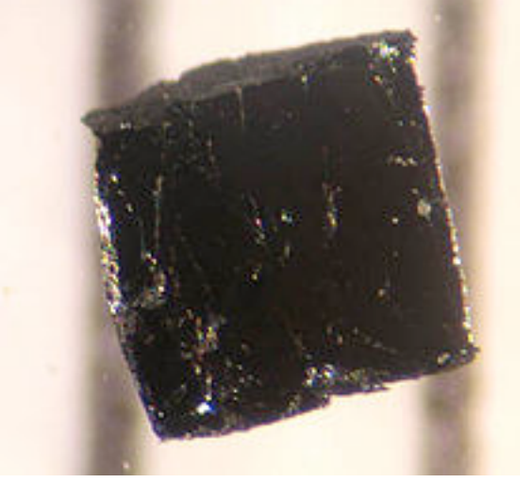
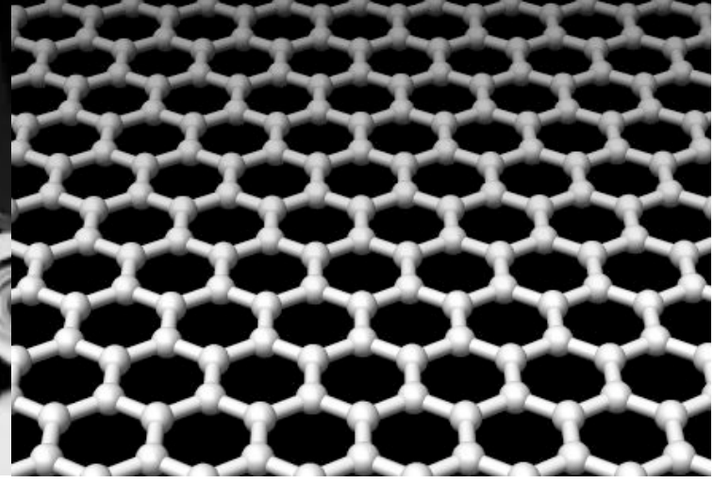
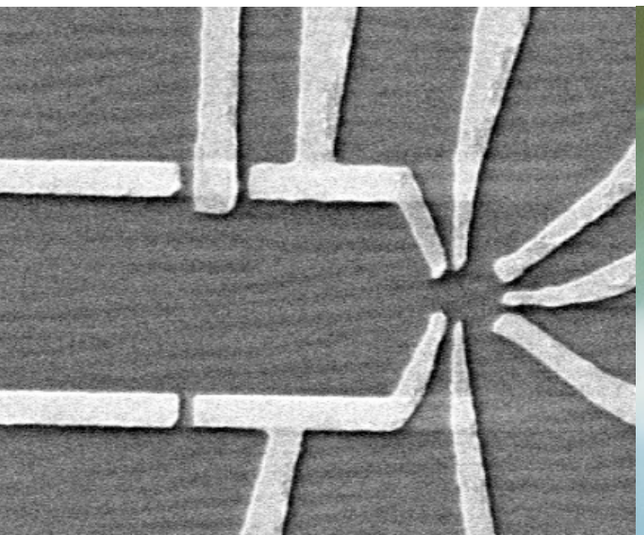




Quantum Science

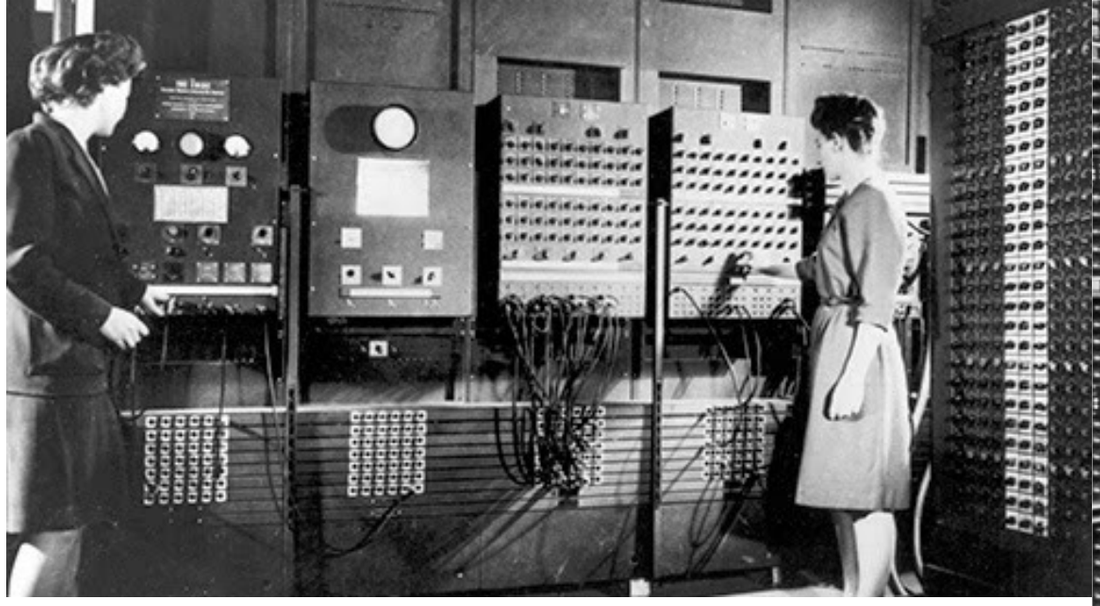
Bruno Uchoa

Department of Physics and Astronomy
University of Oklahoma




Lecture 2

Implications of quantum mechanics



Since 1944, electromechanical and digital computers have been used in a variety of scientific applications.

International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

Richard P. Feynman

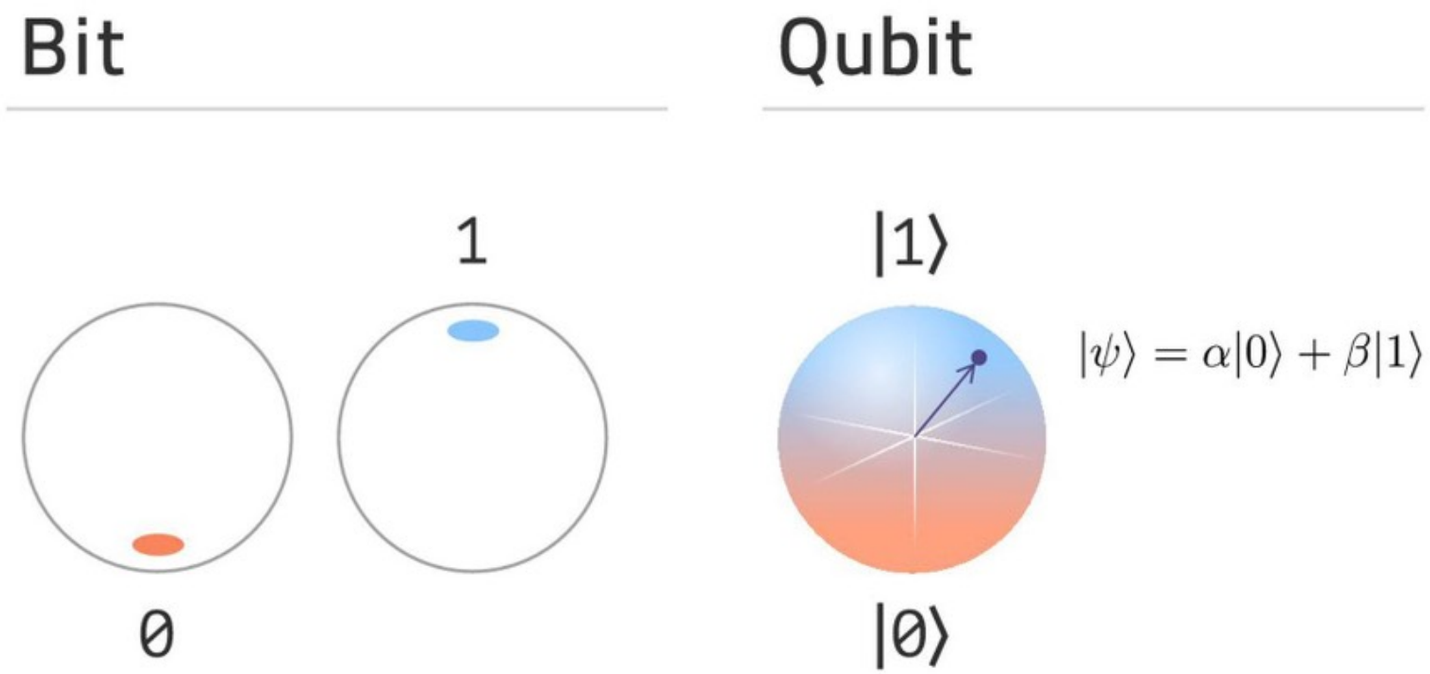
Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

In 1981, Feynman gave a lecture where he proposed that natural processes should be simulated by other natural processes, rather than by classical computers, since nature is quantum mechanical.

