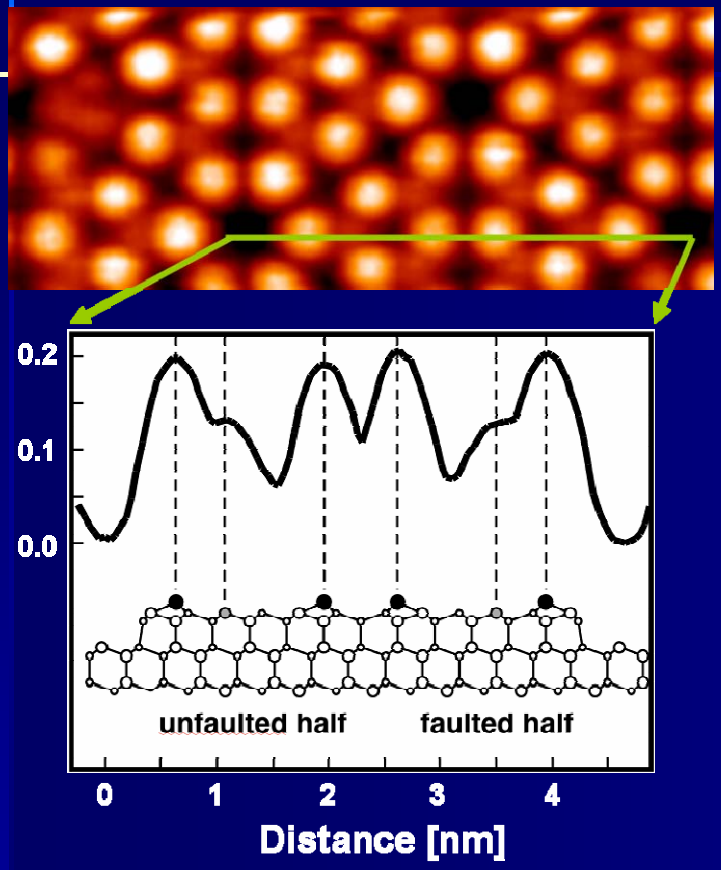


The forces between the atoms in the probe tip and the atoms on the surface are detected.

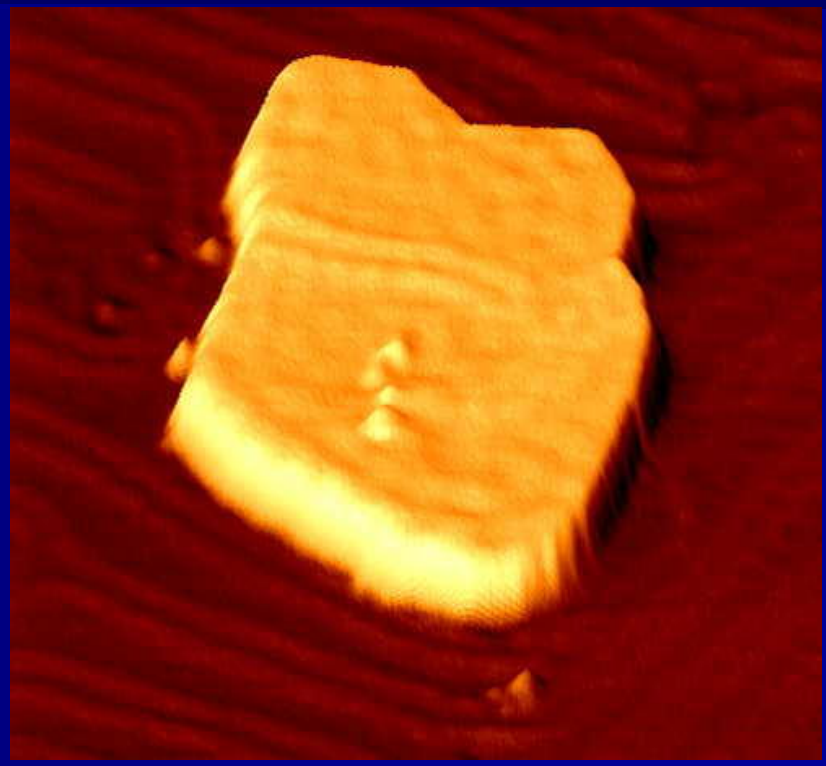


The condition of the bending of the cantilever is detected by a reflected laser beam.

Surface Observation by Scanning Probe Microscope



NC-AFM



STM

The Institute for Solid State Physics, Hasegawa Laboratory ‡

Manipulation of Atoms

IBM Almaden Research Center
Don Eigler, head of the research team.

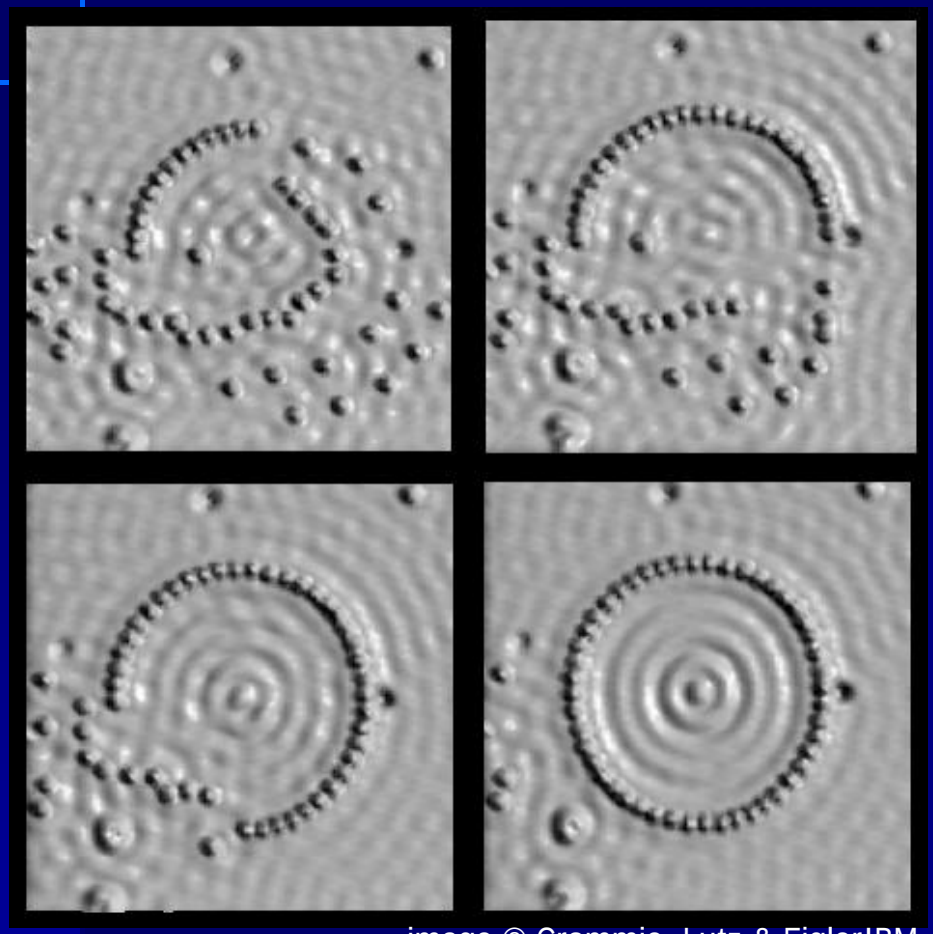


image © Crommie, Lutz & EiglerIBM

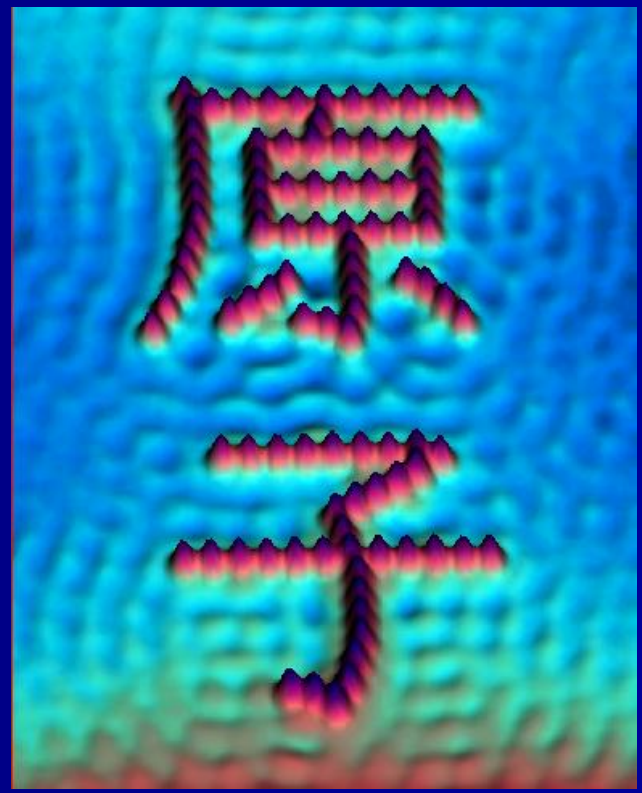


image © Lutz & Eigler IBM

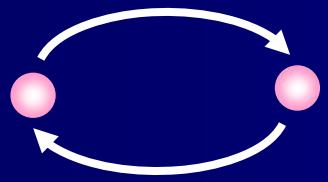
Iron atoms are placed on a copper surface.
The ripple pattern occures by wave interference of the surface electrons.

Macroscopic Quantum Phenomenon

Quantum-mechanical Particles

Quantum-mechanical particles of the same type cannot be discriminated.

Even though the exchange between two particles of the same type may occur, it simply goes back to the same initial state.
(However, the wave function is expressed with the numerical factor in general.)



$$\Psi(\mathrm{b,a}) = C\,\Psi(\mathrm{a,b})$$

$$\Psi(\mathrm{a,b}) = C\,\Psi(\mathrm{b,a}) = C^2 Y\,\Psi(\mathrm{a,b})$$

$$\Rightarrow \quad C^2 = 1$$

$$\Rightarrow \quad C = 1 \quad \text{or} \quad -1$$

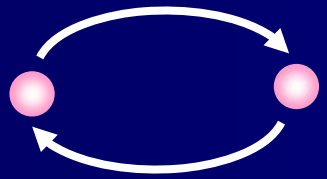
Boson

Fermion

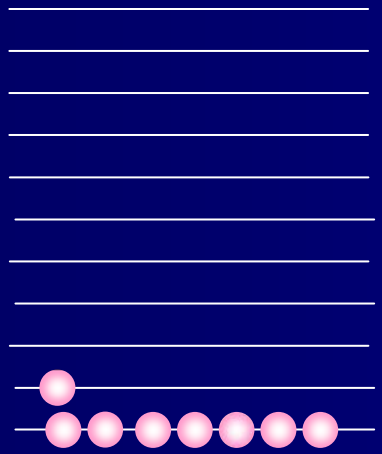
Quantum Statistics

Bose particle (Boson)

Spin: 0, 1, …



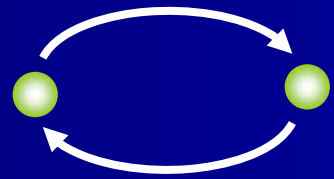
$$\Psi(b,a) = \Psi(a,b)$$



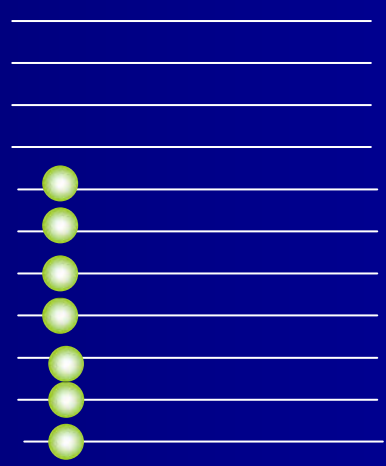
Many particles can be filled in the same state.