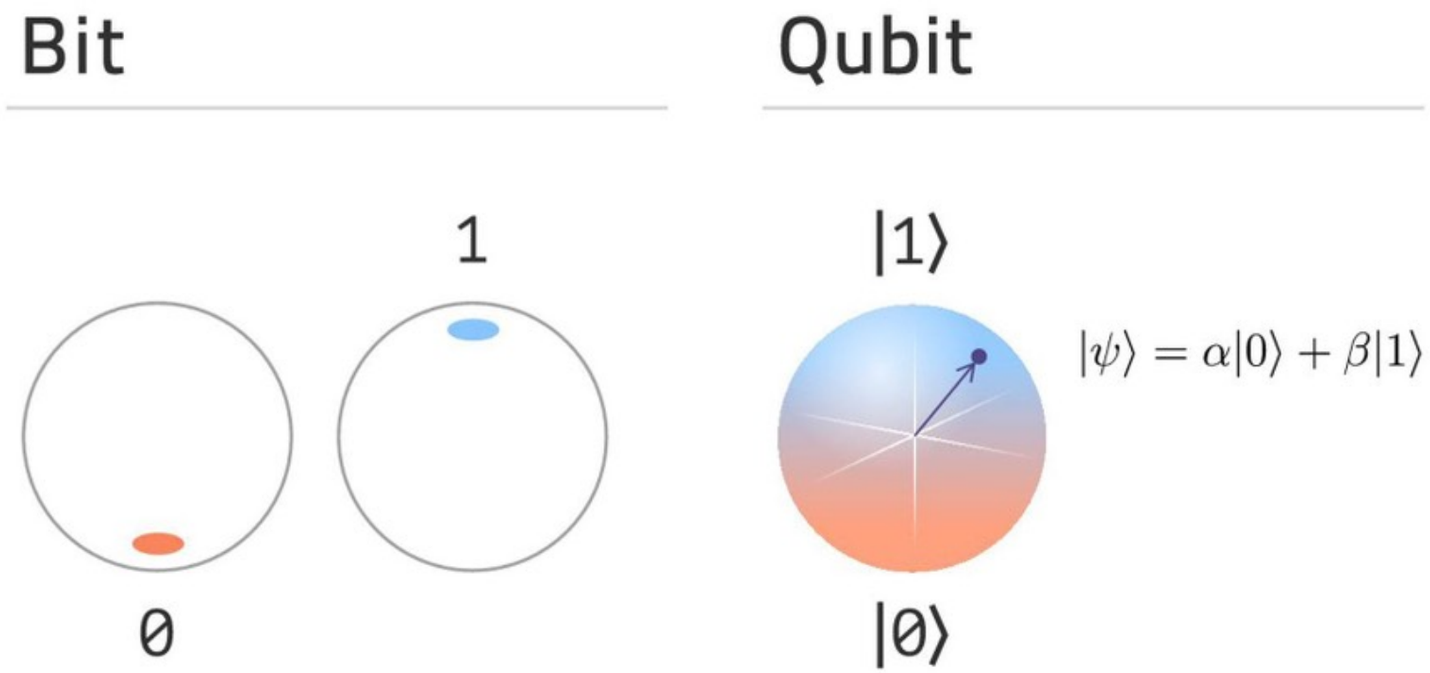
He called computers based on natural processes quantum computers.

Quantum Computers



The elementary unit of information in a quantum computer is the qubit, which exists as a simultaneous superposition of a 0 and a 1 states.

Quantum Computers



N bit: **01111001000011** (one state)

N qubit: $|\psi_1\rangle \cdot |\psi_2\rangle \cdot \ldots \cdot |\psi_N\rangle \longrightarrow |\psi\rangle^N = \underbrace{(\alpha|0\rangle + \beta|1\rangle)^N}_{2^N \text{ states}}$

A quantum computer with N qubits exists simultaneously as a linear superposition of 2^N states!

Quantum Computers

In performing logical operations with those independent 2^N states, quantum computers are capable of massive parallelization that grows exponentially with the number of qubits!

N bit: **01111001000011** (one state)

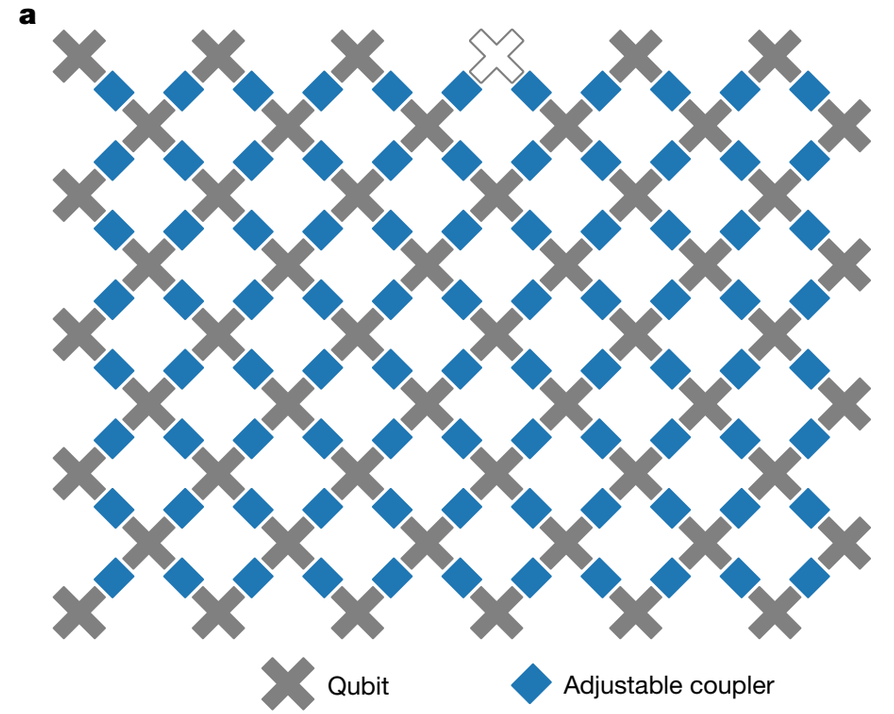
N qubit: $|\psi_1\rangle \cdot |\psi_2\rangle \cdot \ldots \cdot |\psi_N\rangle \longrightarrow |\psi\rangle^N = \underbrace{(\alpha|0\rangle + \beta|1\rangle)^N}_{2^N \text{ states}}$

A quantum computer with N qubits exists simultaneously as a linear superposition of 2^N states!

Nature | Vol 574 | 24 OCTOBER 2019 | 505

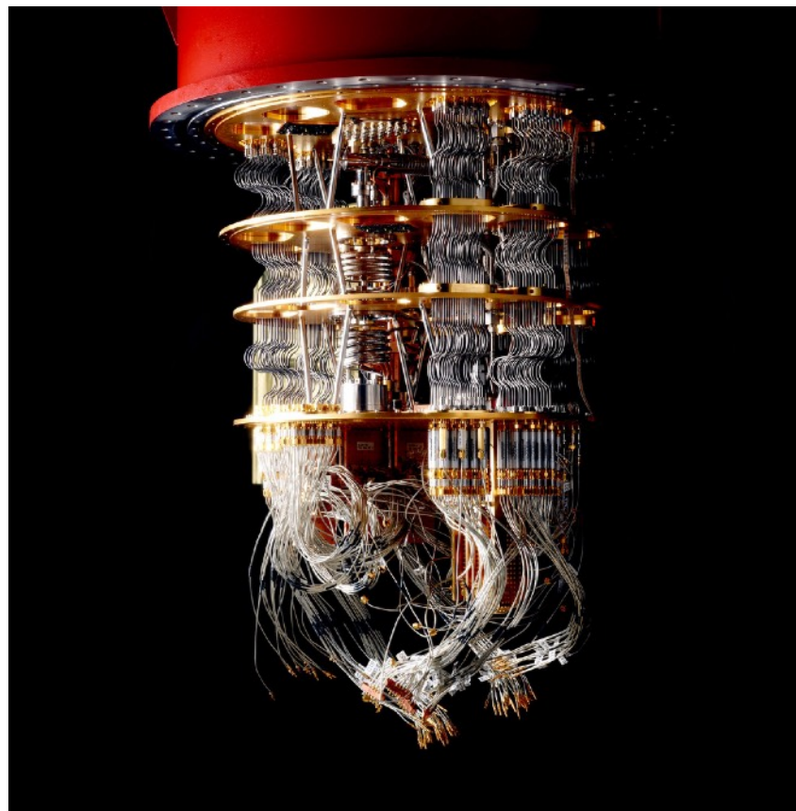
Article

Quantum supremacy using a programmable superconducting processor



Google sycamore quantum computer operates with N=53 qubits!

What makes a good quantum computer?



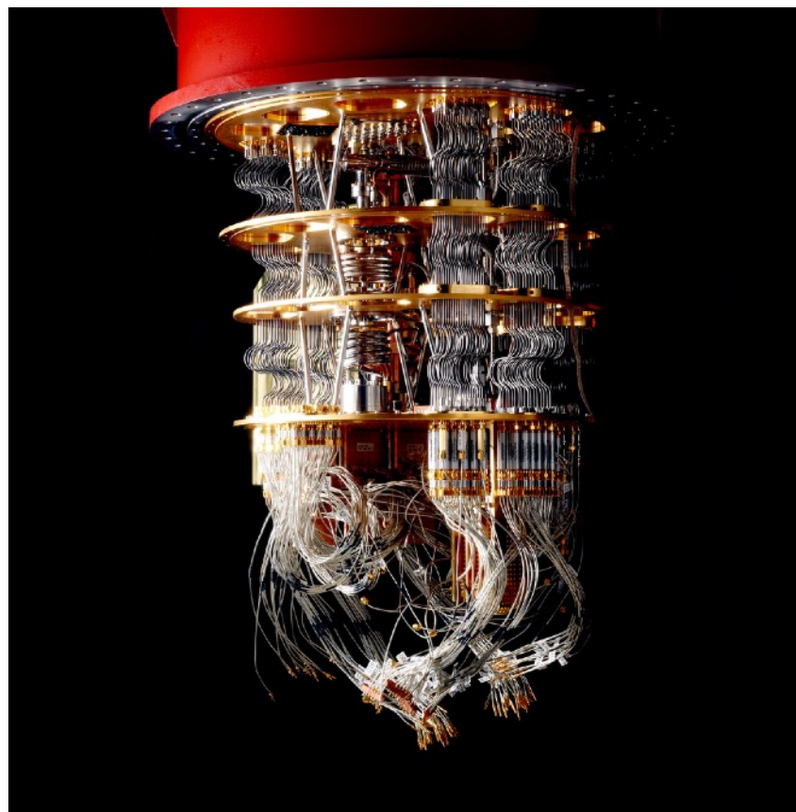
Decoherence time

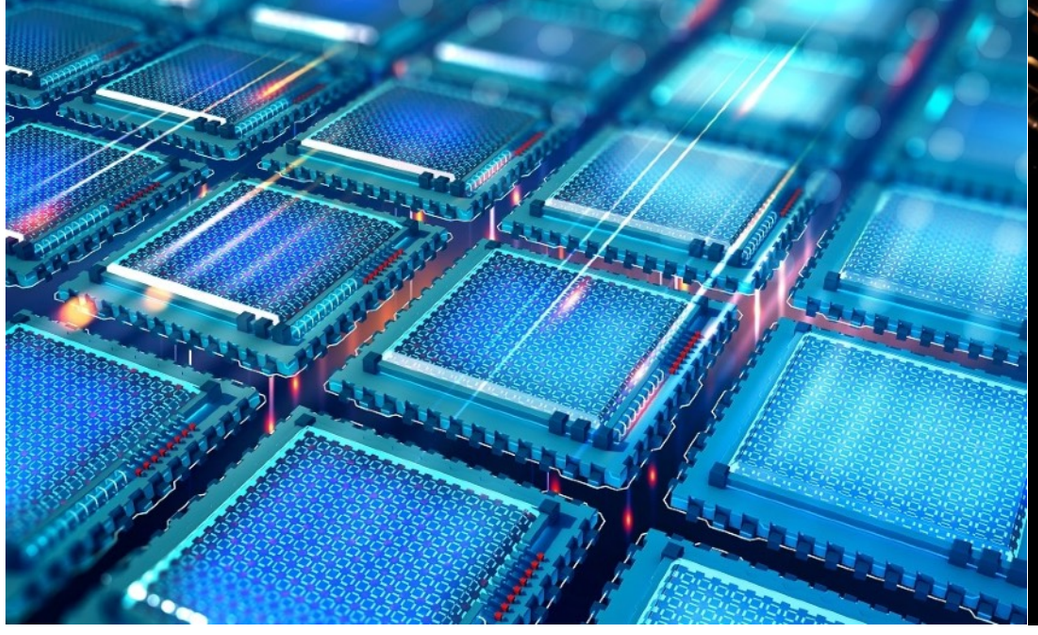
The time evolution in an isolated quantum system is unitary.

$$U|\psi_\alpha(t)\rangle = \mathrm{e}^{iE_\alpha t/\hbar}|\psi_\alpha\rangle$$

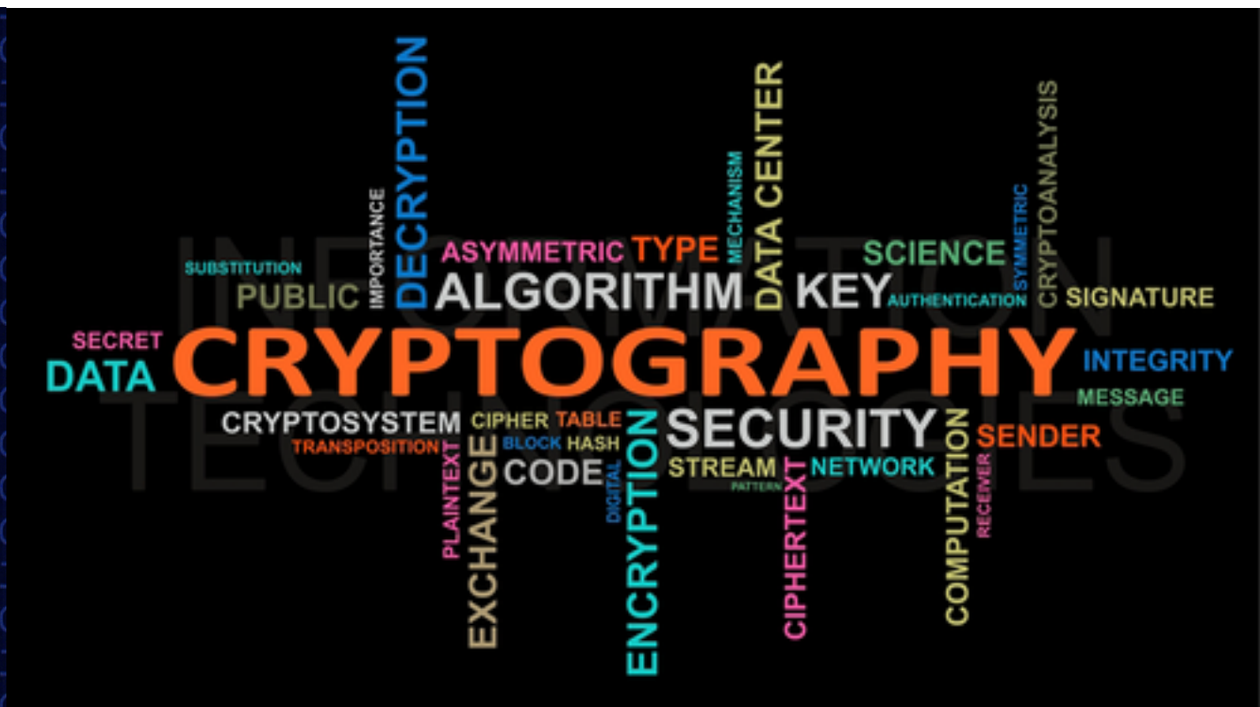
Small perturbations from the environment in individual qubits can make them evolve in time differently.

That could make the phase difference between the simultaneous 2^N states of the quantum computer change in time, eventually destroying quantum information!

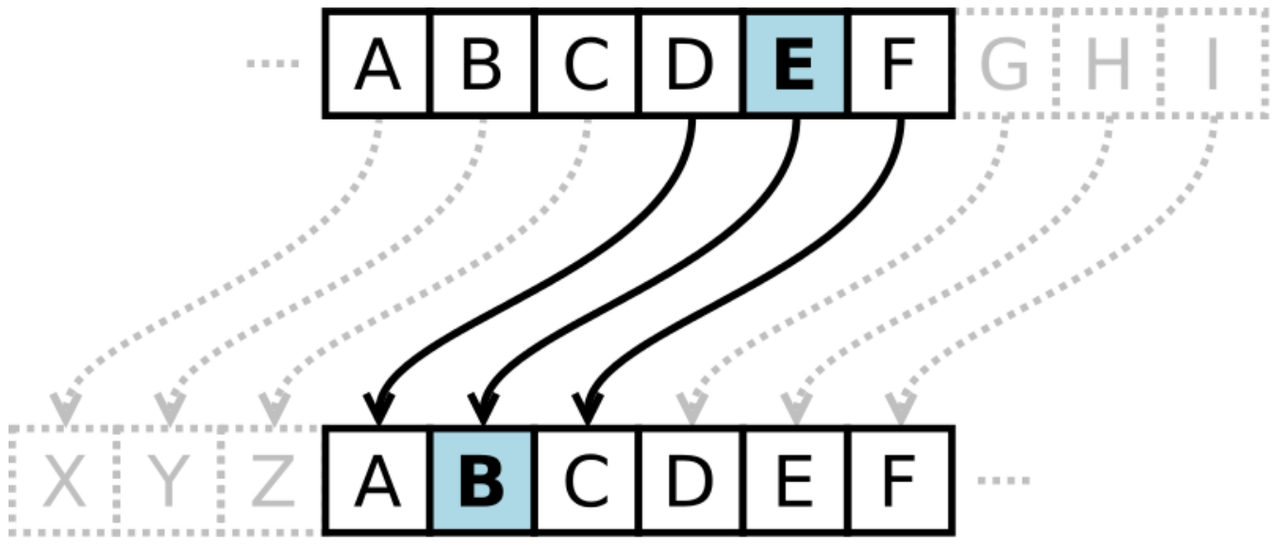




Quantum computers could be a game changer in the field of cryptography!

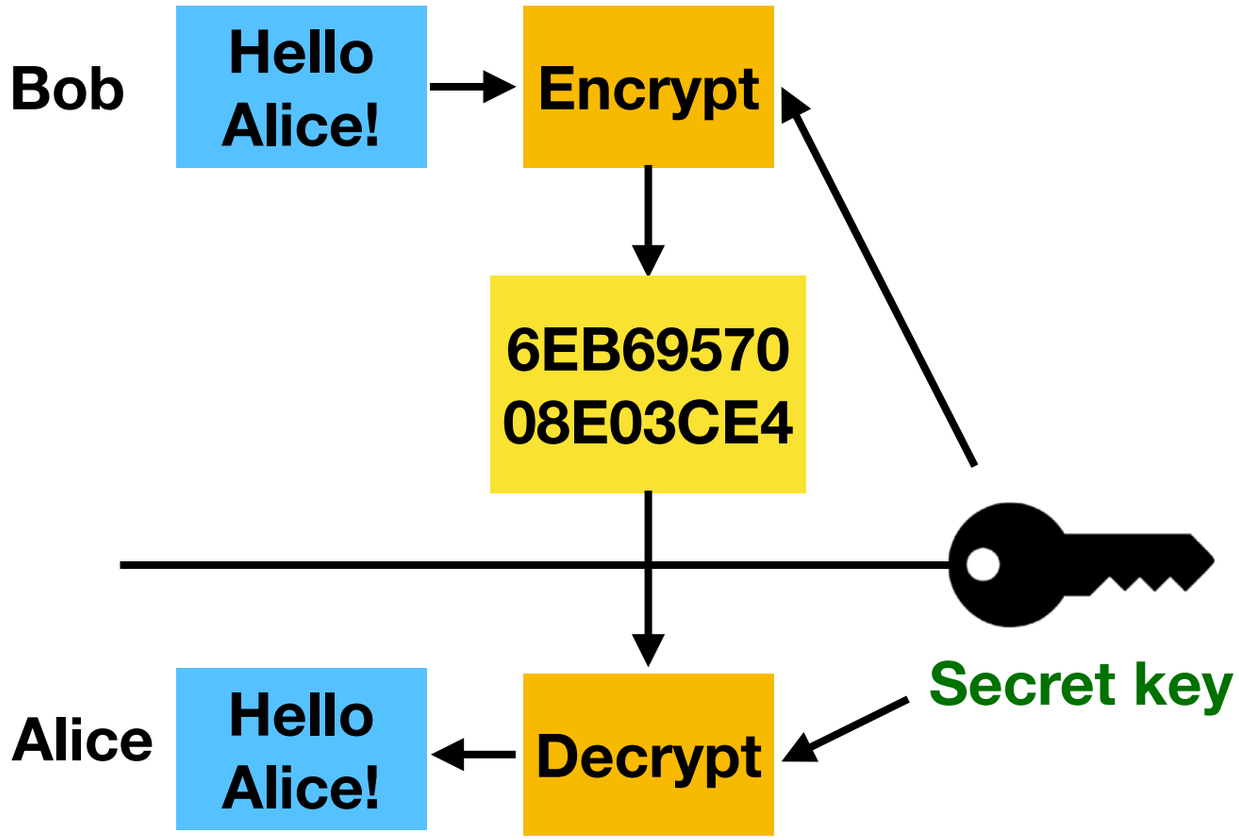


Data encryption



For thousands of years humans have tried to encrypt secret information.