Fermi particle (Fermion)

Spin: 1/2, 3/2, …



$$\Psi(b,a) = -\Psi(a,b)$$



Let a=b,

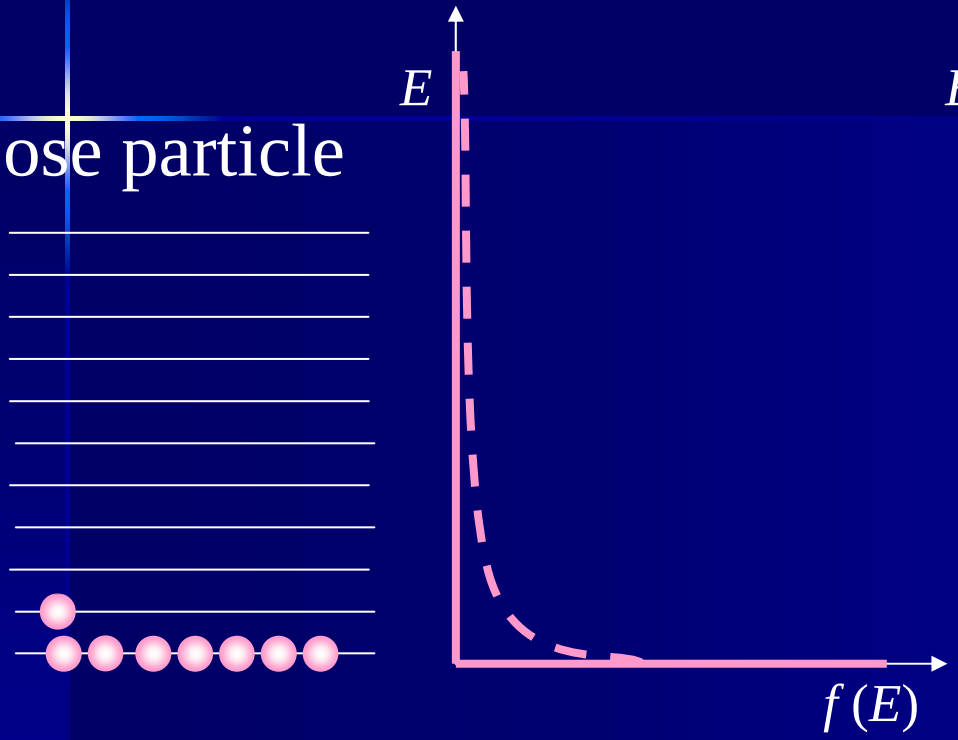
$$\Psi(a,a) = -\Psi(a,a)$$

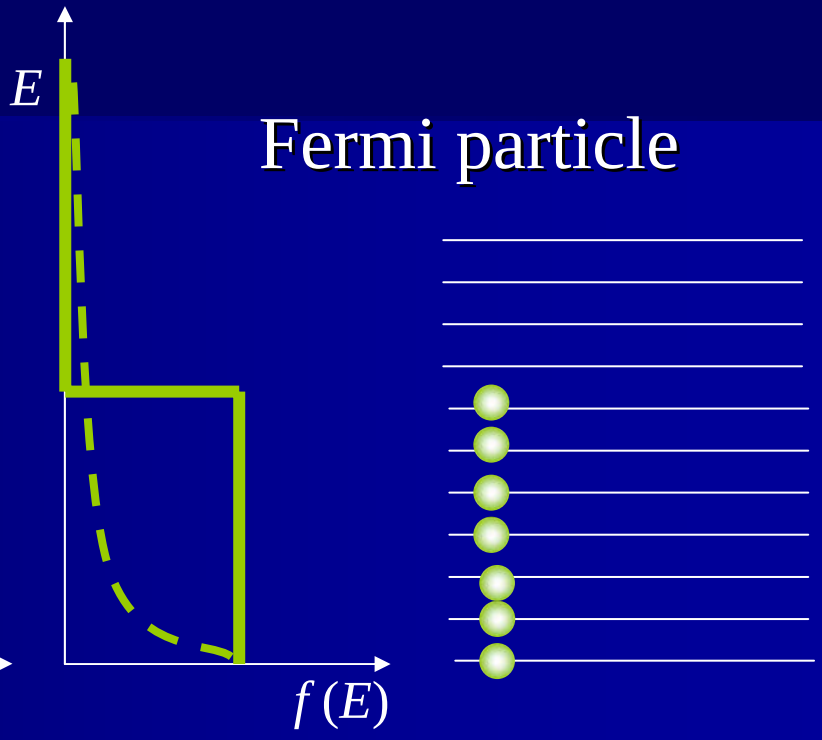
$$\Rightarrow \Psi(a,a) = 0$$

There is only one particle allowed to fill in each state. (Pauli exclusion principle)

Bose-Einstein Distribution and Fermi-Dirac Distribution

Bose particle





Fermi particle

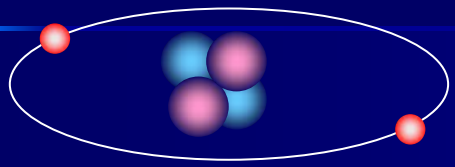
$$f_{\mathrm{BE}}(E) = \frac{1}{e^{(E-\mu)/k_{\mathrm{B}}T} - 1}$$

$$f_{\mathrm{FD}}(E) = \frac{1}{e^{(E-\mu)/k_{\mathrm{B}}T} + 1}$$

The distribution approaches to Maxwell-Boltzmann distribution at a limit of high temperature.

$$f(E) = e^{-(E-\mu)/k_{\mathrm{B}}T}$$

Isotopes of Helium

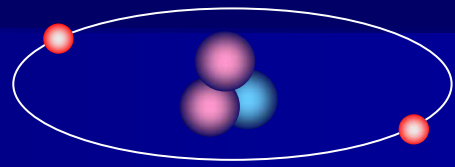


^{4}He

Proton: two
Neutron: two
Electron: two

Total spin = 0

Boson



^{3}He

Proton: two
Neutron: one
Electron: two

Total spin = 1/2

Fermion

Preparation of Very Low Temperatures

Very low temperatures are required in observation of phenomena that are valid quantum statistically.

The internal structure of a liquid helium vessel.

Liquid nitrogen: 77K

Liquid helium (^{4}He): 4.2K

Pressure reduction by vacuum pump: ~ 1.2K

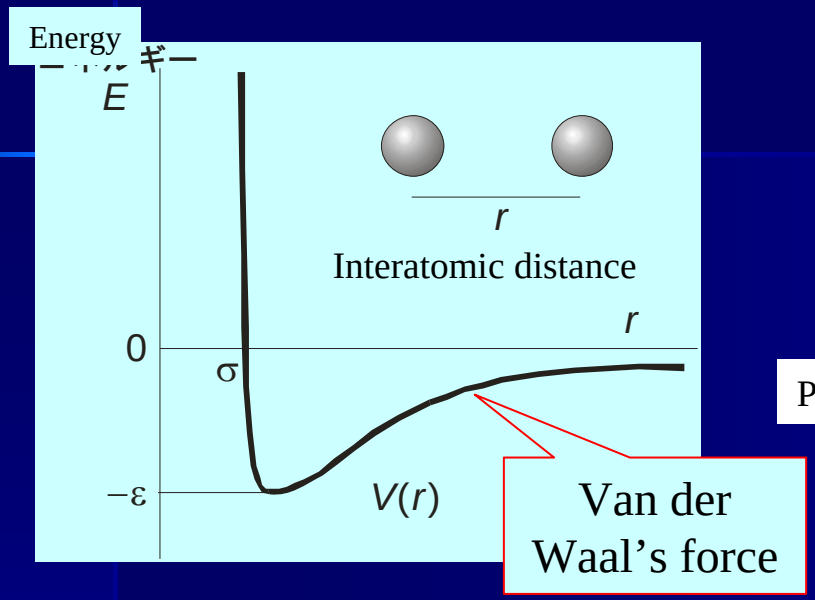
Liquid helium 3 (^{3}He): 3.2K

Pressure reduction by vacuum pump: ~ 0.3K

^{3}He-^{4}He dilution refrigerator: ~ mK

Nuclear adiabatic demagnetization: ~ μK

Helium Phase Diagram

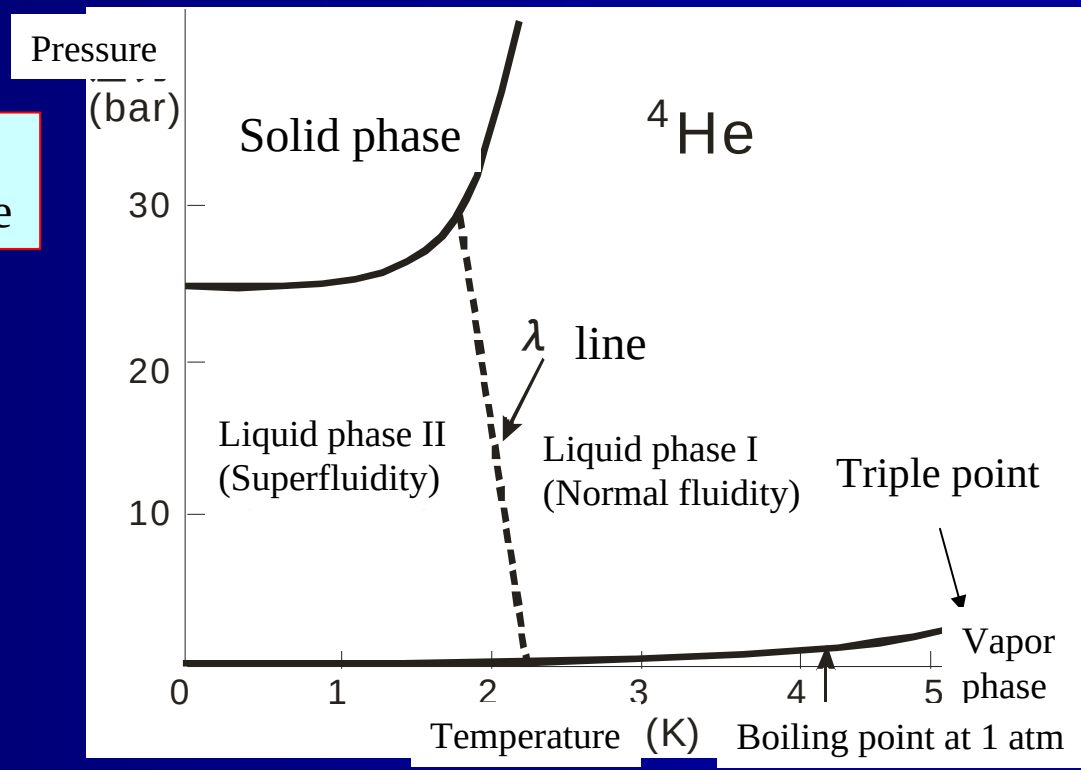


Under normal pressure, helium will not form a solid state even at absolute zero.

⇒ Quantum liquid

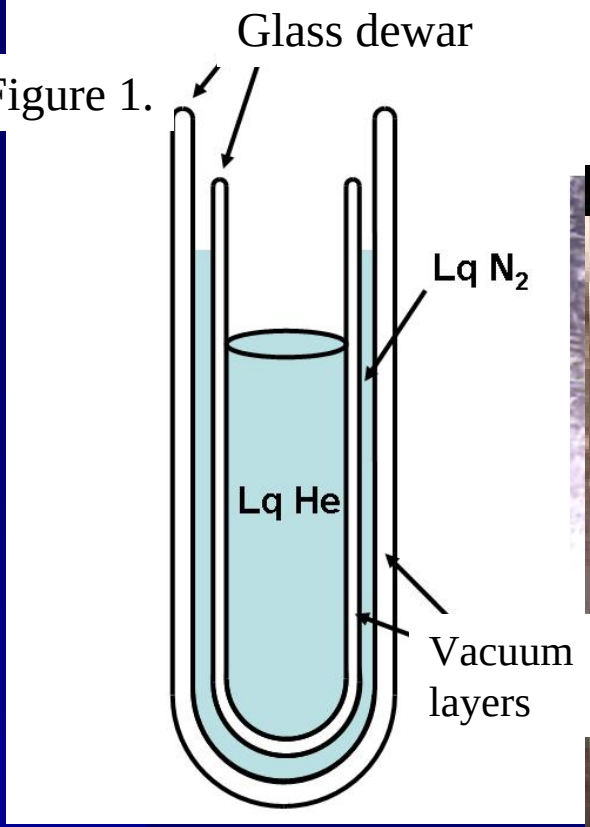
Helium atoms have
(1) Small weight
(2) Weak interaction

Kinetic energy
> Interacting energy



Superfluidity of Liquid Helium

Figure 1.