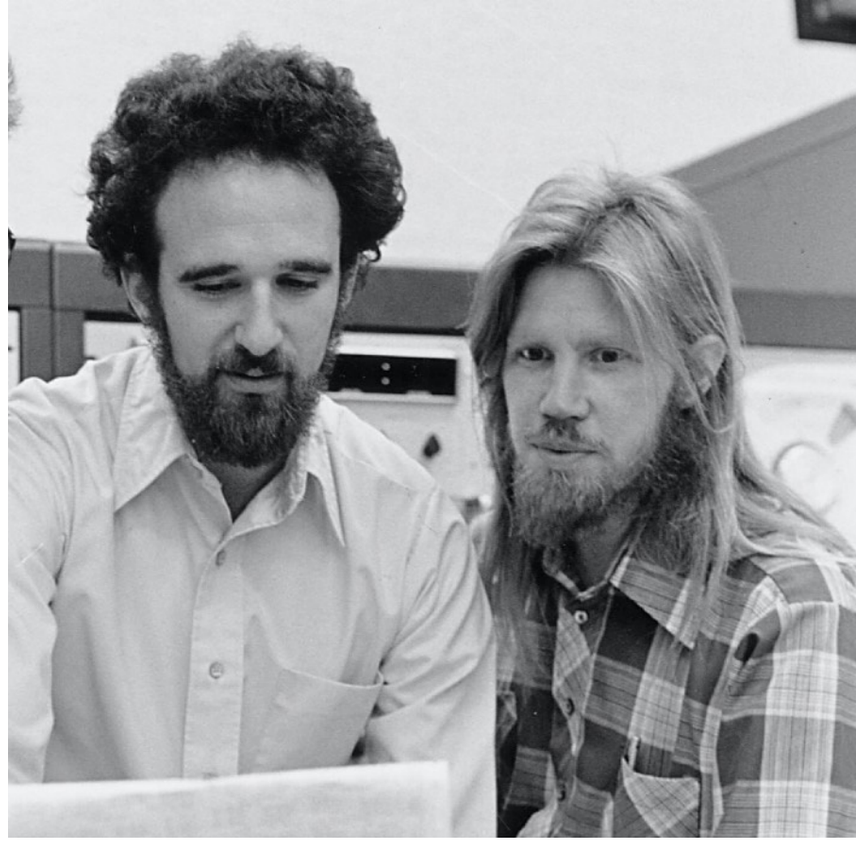
Data encryption



Until 1970's, all secret communications where secured with symmetric-key encryption, where both the sender and the receiver share the same secret key to encrypt and decrypt the message.

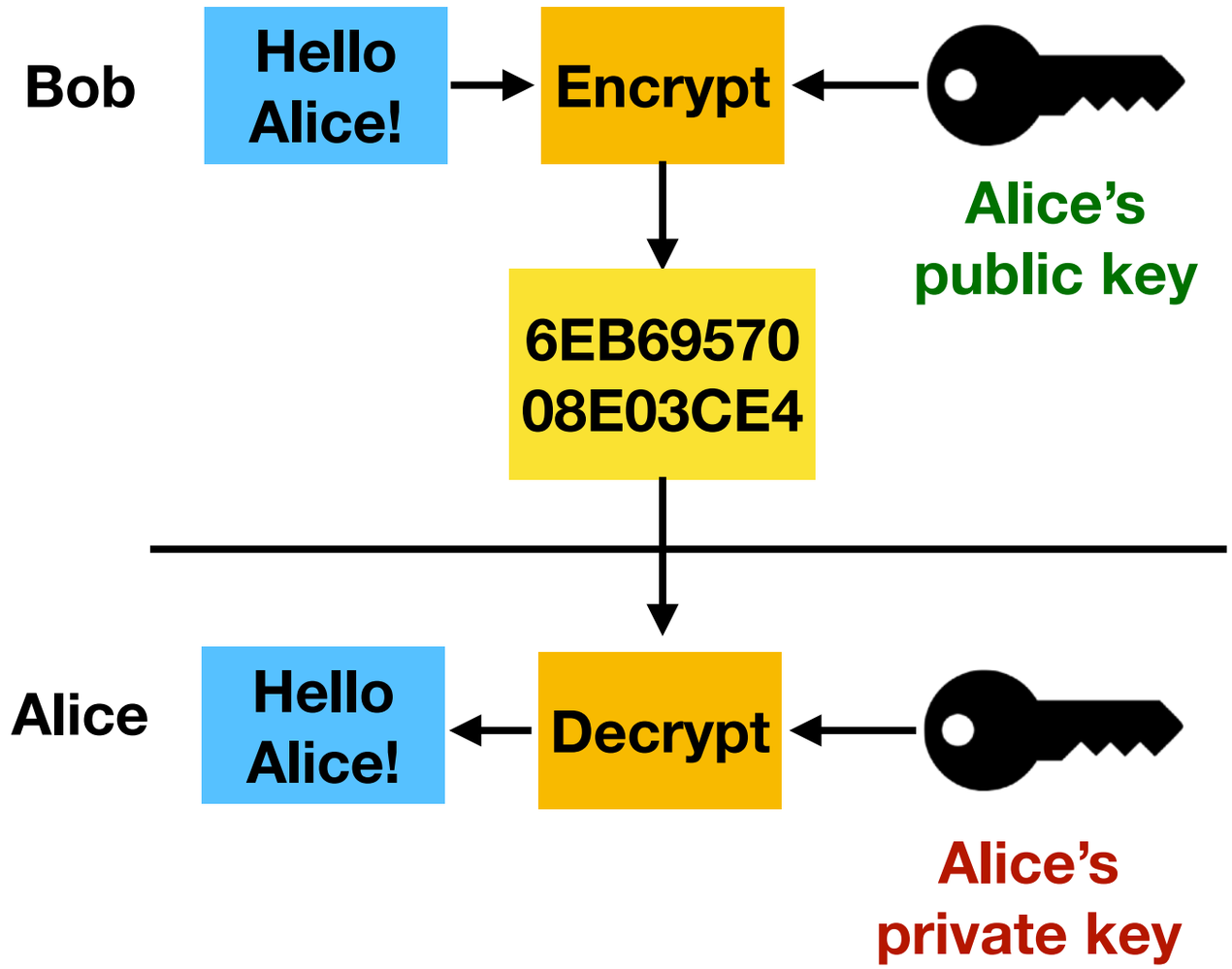
The problem is when someone intercepts that secret key!

Public-key encryption



In 1976, it was theoretically shown by Diffy and Hellman that one could safely encrypt messages with both public and a private keys (Public-key encryption).

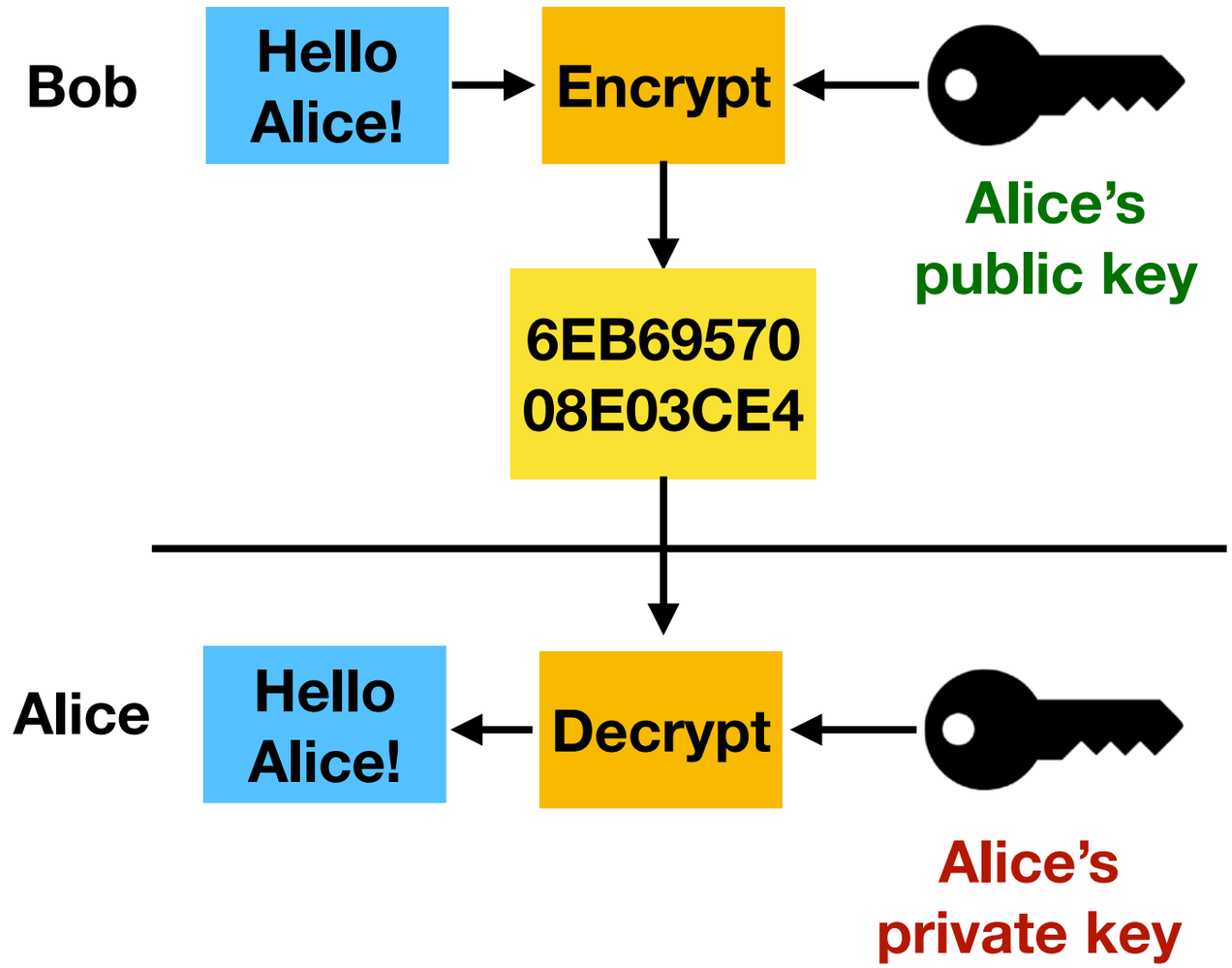
Public-key encryption



Alice wants to receive an encrypted message from Bob.