The University of Tokyo,
Cryogenic Research Center

‡

Superfluidity of Liquid Helium

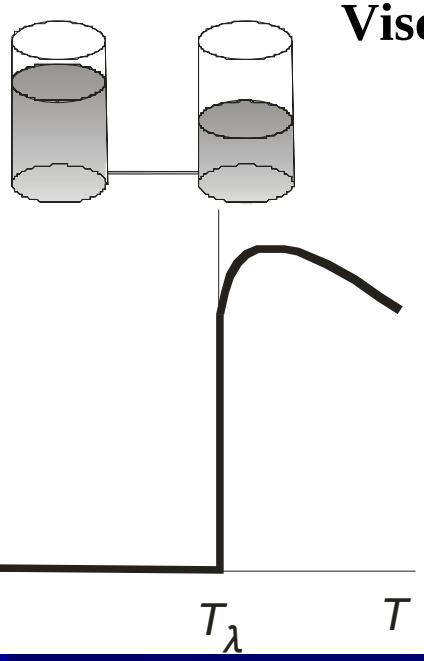
Binary fluid model

Superfluidity components＋Normal fluidity components

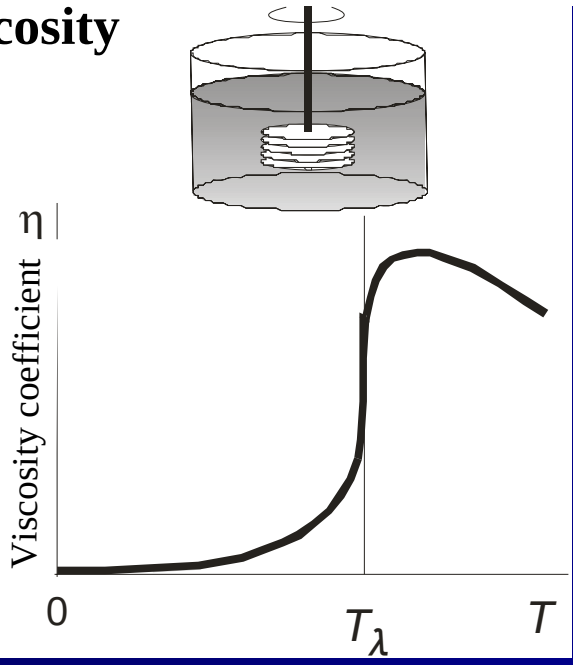
$$\rho = \rho_s + \rho_n$$

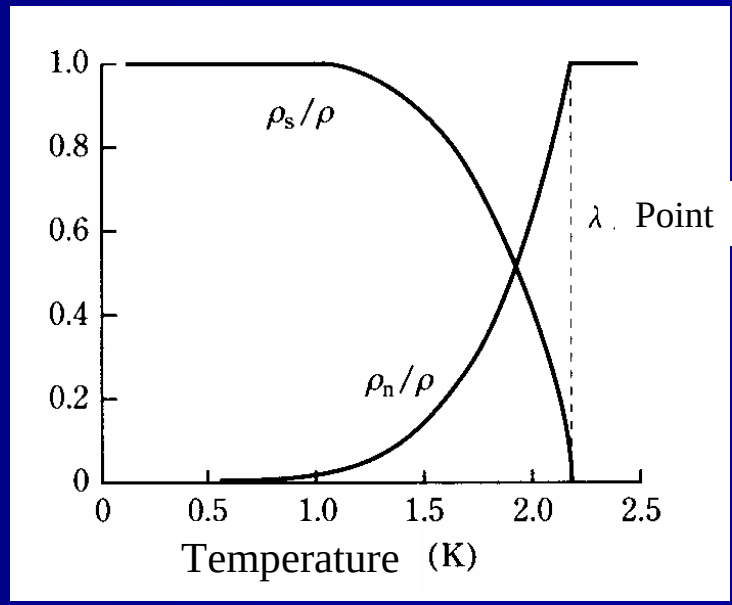
Viscosity

Flow in the canaliculi



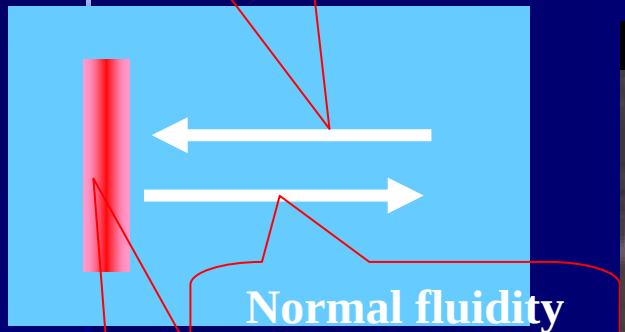
Torsional vibration damping

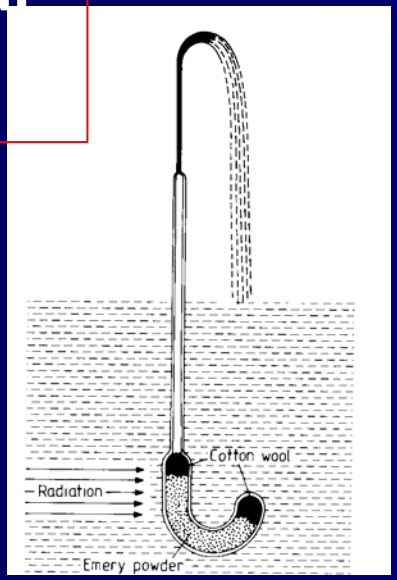




The Fountain Effect

Mechanocaloric effect (internal convection)





The University of Tokyo,
Cryogenic Research Center

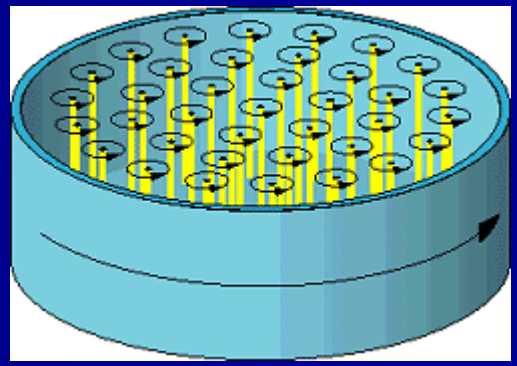
Quantum Vortexes

Macroscopic wave function $\Psi = \Psi_0 e^{i\theta}$

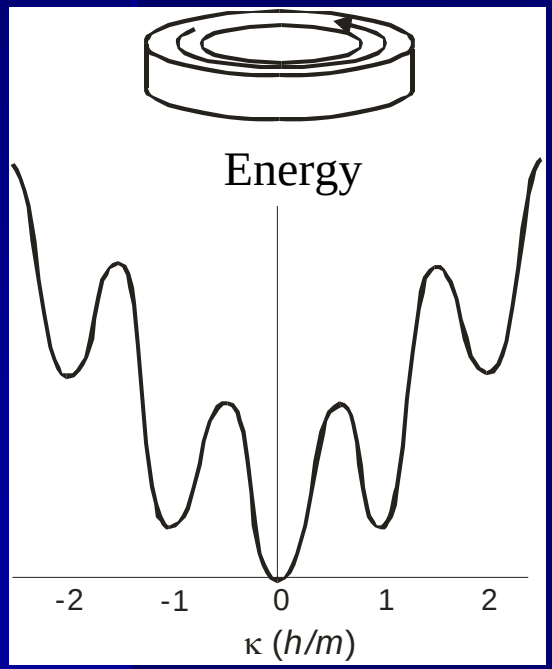
Quantization of circulation

$$\kappa \equiv \oint_C \mathbf{v}_s \cdot d\mathbf{s} = \frac{\hbar}{m}\oint_C \nabla\theta \cdot d\mathbf{s} = \frac{\hbar}{m} 2\pi m = n\frac{h}{m}$$

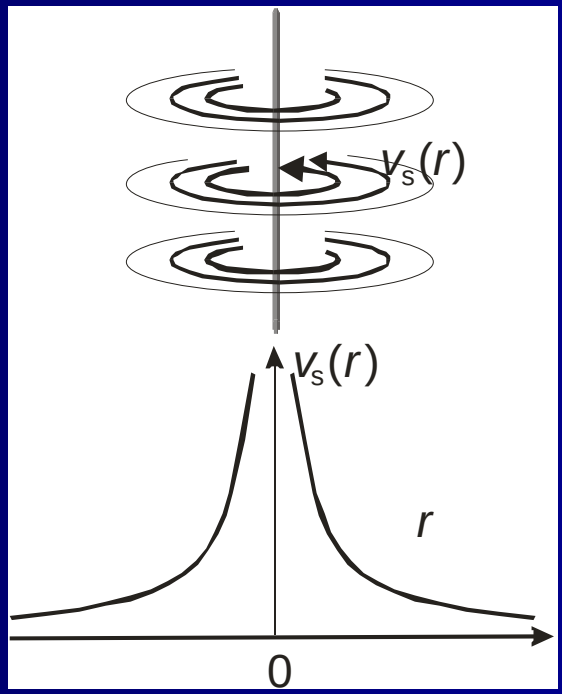
Rotating bucket experiment

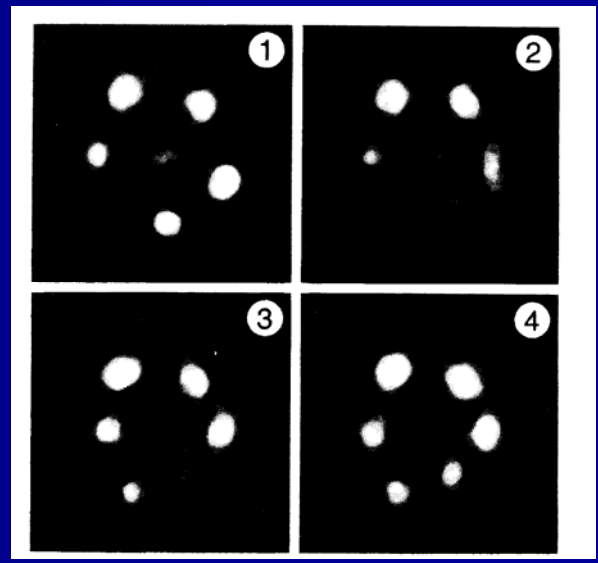


Persistent current

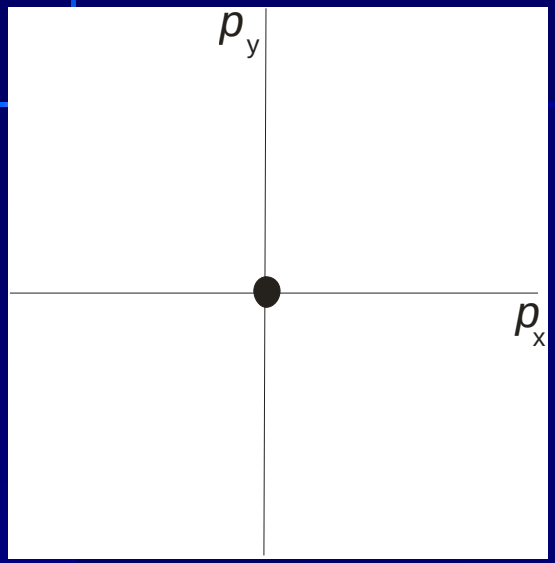


Quantum vortex string

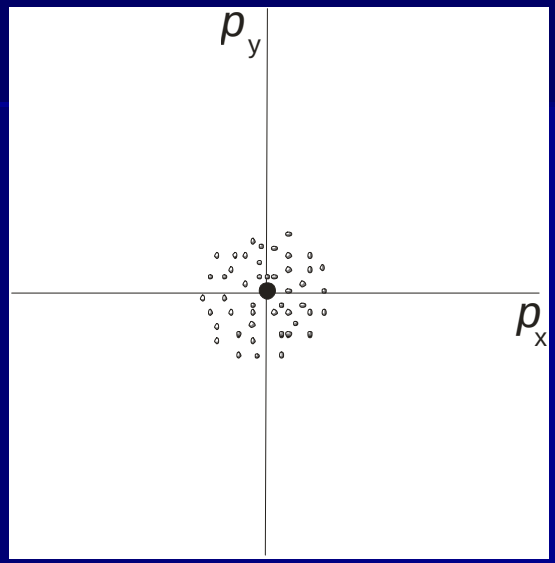




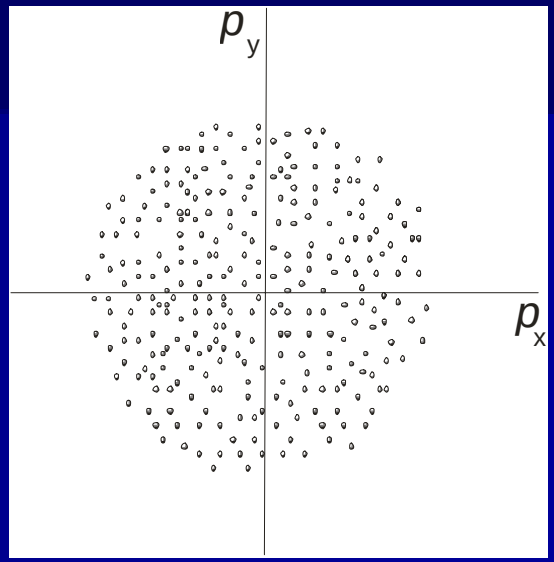
Bose-Einstein Condensation



$T = 0$



$T = T_{BE}$



$T > T_{BE}$

Thermal de Broglie wavelength

$$\lambda_T = \left(\frac{2\pi\hbar^2}{mk_B T} \right)^{1/2}$$

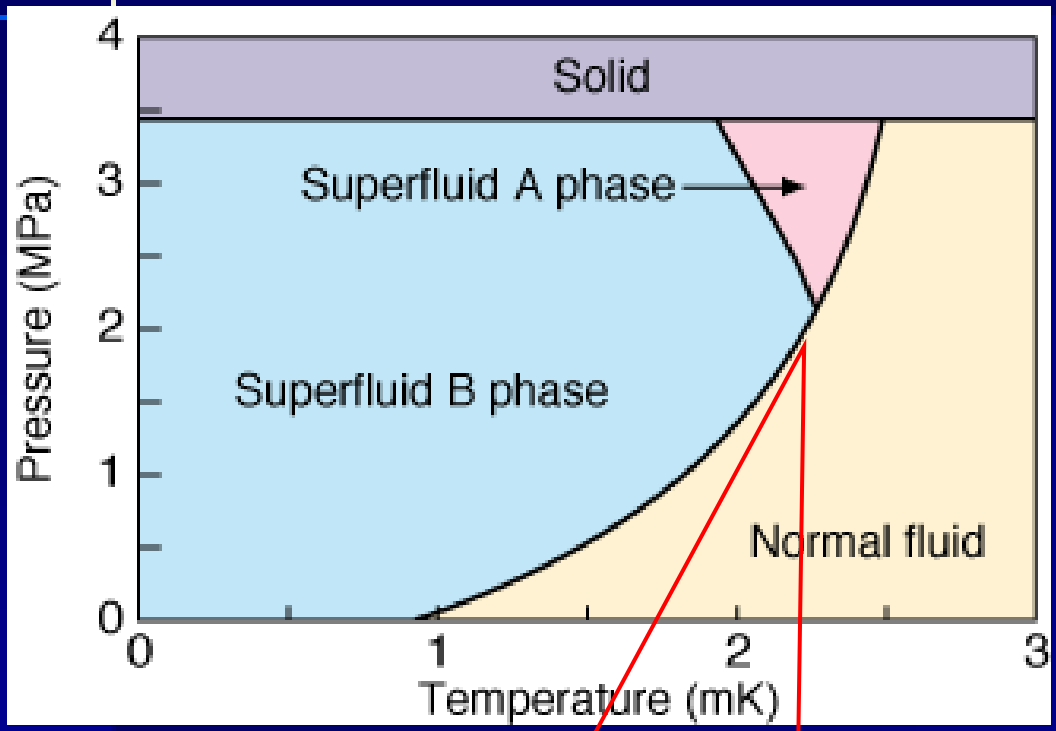
Bose condensation occurs when the thermal de Broglie wavelength reaches the interval of the particles.

$$\lambda_T \approx n^{-\frac{1}{3}}$$

$$T_{BE} = \frac{2\pi\hbar^2}{mk_B} \left(\frac{n}{2.612} \right)^{\frac{2}{3}}$$

Superfluidity of Helium-3

Phase diagram of ^{3}He



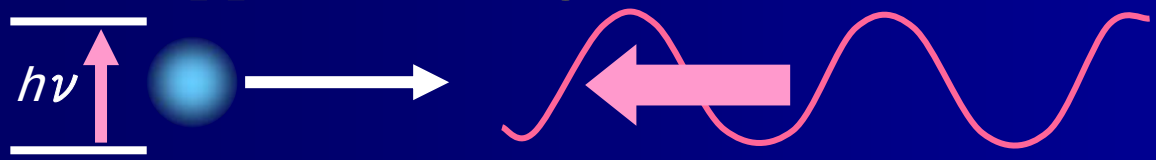
^{3}He becomes superfluidity at a very low temperature ~2mK.