Alice shares a public key with Bob (and the rest of the world), which Bob uses to encrypt the message. But only Alice's private key can decrypt the message.

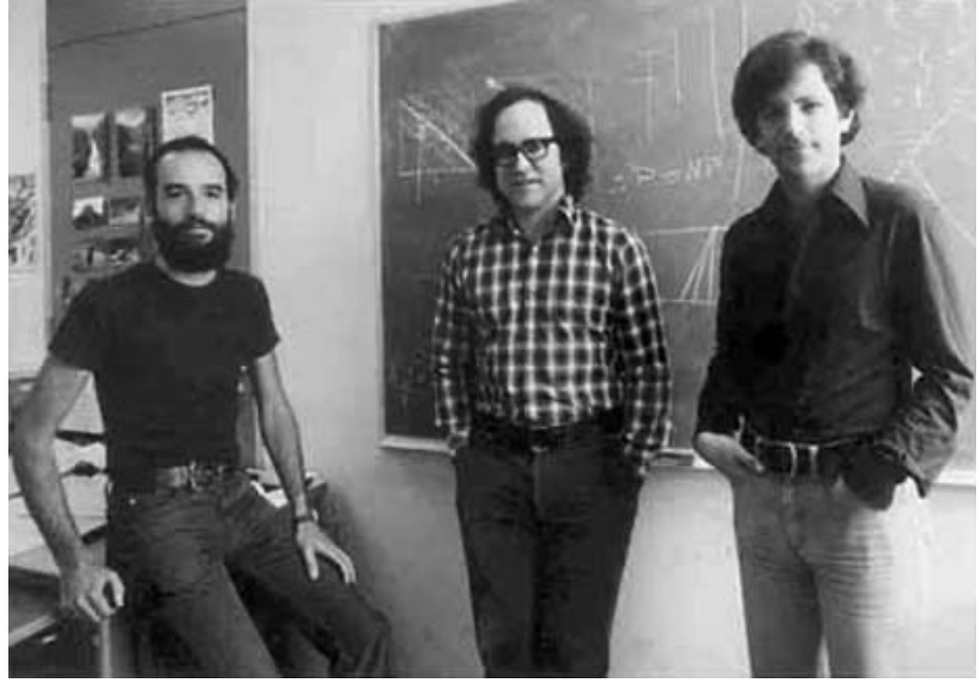
Public-key encryption



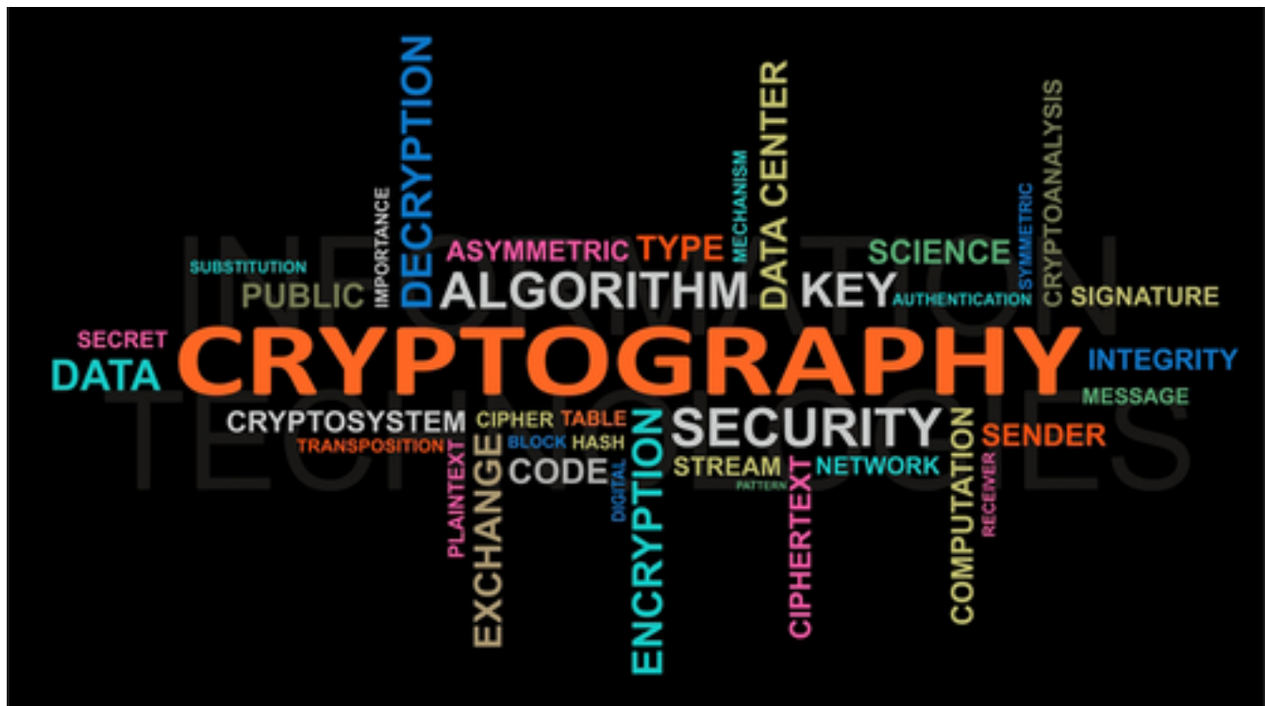
The idea is that one needs a simple one-to-one mathematical connection between the public and the private keys.

Alice's private key should be able to easily generate a unique public key. Conversely, it should be extremely difficult to infer the private key from the public one!

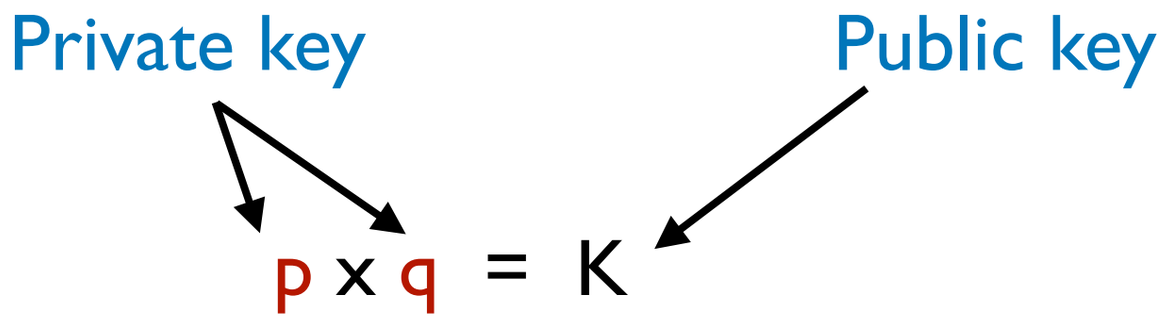
Public-key encryption



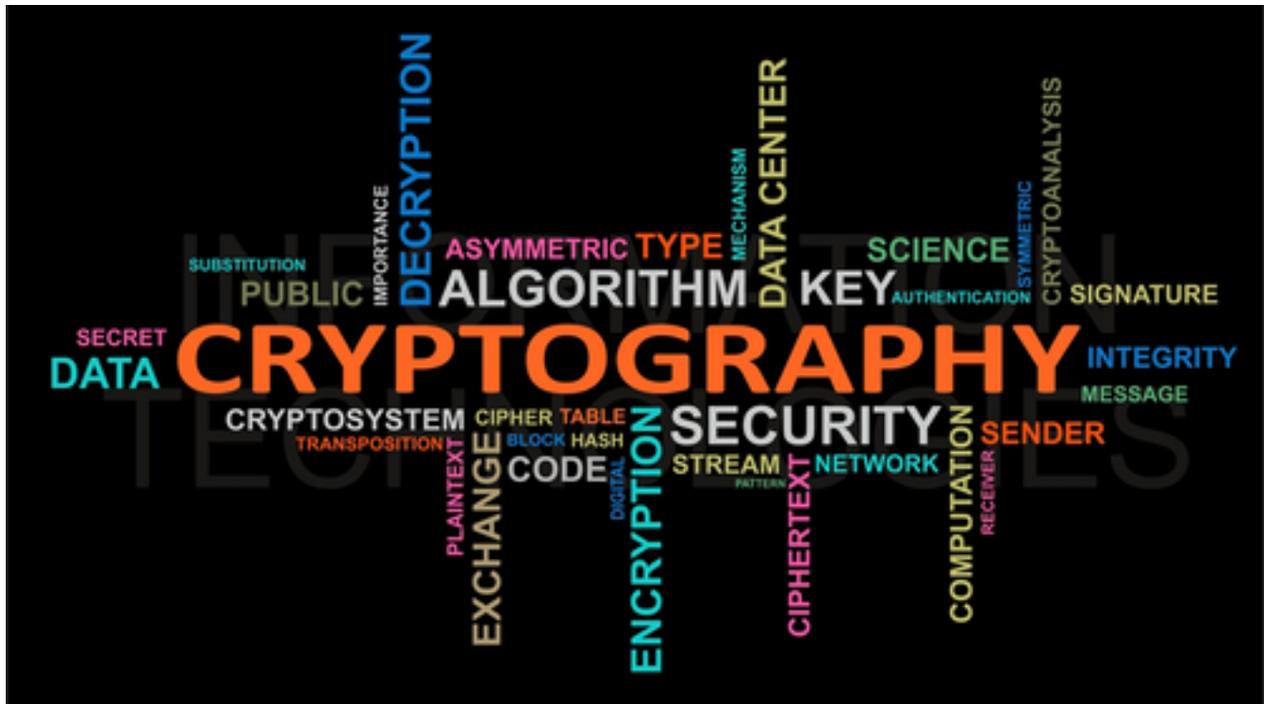
In 1979, three mathematicians from MIT (Rivest, Shamir and Adleman) developed the first algorithm to implement public-key encryption.



Public-key encryption



Public-key cryptography is based on the product of prime numbers!



Public-key encryption

$$p \times q = \underbrace{187{,}621{,}975{,}719{,}284{,}736{,}453{,}892{,}173{,}893{,}871{,}712{,}991{,}\ldots}_{\text{400 digits}}$$

For a 400 digit product (K) there are $\sqrt{K} \sim 10^{200}$ possibilities for p and q (and only one solution).

Data encryption

$$p \times q = \underbrace{187{,}621{,}975{,}719{,}284{,}736{,}453{,}892{,}173{,}893{,}871{,}712{,}991{,}\ldots}_{\text{400 digits}}$$

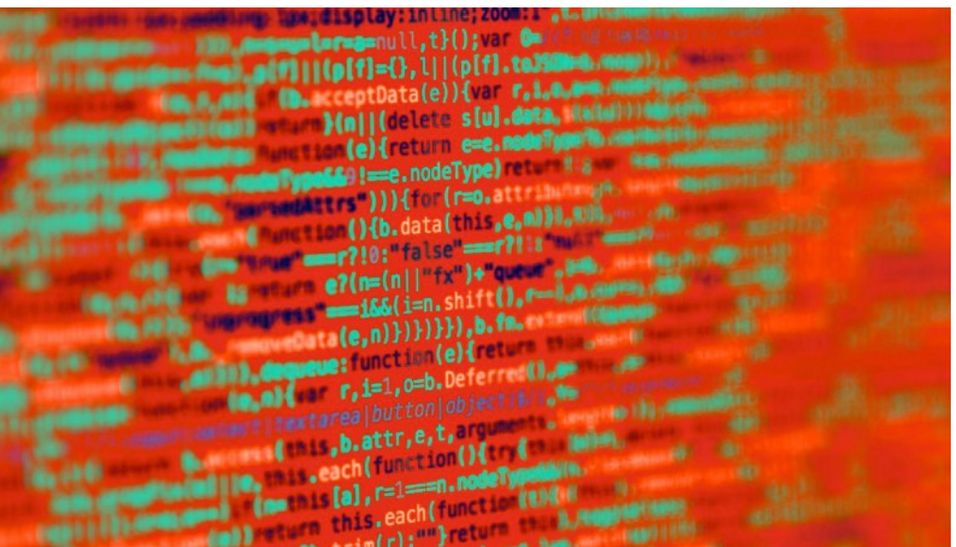
For a 400 digit product (K) there are $\sqrt{K} \sim 10^{200}$ possibilities for p and q (and only one solution).

A computer that can check 10^{12} combinations per second would take 10^{170} times the age of the universe (10^{18} s) to break encryption!

Data encryption

$$p \times q = \underbrace{187{,}621{,}975{,}719{,}284{,}736{,}453{,}892{,}173{,}893{,}871{,}712{,}991{,}\ldots}_{400\ \text{digits}}$$

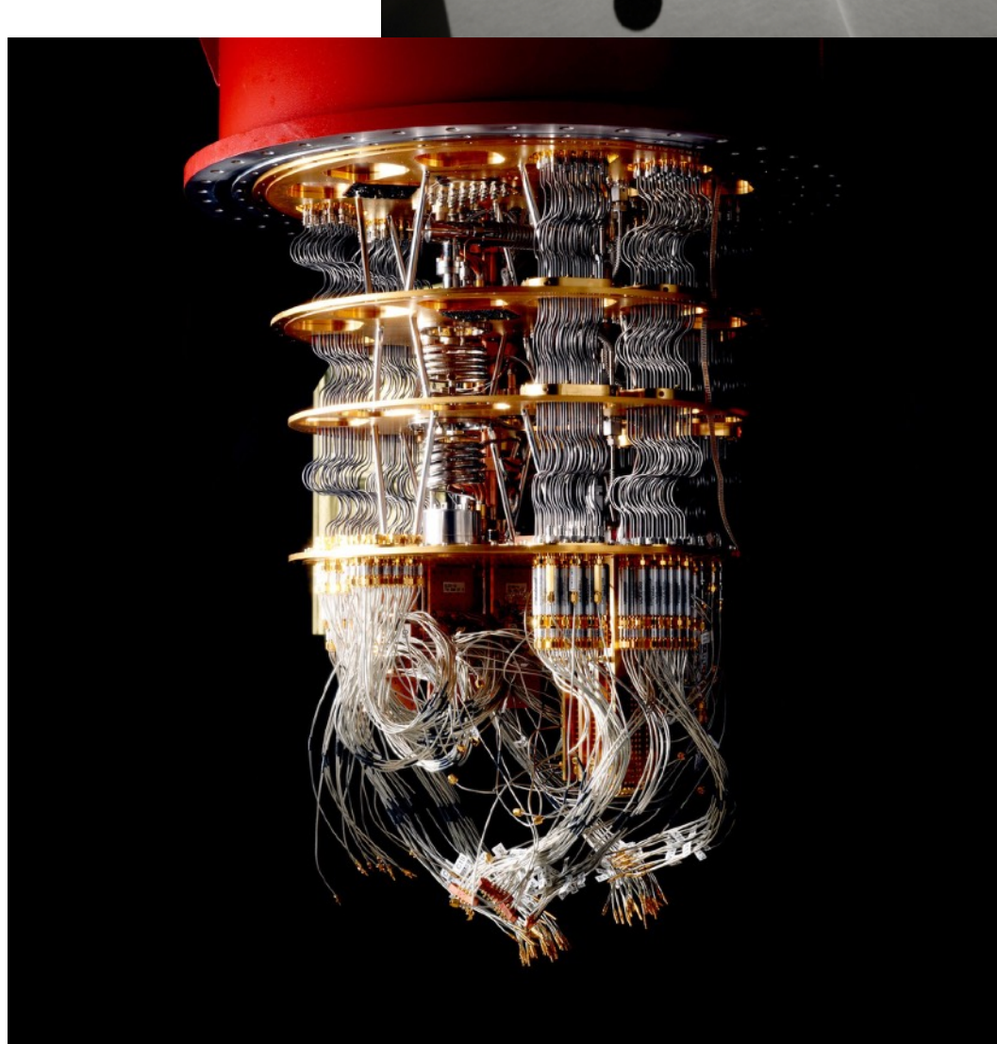
The problem of factorization of large numbers into the product of two prime numbers is NP (non-polynomial), as the complexity grows exponentially with the number of digits!



P=NP?

P≠NP

What about quantum computers?

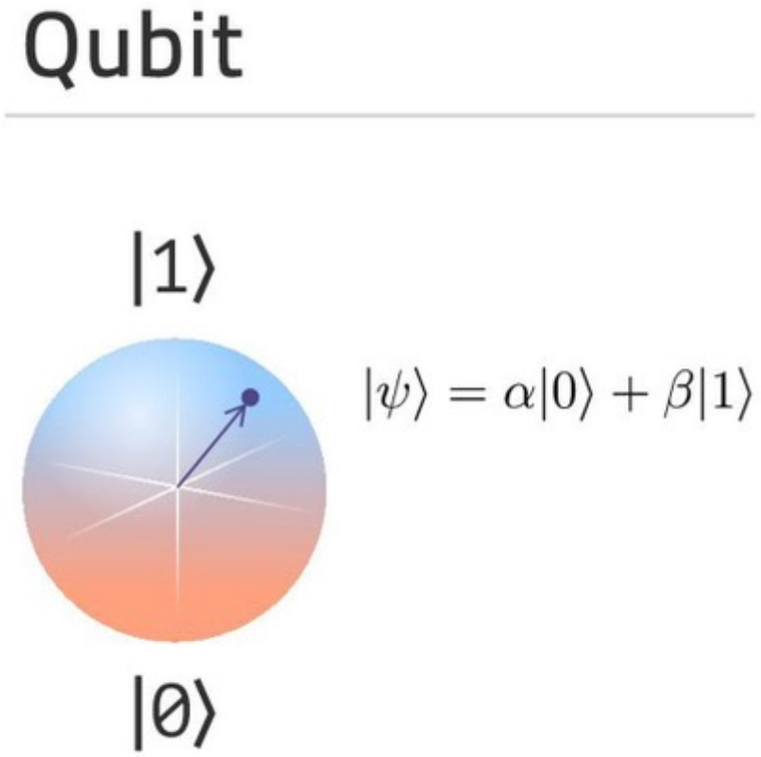


Shor algorithm

In 1994, Peter Shor demonstrated (theoretically) that a quantum computer can factorize an integer in polynomial time.

Quantum computers could break any public keys!