Although, the Bose condensation does not occur for the fermion ^{3}He, boson-like behaving paired ^{3}He causes the phase transition and becomes superfluidity. (This is the same framework observed in superconductivity)

Laser Cooling of Atomic Vapor

Atomic vapor, e.g., Rb is stored in a trap and cooled.

Doppler cooling



- Light with slightly lower than resonance frequency of the atom is radiated.
- The atoms that travel opposite from the direction of the light catch higher frequency of the light due to the Doppler effect; the atoms become almost in a resonance state. They will be possessed with higher probability of absorption thereby, the velocity of the atoms is decreased due to the high absorption probability of the light and momentum.
- In average, the velocity of atoms is decreased because the re-emission of the light is conducted in the same direction.
- Doppler cooling in every direction can be observed by preparing the radiation of six laser beams from both positive and negative x, y, and z directions.
- Doppler cooling limit is approximately $T \sim 100\ \mu$ K.

  ⇒ 3-4 digits of this temperature in above are further lowered.

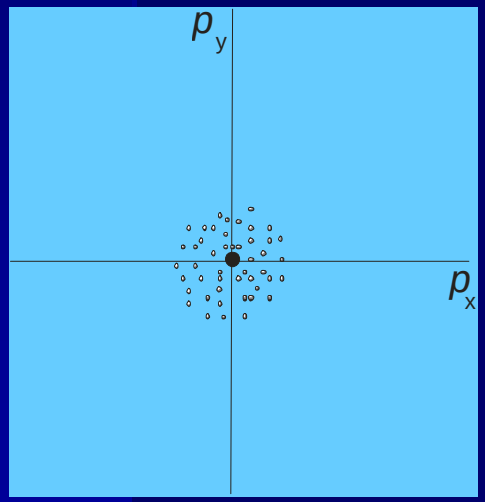
Bose-Einstein Condensation of Atomic Vapor

Atomic vapor is cooled down to be collected in a magneto-optic trap. The condition requirement for the Bose-Einstein condensation is fulfilled by lowering the temperature by evaporative cooling.

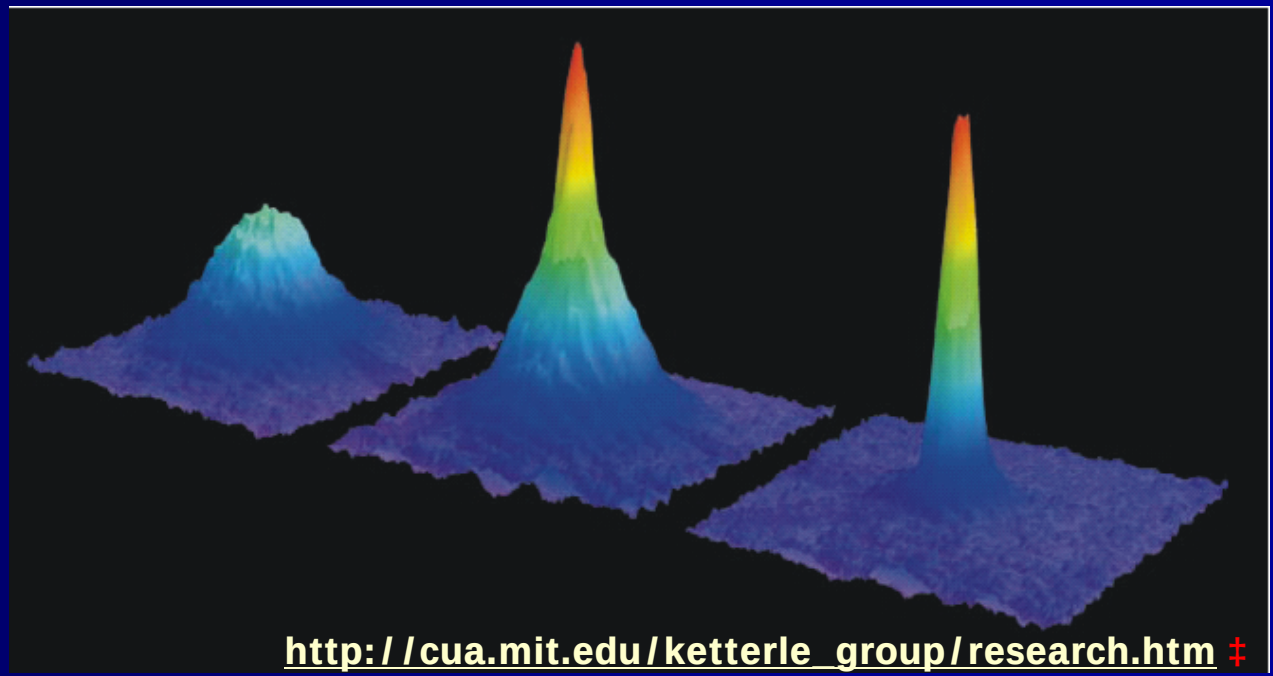
$$\lambda_T \approx n^{-1/3}$$

$T \sim 10^{-7}$K

The switched-off atomic cloud will expand by reflecting the falling velocity distribution due to gravity.