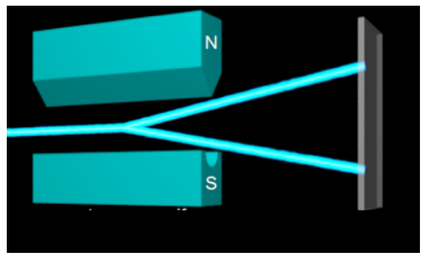
Quantum cryptography



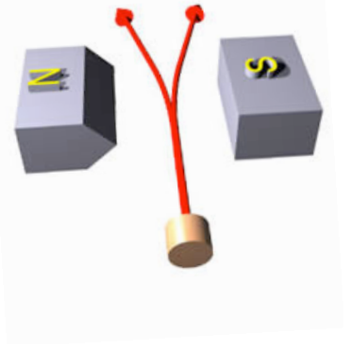
In a world with quantum computers, information can be securely transmitted with quantum encryption!

Quantum cryptography

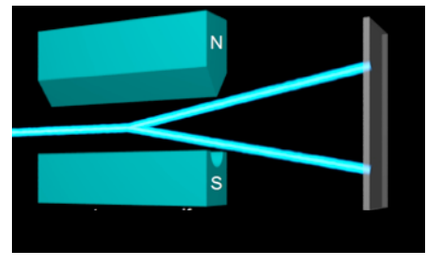
Bob



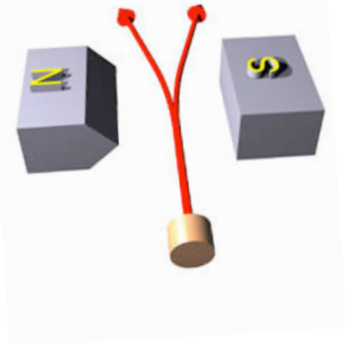
or



Alice



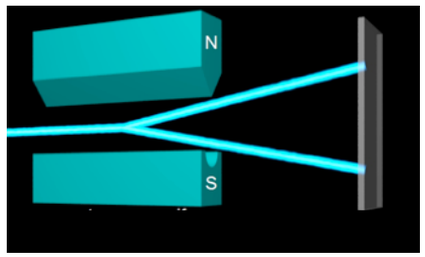
or



Suppose bob can send a qubit $|0\rangle$ or $|1\rangle$ from either a vertical or a horizontal apparatus. Alice can read the same qubit with either type of apparatus as well.

Quantum cryptography

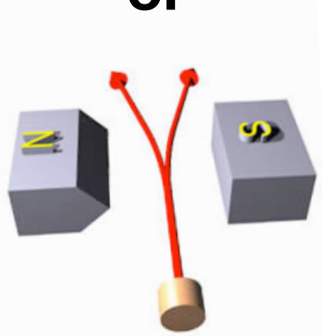
Bob



$|1\rangle$

$|0\rangle$

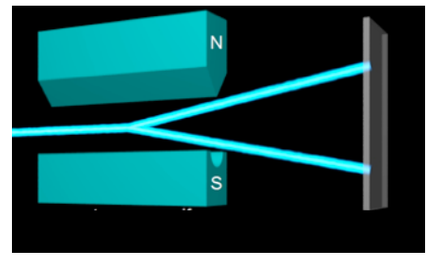
or



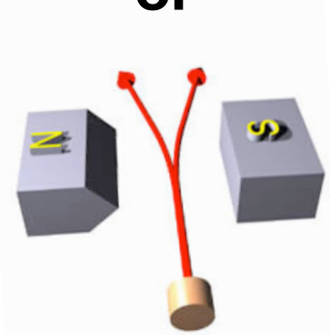
$$|1\rangle_x = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

$$|0\rangle_x = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

Alice



or



When Bob and Alice use the same apparatus, Alice will read the same qubits sent by Bob (sharp measurement).

When they use different apparatuses, Alice will read the correct qubits (1 or 0) only half the time (no information transmitted)!

Quantum cryptography

Alice and Bob would like to agree on a secure key that would prevent Eve to eavesdrop!

No-cloning theorem

It is impossible to create an independent and identical copy of an arbitrary unknown quantum state!

$$|\psi\rangle \nrightarrow |\psi\rangle|\psi\rangle$$

Two identical unknown quantum states must be entangled!

No-cloning theorem

Suppose there is a cloning operator

$$U_C|\alpha\rangle = |\alpha\rangle|\alpha\rangle$$

$$U_C|\beta\rangle = |\beta\rangle|\beta\rangle$$

If we define

$$|\gamma\rangle = |\alpha\rangle + |\beta\rangle$$

then

$$U_C|\gamma\rangle = U_C(|\alpha\rangle + |\beta\rangle) = |\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle \neq |\gamma\rangle|\gamma\rangle$$

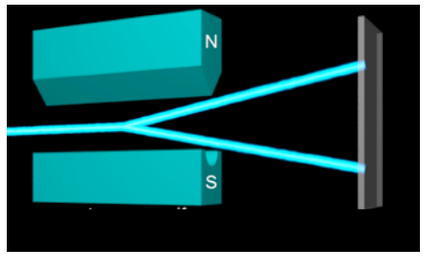
Therefore this operator does not exist!

No-cloning theorem

Eve

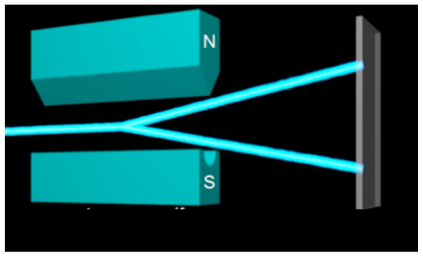
Bob

Alice

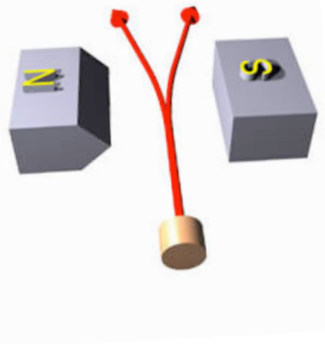


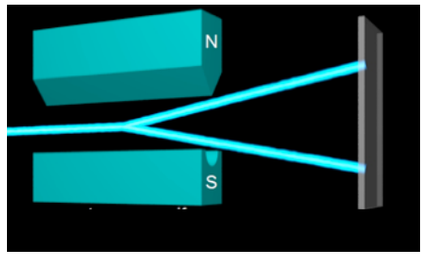
$|1\rangle$

$|0\rangle$



or

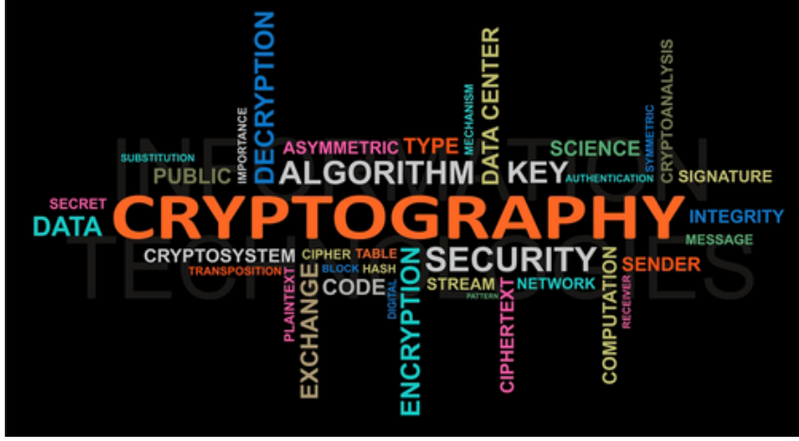


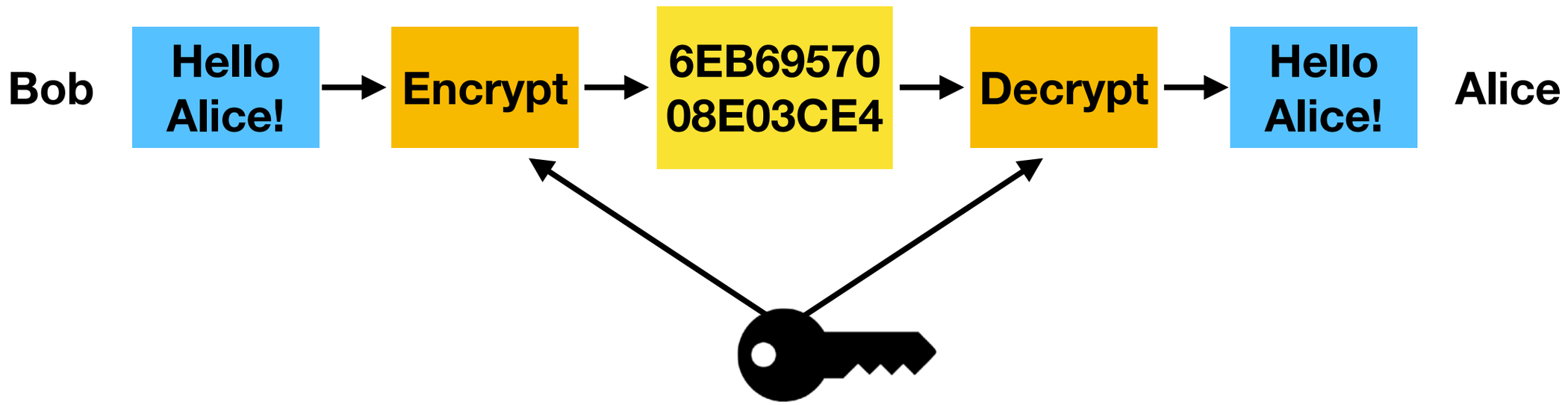


Eve cannot measure a qubit without destroying it.

Since Eve does not want Alice to know that she is intercepting the qubits, she will generate new qubits and send them to Alice.

BB84 Protocol (quantum key distribution)



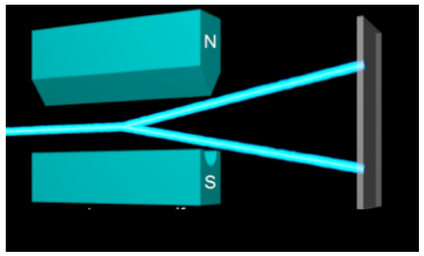


Suppose Bob wants to send Alice a private key for quantum decryption with n bits.