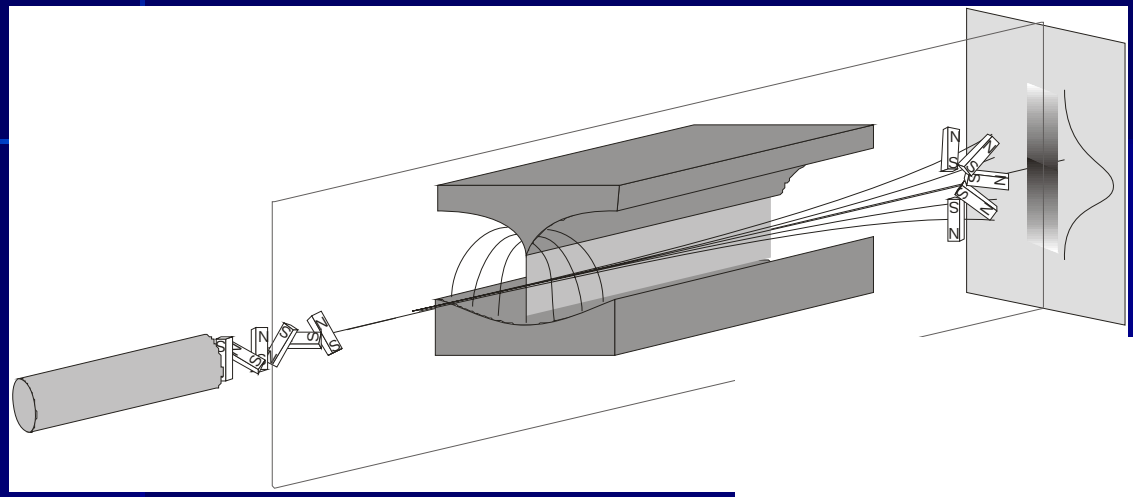


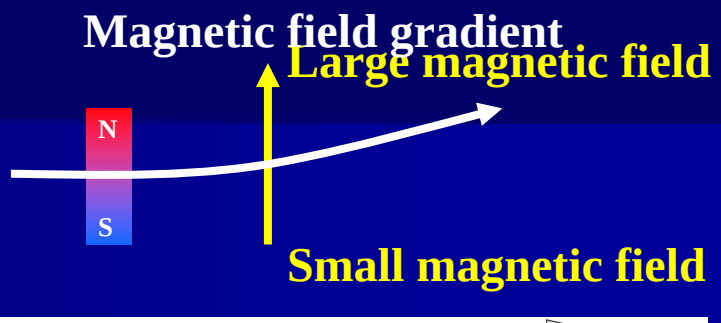
$T = T_{BE}$



Measurement in Quantum Mechanics

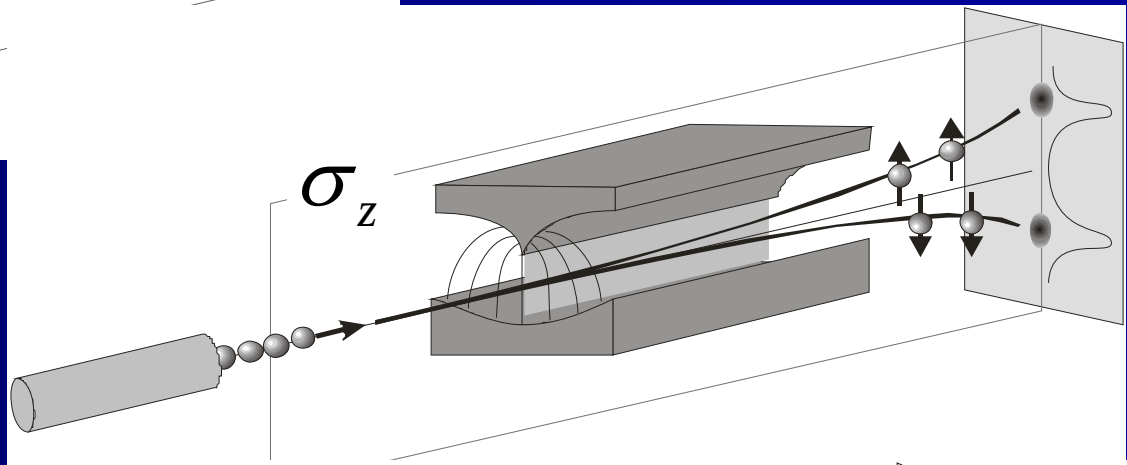
Stern-Gerlach Experiment

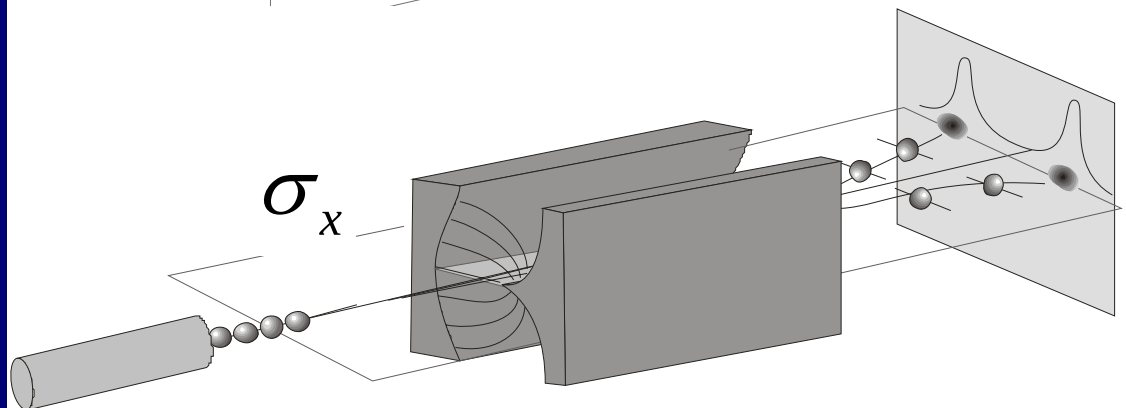




(Classical) bar magnet

Spin-1/2 particle

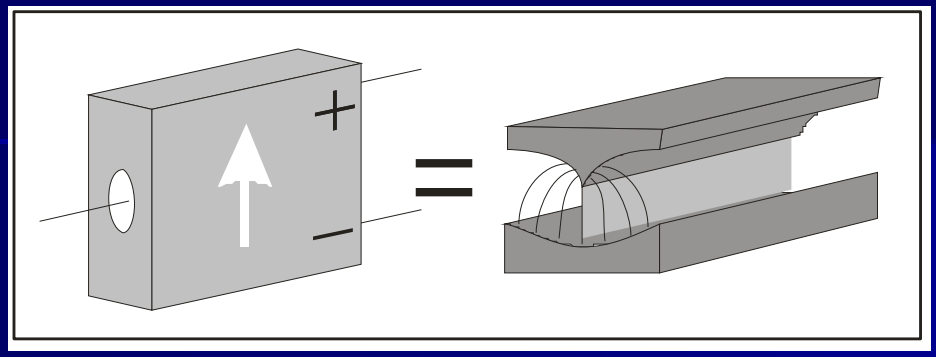


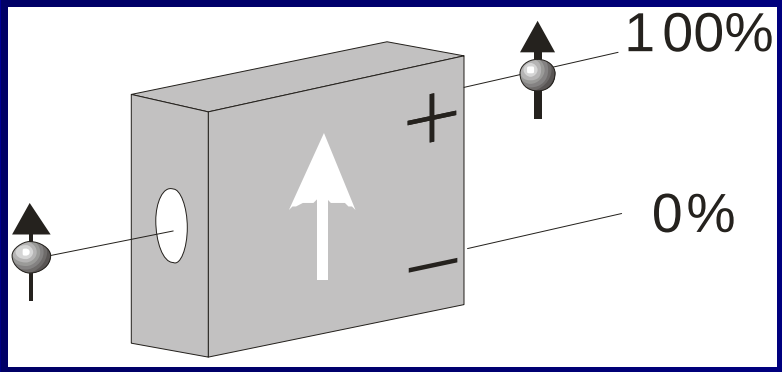


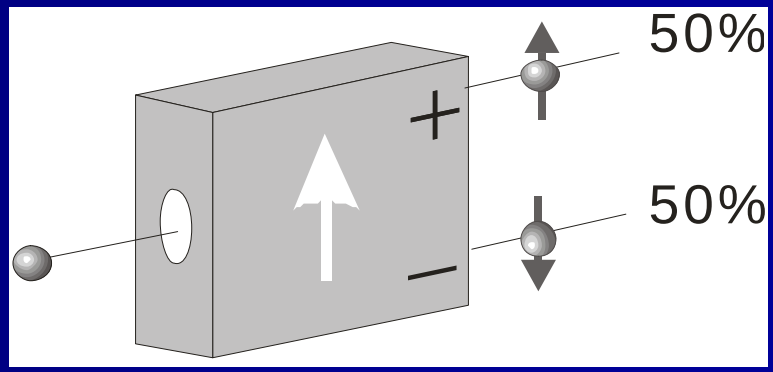
Iye, Yasuhiro. *Alice no Ryoshi Rikigaku*. **In** *Parity*. **Tokyo: Maruzen, 2006.**

‡

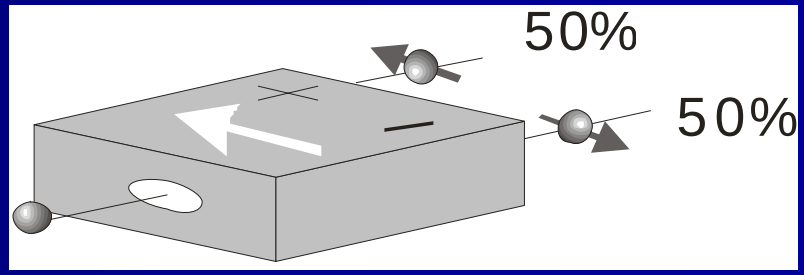
Stern-Gerlach Device







Measurement of the *Z* component of the spin



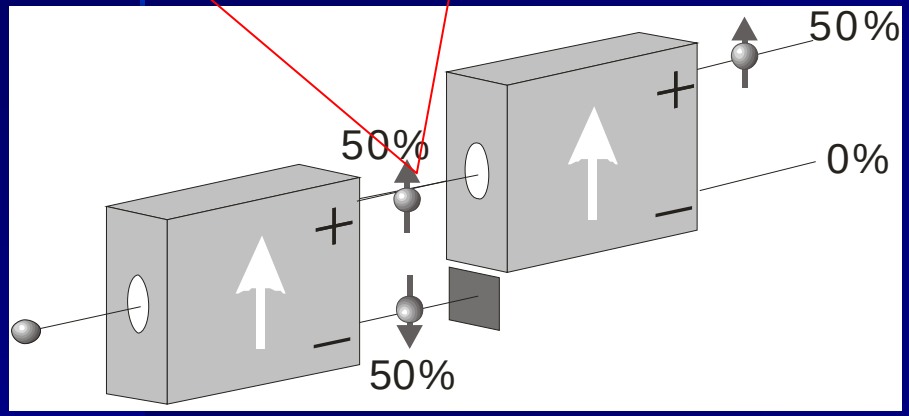
Measurement of the *X* component of the spin

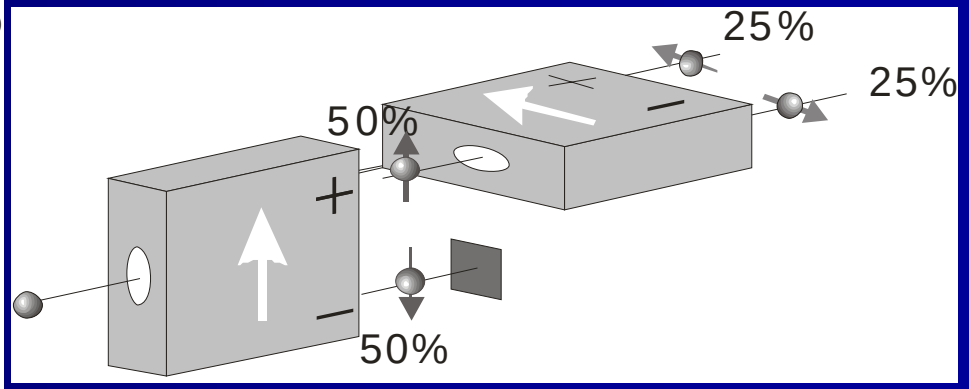
Iye, Yasuhiro. *Alice no Ryoshi Rikigaku*. **In** *Parity*. **Tokyo: Maruzen, 2006.**

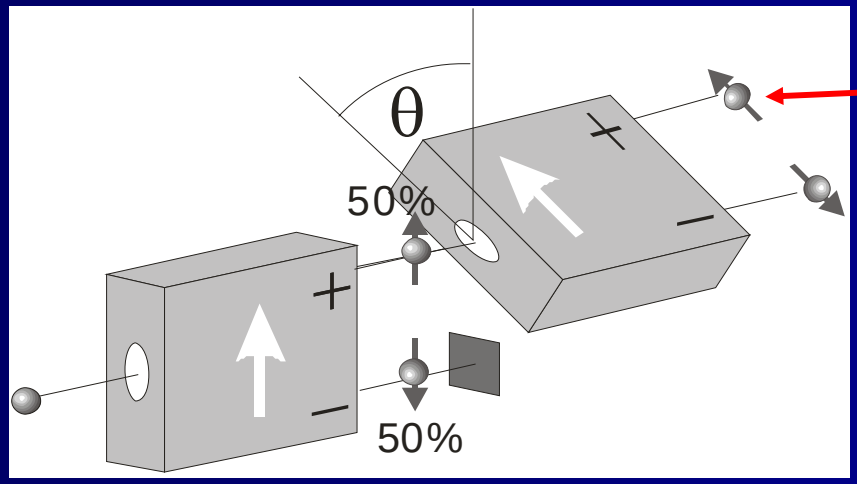
The Defined State by Measurement (Shrinking of the State)

The spin-up state is defined via the measurement of the Z component in spin.

The state is prepared by measurement.



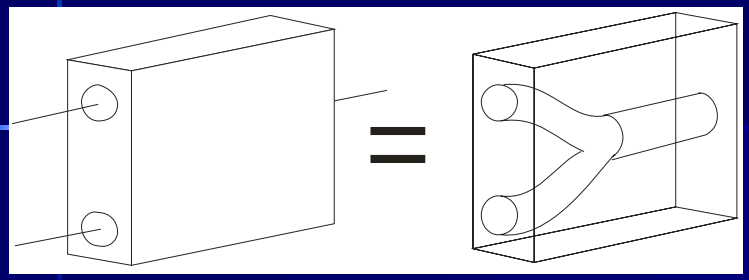




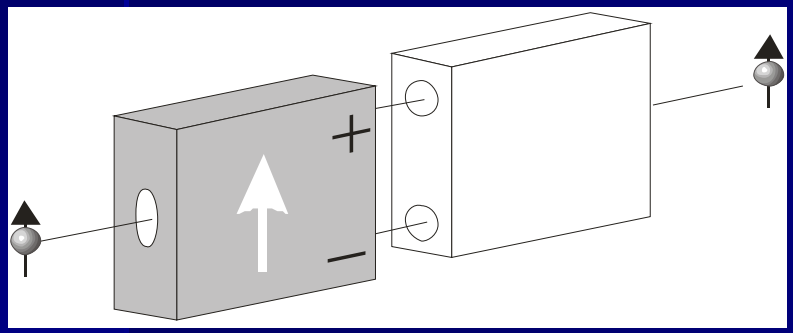
$$P_{+}(\theta) = \frac{1+\cos\theta}{2}$$

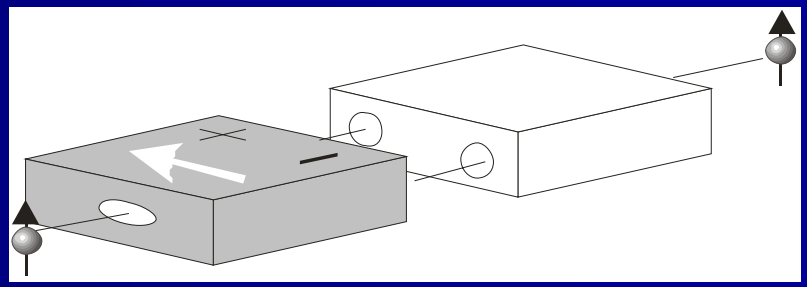
Iye, Yasuhiro. *Alice no Ryoshi Rikigaku*. **In** *Parity*. **Tokyo: Maruzen, 2006.**

Converging Device and Interferometer



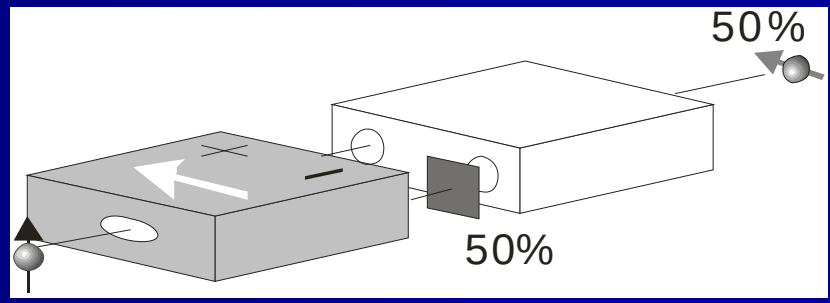
The output from the Stern-Gerlach device is converged.





Converging the output without observing it means next to doing nothing. (There is no information about which path is being taken.)

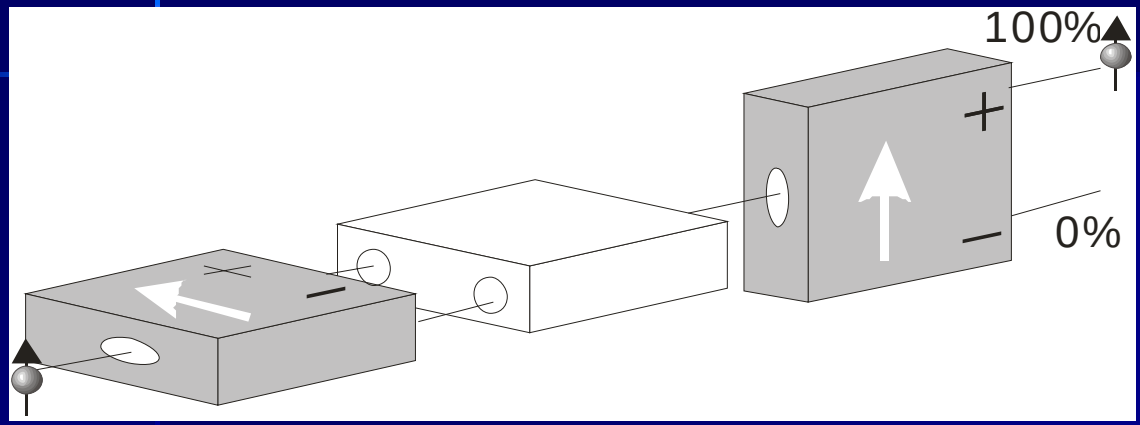
If one of the outputs is blocked:



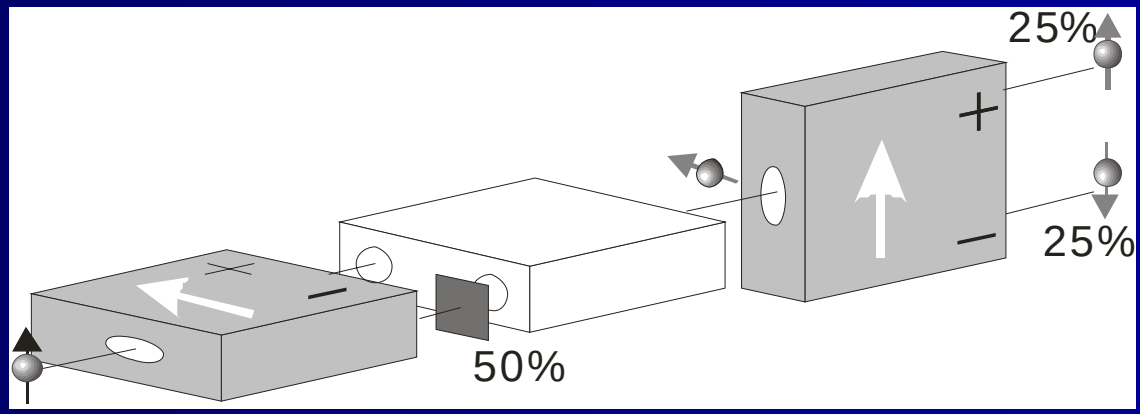
Iye, Yasuhiro. *Alice no Ryoshi Rikigaku*. **In** *Parity*. **Tokyo: Maruzen, 2006.**

‡

Interferometer Output



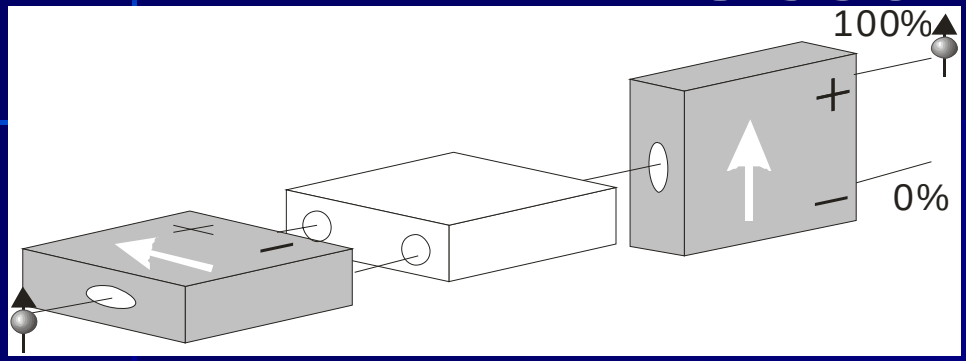
Converging the output without observing it means doing nothing. The probability of the negative path being taken is zero.



The probability in marking the negative path will increase from 0% to 25% by blocking either of the paths.

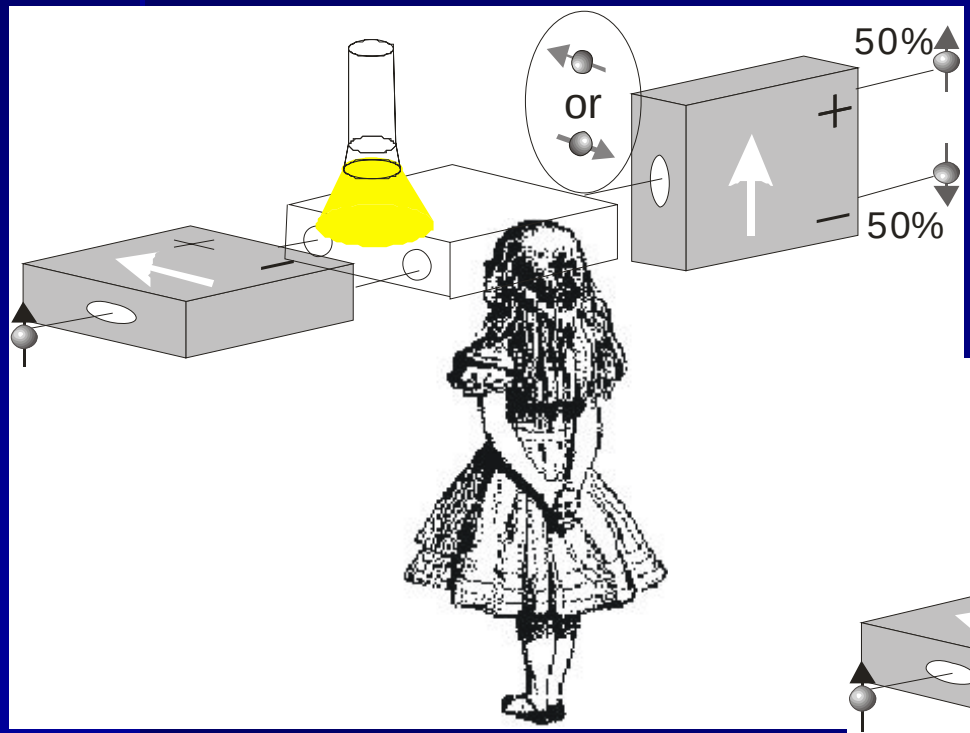
Iye, Yasuhiro. *Alice no Ryoshi Rikigaku*. **In** *Parity*. **Tokyo: Maruzen, 2006.**

Decoherence Through Observation

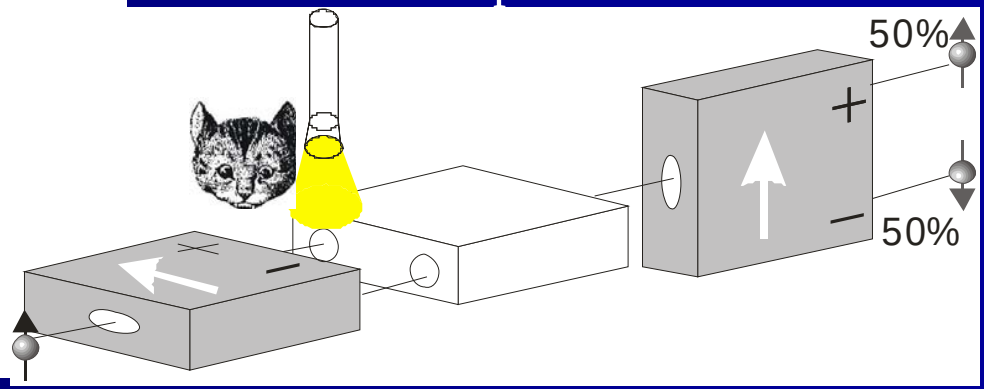


$$|\uparrow\rangle = \frac{1}{\sqrt{2}}\left(|\leftarrow\rangle + |\rightarrow\rangle\right)$$

The observation of path selection prevents interference from occurring.

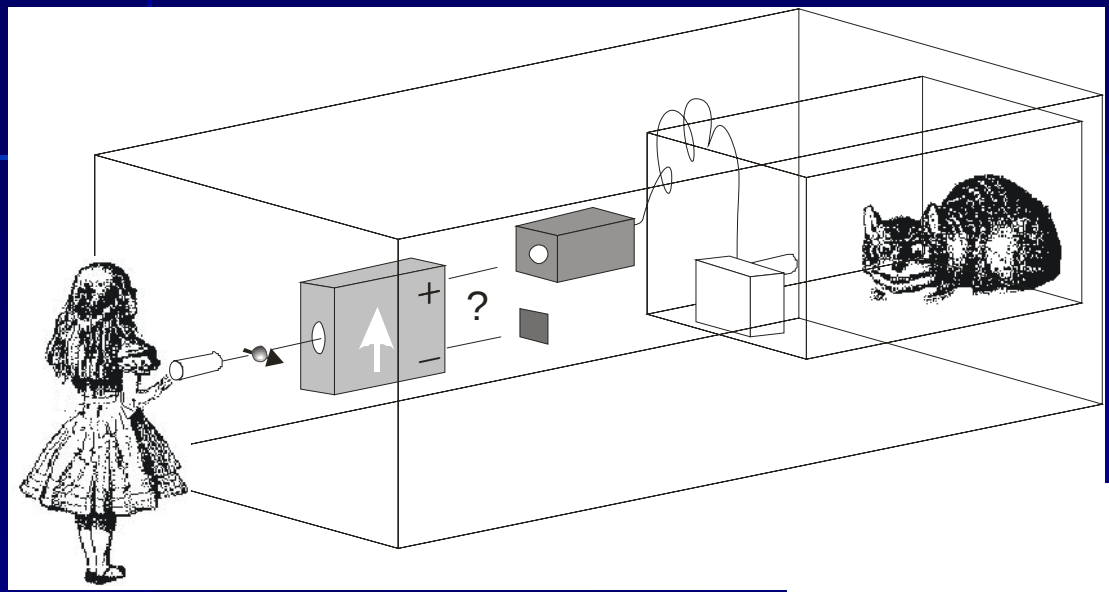


Observation of one side of the path is the same as obtaining all information because there are only one or the other choices for the path.

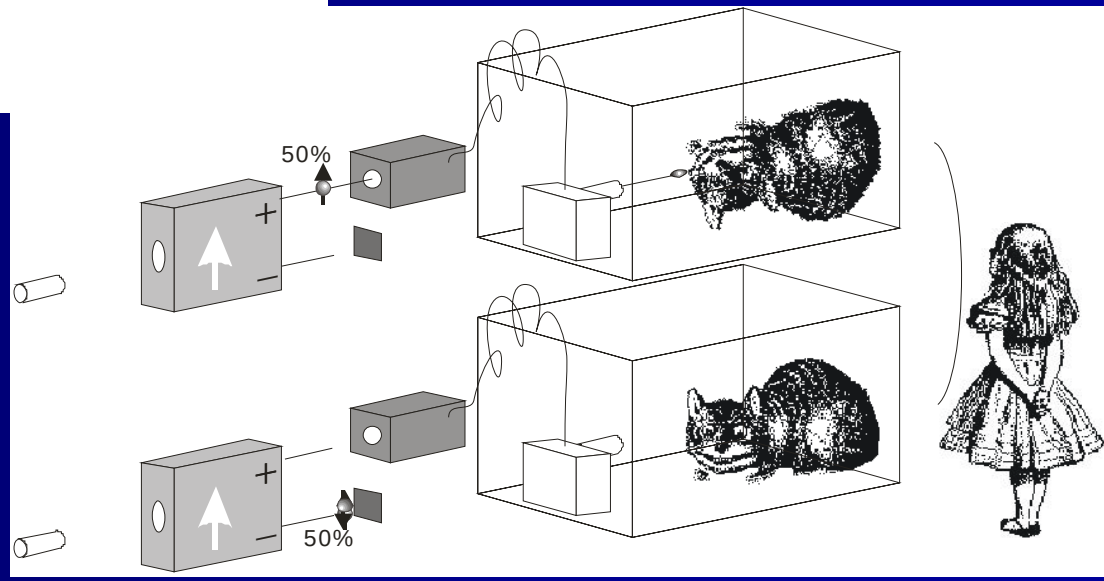


Iye, Yasuhiro. *Alice no Ryoshi Rikigaku*. **In** *Parity*. **Tokyo: Maruzen, 2006.** ‡

Schrodinger's Cat



Detection of spin-up will cause firing of the bullets and the cat will die.



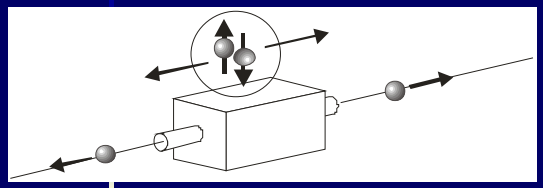
Is this superposition of states in which the cat is in the condition of both being dead and alive at the same time?

$$|\Psi\rangle = |\uparrow\rangle \left| \begin{matrix} \text{Cat is} \\ \text{dead.} \end{matrix} \right\rangle + |\downarrow\rangle \left| \begin{matrix} \text{Cat is} \\ \text{alive.} \end{matrix} \right\rangle$$

Iye, Yasuhiro. *Alice no Ryoshi Rikigaku*. **In** *Parity.* **Tokyo: Maruzen, 2006.**

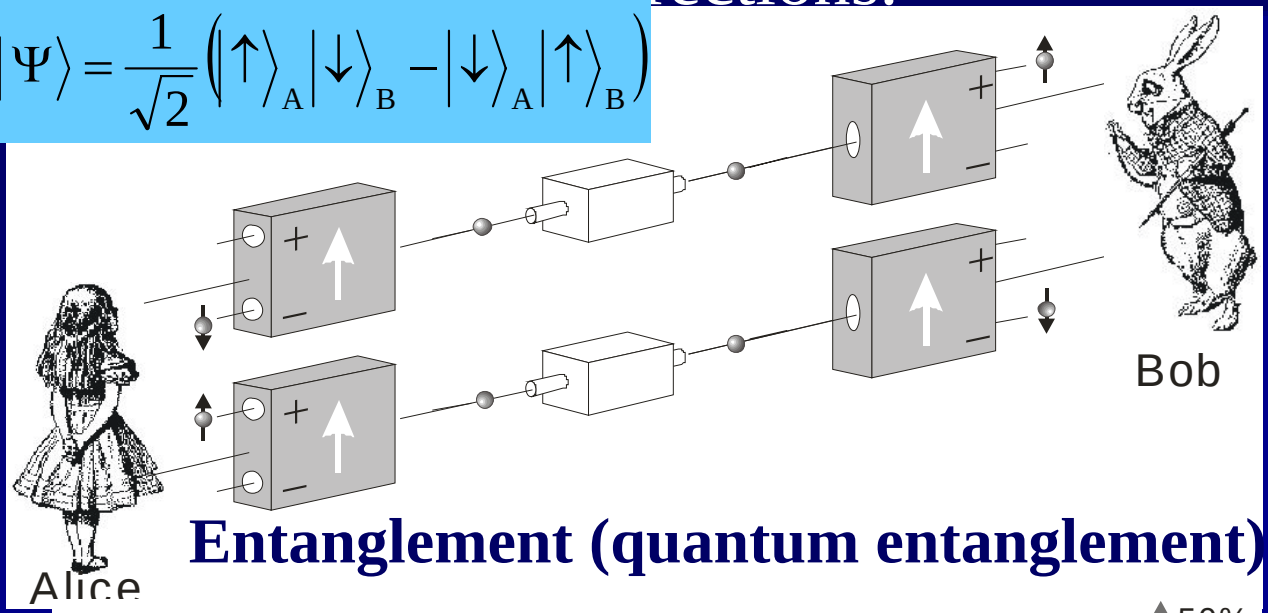
‡

Einstein-Podolsky-Rosen(EPR) Experiment

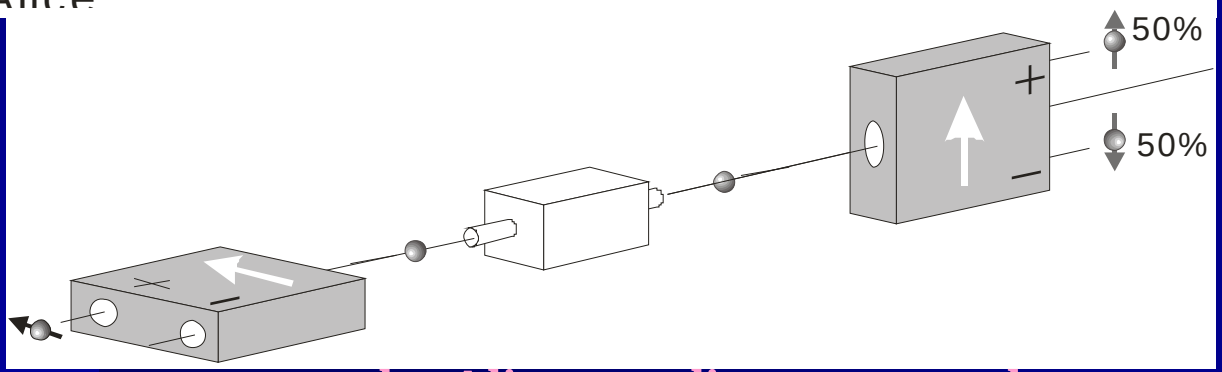


Two particles have opposite spin directions.

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_A|\downarrow\rangle_B - |\downarrow\rangle_A|\uparrow\rangle_B\right)$$



Entanglement (quantum entanglement)



If Alice observes spin ↑ then Bob observes the spin ↓ . (There is a complete correlation in the measurement results.)

What if Alice and Bob observe opposite spin directions? (A characteristic correlation in quantum mechanics: entanglement.)

Iye, Yasuhiro. *Alice no Ryoshi Rikigaku*. **In** *Parity*. **Tokyo: Maruzen, 2006.** ‡

Does measurement by Alice at a distance away have some kind of effect on Bob's measurements?

Bell's Inequality

Particles do not know spin measurement directions.

The local objective theory suggests that the results obtained by measurement depend on the hidden variables in the first place.

Let us consider the quantity: $F \equiv \sigma_z^A \sigma_z^B + \sigma_y^A \sigma_y^B + \sigma_y^A \sigma_z^B - \sigma_z^A \sigma_y^B$

$-2 \le \langle F \rangle \le 2$ Bell's inequality should be established.

A	**z**	+	+	+	+	+	+	+	+	−	−	−	−	−	−	−	−
A	**y**	+	+	+	+	−	−	−	−	+	+	+	+	−	−	−	−
B	**z**	+	+	−	−	+	+	−	−	+	+	−	−	+	+	−	−
B	**y**	+	−	+	−	+	−	+	−	+	−	+	−	+	−	+	−
F		**2**	**2**	**-2**	**-2**	**-2**	**2**	**-2**	**2**	**2**	**-2**	**2**	**-2**	**-2**	**-2**	**2**	**2**

Quantum mechanics states that Bell's inequality can be broken under certain conditions.

Aspect's experiment verified that Bell's inequality can be broken. The experiment was conducted by using polarized light of photons instead of spin.

Cryptography

Necessity for Cryptosystems

- Secured information commutation:
  - Handling of credit card numbers for Internet shopping.
  - Confirming the authenticity of information, e.g., ID confirmation.
- Tackling Eavesdropping:
  - Security systems are designed on the understanding that the DATA CAN BE EVESDROPPED ⇒ cryptography
  - Short-time-use only random number sequence is used to encrypt the data to be sent. The encrypted data is impossible to read.

  ⇒ A sender and a receiver need to share the necessary length of the random sequence without other people's knowledge.

  (Private key distribution)

Quiz

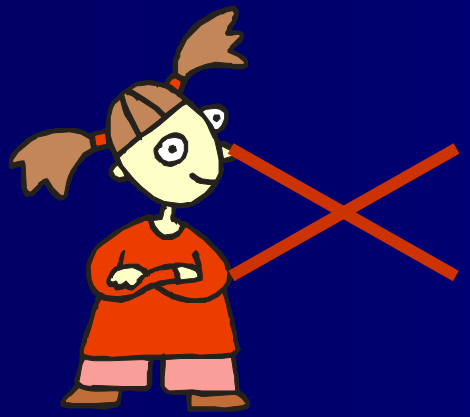
- There is a country where thieves are in charge of the postal service. They open all the unlocked packages and steal what is inside, however, they would never touch the packages that have been locked. Bob and Alice are engaged, and Bob wishes to send Alice an engagement ring via the country's postal service. How does Bob send the ring safely to Alice?
- A sturdy locked box would keep the ring from being stolen though, Alice will not be able to open the package without a key. The lock can be obtained at any stores nearby but the key which goes to the lock remains where the sender is; the package receiver does not have the key in this case. If the lock itself is being sent in another package, it has to be locked again to prevent it from being stolen.
- Bob, at his wit's end, called Alice. She evidently came up with a very good idea, i.e., use a box that can have as many locks as possible attached. How did Alice eventually receive the ring safely from Bob?

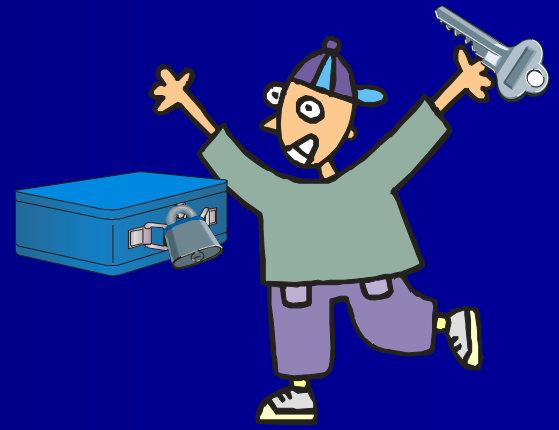
Bob Wants to Send a Ring to Alice

Alice

Bob

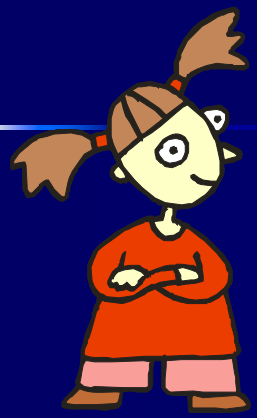
①Bob sends a package with a ring inside a locked box.

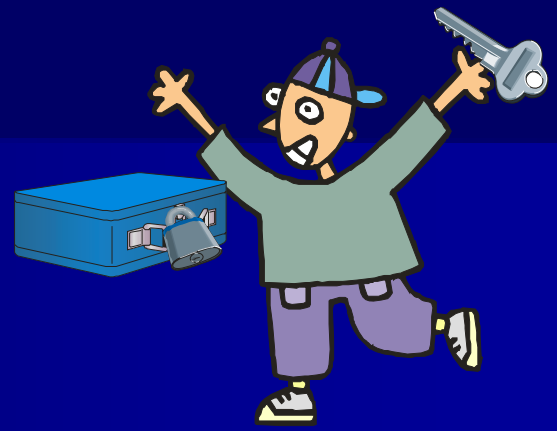




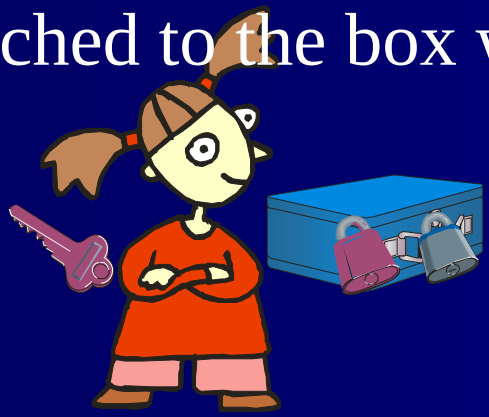
But Alice, having no key, cannot open the box.

①Bob sends a ring in a locked box.

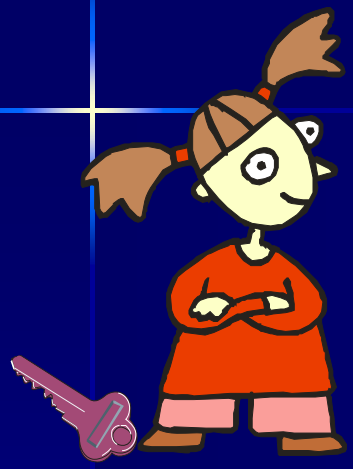




②Alice sends back the package with her own lock attached to the box which Bob had sent to her.



③Bob removes his lock with his own key and sends it back to Alice again.



④Alice receives the ring safely by unlocking the box with her key.

What is Cryptography?

The sending data in plaintext is encrypted by following a certain rule.

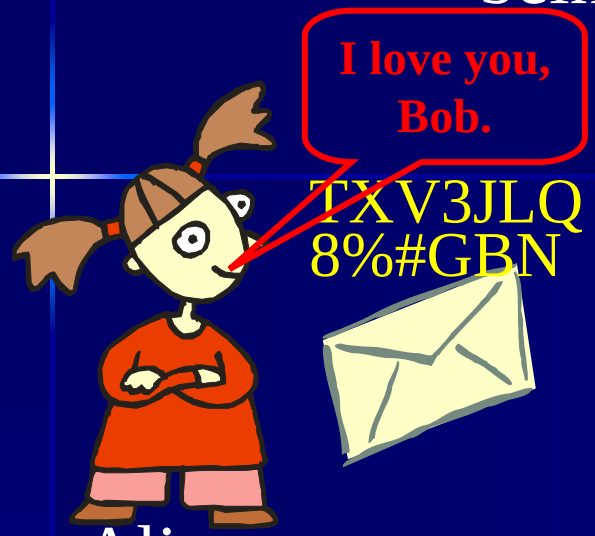
⇒It is the same as attaching a lock to a package.

This prohibits other people from decrypting the text, and allows the communication with a target person to decipher the text.

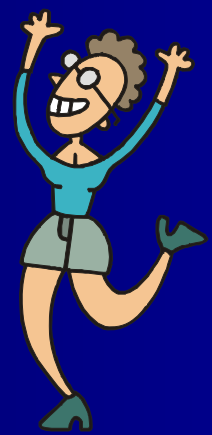
⇒ No one without the key can open the package. The key is passed only to the target person.

The problem here is how to safely pass the key.

Alice sends a coded love letter to Bob to avoid being eavesdropped on by Eve.



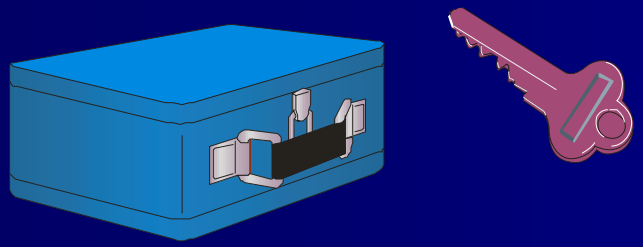
If the two communicators are the only people having private keys, then their communication will be secure.



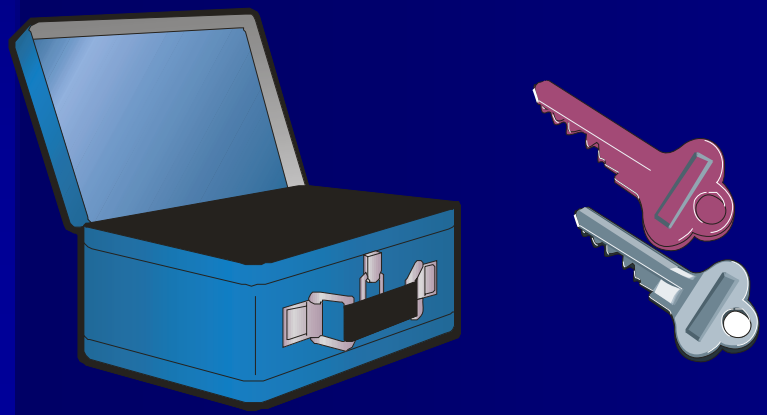
However, we must not send the private key by public communication methods such as telephone lines and Internet channels.

The private key must be decided individually by each communicating pair.

Let Us Suppose a key:



Only a purple key is required to lock the box. Reveal this key in public.



To open the box, both purple and silver keys are required. Only the target communicator is allowed to have this silver key.

Public Key Cryptosystem

Reveal the public key to anyone who wants to read and encrypt data.

Another key (a private key) is required to decrypt the data.

Public-key Cryptosystem

Encryption can be conducted by using only one key while the decryption process requires a complete pair of keys.

① Alice decides on a private key and a public key; the communication with herself, permitting the use of this public key to any users who wish to do so.

② Bob uses Alice's public key to encrypt data and sends the encrypted data to Alice.

③ Alice uses her public key and private key to decrypt and read the message.

④ Without the private key, no one except Alice who has the private key is allowed to read the encrypted data.

Public Keys and Private Keys

There must be some kind of relationship between the public key and the private key given what is being locked by the public key is being unlocked by the private key.

The private key must not be something simple for people to easily predict by looking at the structure of the public key.

This problem can be solved by taking advantage of the characteristics of a computation; simple in a certain direction but complicated in the opposite direction: Factorization in prime numbers.

114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147147599290026879543541
= 349052951084765094914784961990389813341776463849338784399082057 7
×
327691329926670954996198819083446141317764296799294253997828853 3

Public Key Cryptosystem (RSA Encryption) (1)

Bob generates a public-private key pair:

(1) Bob selects two arbitrary prime numbers. Let us say, p = 5 and q = 11 for now.

(2) Computation with the two selected numbers are conducted in multiplication: n = p × q = 55 Which will be a part of public key.

(3) Select a number e that is relatively prime to the product (p-1) × (q-1) = 4 × 10 = 40 Here, we select e=7

e = 7 and n = 55 are Bob's public key.

(4) Now we calculate for the private key. Select an integer d from the quotient {ed = 1 mod(p-1)(q-1)}, i.e., d × e is divided by (p-1)(q-1) to have a remainder of 1. Given (p-1)(q-1) = 40 and e = 7, we can have d = 23. (d × e = 23 × 7 = 161, which has remainder of 1 when divided by 40.) This d will be Bob's private key.

Public Key Cryptosystem (RSA Encryption) (2)

Alice encrypts her message:

(1) Alice encrypts a message, M= “2” and wishes to send it to Bob. The encrypted message C is expressed by public key e and n:

$$C = M^e \pmod{n} = 2^7 \pmod{55} = 128 \pmod{55} = 18$$

Alice sends this message to Bob.

Bob decrypts the message:

(2) Having received message “18” from Alice, Bob decrypts the message with his private key d in addition to the public key n. The message is decrypted in the following way:

$$M = C^d \pmod{n} = 18^{23} \pmod{55} = 2$$

Bob successfully received message “2” from Alice.

Quantum Computers

Quantum Computers

A quantum computer does not eliminate the role of the classical computer.

For certain types of problems, a quantum computer can perform computations faster than a classical computer.

- Grover's algorithm for quantum database searching.

- Shor's factorization algorithm.

  ⇒ Possible breaking of the public key cryptosystem?

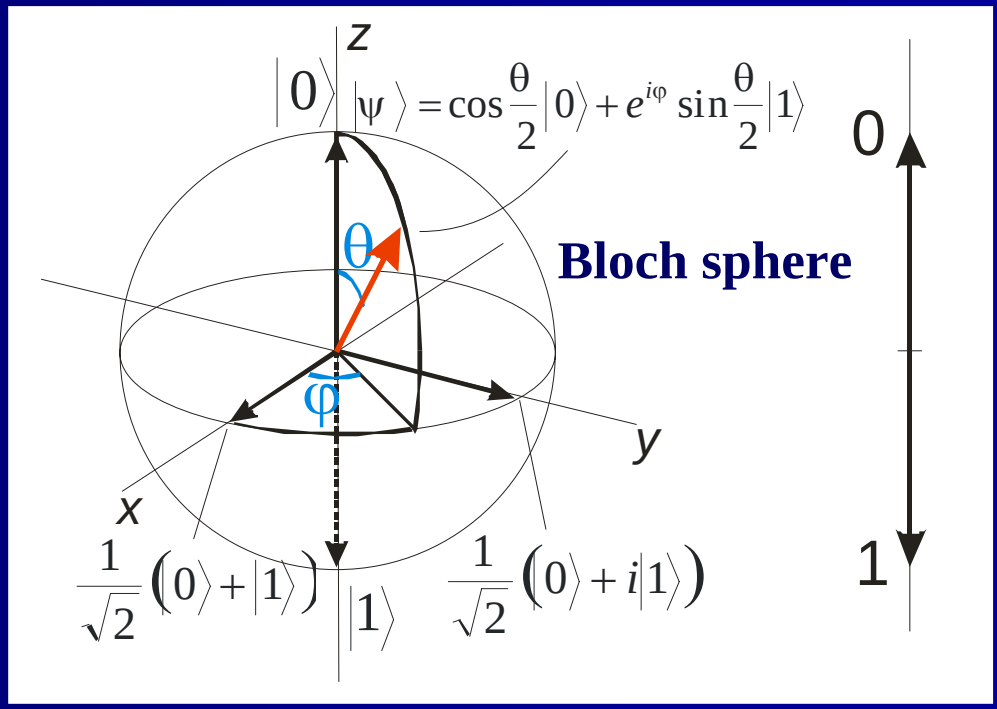
Quantum Bits (Qubits)

【Classical bit】 Two types of states; either 0 or 1 is chosen.

【Quantum bit】 Two types of states; arbitrary superposition of $|0\rangle$and$|1\rangle$.

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

N qubits can express 2^N superposition states, which can also perform parallel computation of 2^N input values.

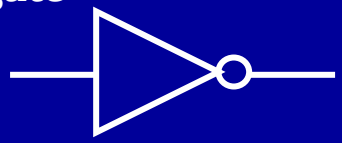


Quantum computer: uses superposition and entanglement to perform computations that are beyond the capability of classical computers.

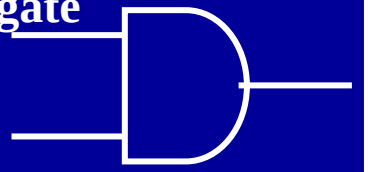
The Logic Gate

Logic operation by classical computer:

NOT gate



AND gate

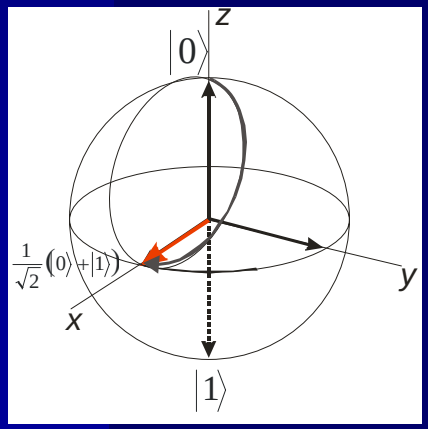


$\|a\rangle$	$\|b\rangle$	$\|c\rangle$	$\|d\rangle$
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

Logic operation by quantum computer:

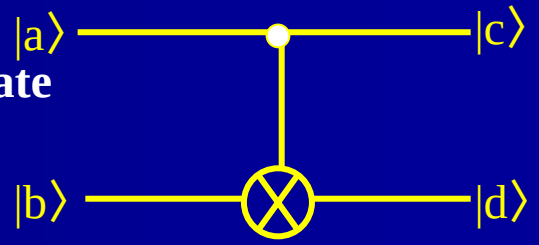
Hadamard gate

$$|0\rangle \Rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$



Preparation for the superposition state.

Control-NOT gate



Input: $$|a,b\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)|0\rangle$$

Output: $$|c,d\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right)$$

The state of entanglement is made.

Essential Conditions for the Achievement of a Quantum Computer

- Ability to initialize qubits.
- Readout method to determine the state of qubits.
- Gate operation by Hadamard gate and control-NOT gate.
- Physically scalable to increase the number of qubits.
- Relatively long decoherence time when compared with the operation time. (Isolation from environment.)

Qubit Candidates

The classical bit is physically formed in many different shapes.

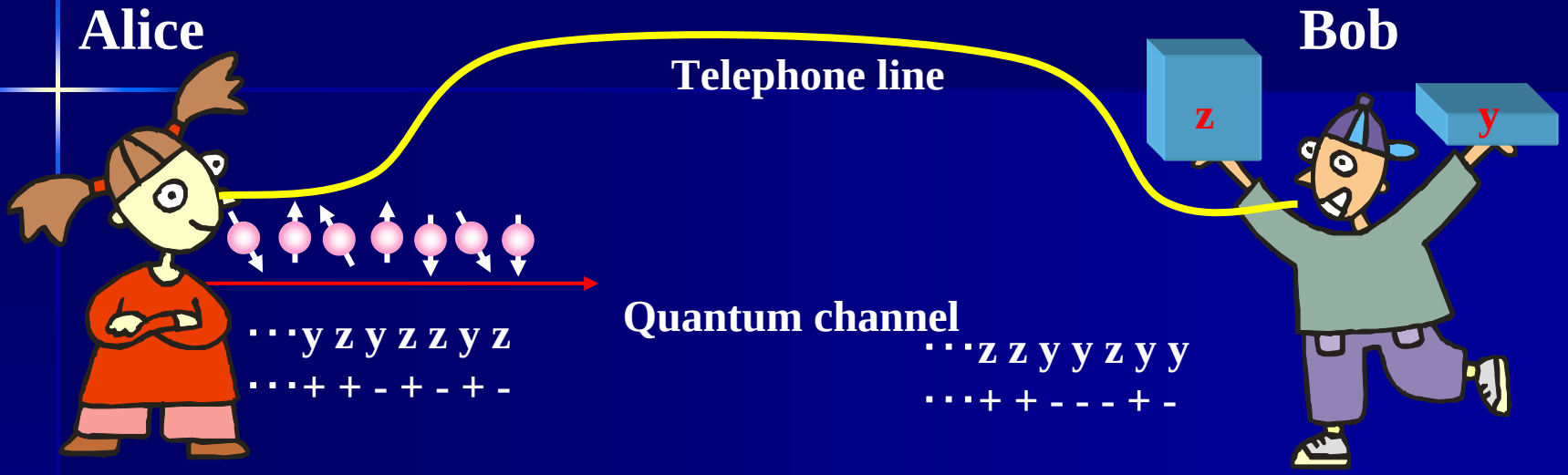
High/low electric voltage, on/off of the light, direction of magnetism, and presence of an electric charge.

Anything that belongs to the quantum two-level system can be a qubit candidate.

- Photons
- Trapped ions
- Microresonator
- Quantum dots (electric charge, spin, and nuclear spin)
- Superconductive qubits (Josephson junction)
- Nuclear Magnetic Resonance (NMR), nuclear spin in molecule
- Electrons on liquid helium surface

Quantum Cryptography
(Private Key Distribution)

Quantum Cryptography (Private Key Distribution)



Alice's configuration: · · · y z y z z y z

Measured value: · · · + + - + - + -

Bob's configuration: · · · z z y y z y y

Measured value: · · · + + - - - + -

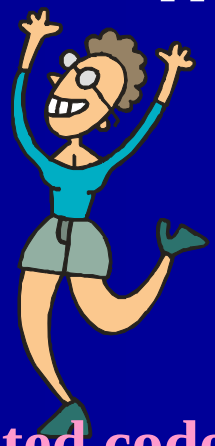
· · · × ○ ○ × ○ ○ ×

Adopting code: · · · 1 0 0 1

If their conversation is wiretapped,

· · · z z y y z y y

· · · + + + - - + -



Eavesdropping can be detected by using a part of the adopted code.

Quantum Cryptography (Private Key Distribution)

・Alice sends Bob randomly-selected spin (↑ , ↓ →, and ←) particles one after another. (Quantum channel)

・Bob records the z or y component of the spin toward the incoming particles.

・After the course of measurement, Alice communicates with Bob via a classical channel to pass the information about the initial configuration. (The measurement results must be kept secret.)

・Only when the configuration matches, the data can be used.

・To detect eavesdropping, revealing to each other a small sequence of bits in public.

Alice's configuration	z y z z y z y y z y ･･･
Spin value	+ - - + + + - - - + ･･･
Bob's measurement	y z z y y z y z z y ･･･
Spin value	- - - - + + - - - + ･･･
The set-up match	× × ○ × ○ ○ ○ × ○○･･･
Private key	0 1 1 0 0 1 ･･･

・Apparently, the quantum state disturbed by eavesdropping does not produce a configuration match. (The eavesdroppers do not know the initial configuration thus, they use the wrong configuration by a chance of 50%.)

Summary

Atom manipulation and quantum manipulation:

- Observation and manipulation of atoms
  - STM, AFM and nanoscience
- Macroscopic quantum phenomena
  - Quantum statistics
  - Quantum liquids
  - Bose-Einstein condensation
- Quantum information processing
  - Cryptography
  - Quantum computers
  - Quantum ciphers (private key distribution)