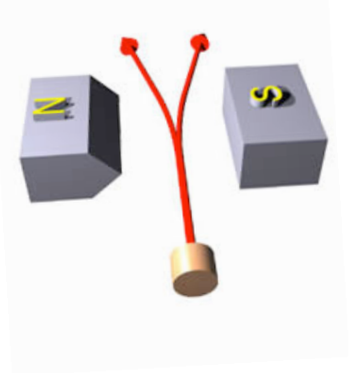
He wants to do it in a secure way, such that the key cannot be intercepted, not even by a quantum computer.

BB84 Protocol (quantum key distribution)

Bob **Alice**



or

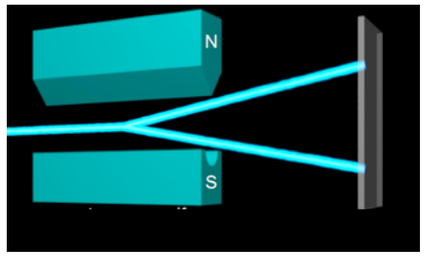


Bob sends Alice 4n qubits generated randomly in either a V or H apparatus and keeps a record of which apparatus generated each qubit.

Bob's record are two strings with 4n bits {V,V,H,V,H,H…} and {0,1,1,1,0,0…}

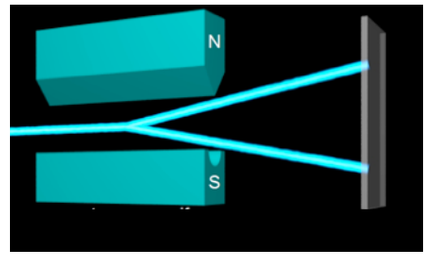
BB84 Protocol (quantum key distribution)

Bob



or

Alice



or

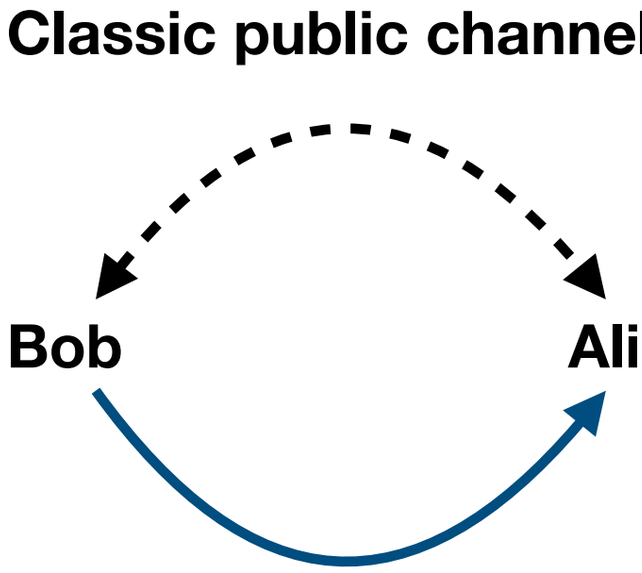
Alice measures the 4n qubits from Bob randomly in either a V or H apparatus and also keeps a record of which apparatus measured each qubit.

Alice's record are two different strings with also 4n bits, {V,H,H,V,V,H…} and {0,0,1,1,1,0,…}

BB84 Protocol (quantum key distribution)

Alice and Bob are only interested in the bits where the apparatuses agree.

After Alice publicly announces that the transmission is over, they compare their strings of H's and V's



Bob

$\{V, V, H, V, H, H, \cdots\}$

✓ ✗ ✓ ✓ ✗ ✓

Alice

$\{V, H, H, V, V, H, \ldots\}$

✓ ✗ ✓ ✓ ✗ ✓

in a public channel (classic), and discard the bits where they disagree.

BB84 Protocol (quantum key distribution)

Alice

$\{V, V, H, V, H, H, \cdots\}$

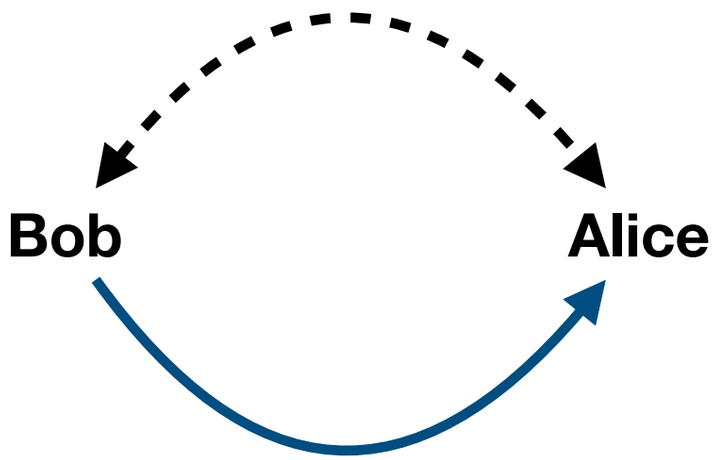
✓ ✖ ✓ ✓ ✖ ✓

$\underbrace{\{0, 0, 1, 1, 1, 0, \ldots\}}_{4n}$

$\underbrace{\{0, 1, 1, 0, \ldots\}}_{2n}$

Randomly choose n bits and compare

Classic public channel



Quantum channel

Alice and Bob now randomly pick n bits in the strings of 0's and 1's (length 2n) and compare them in the public channel.

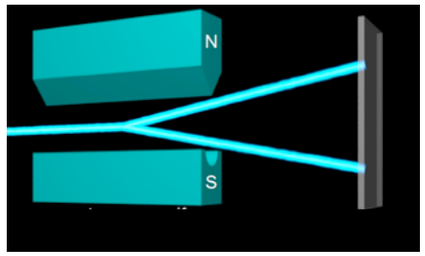
If Eve is not eavesdropping, all n bits will agree. The channel is secure and hence the other n bits can be used as a private key!

BB84 Protocol (quantum key distribution)

Eve

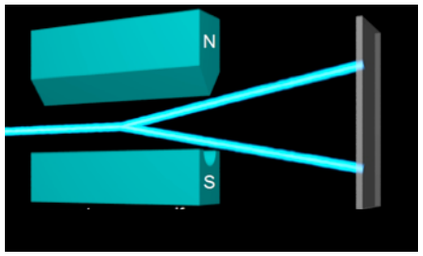
Bob

Alice

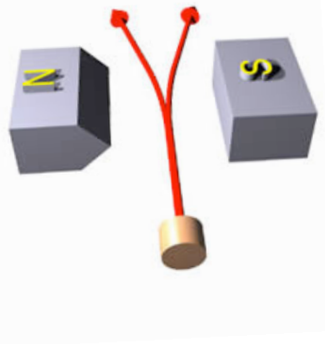


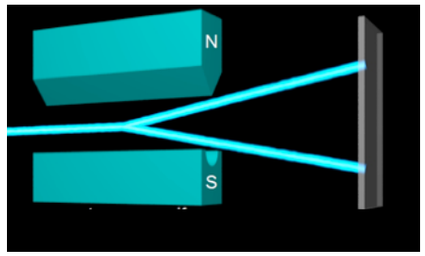
$|1\rangle$

$|0\rangle$



or

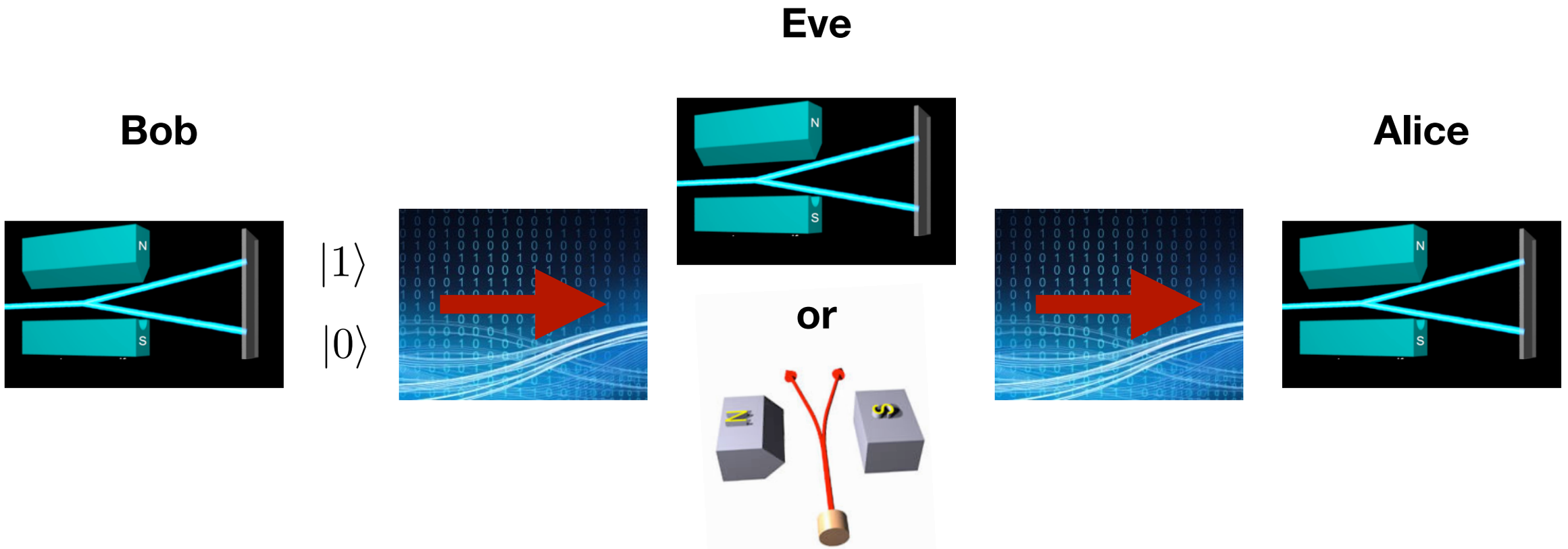




Suppose now that Eve is eavesdropping. When Bob and Alice's apparatuses agree, Eve's apparatus will disagree half the time.

When Eve's apparatus disagrees with the one of Bob and Alice, Alice will receive no information.

BB84 Protocol (quantum key distribution)

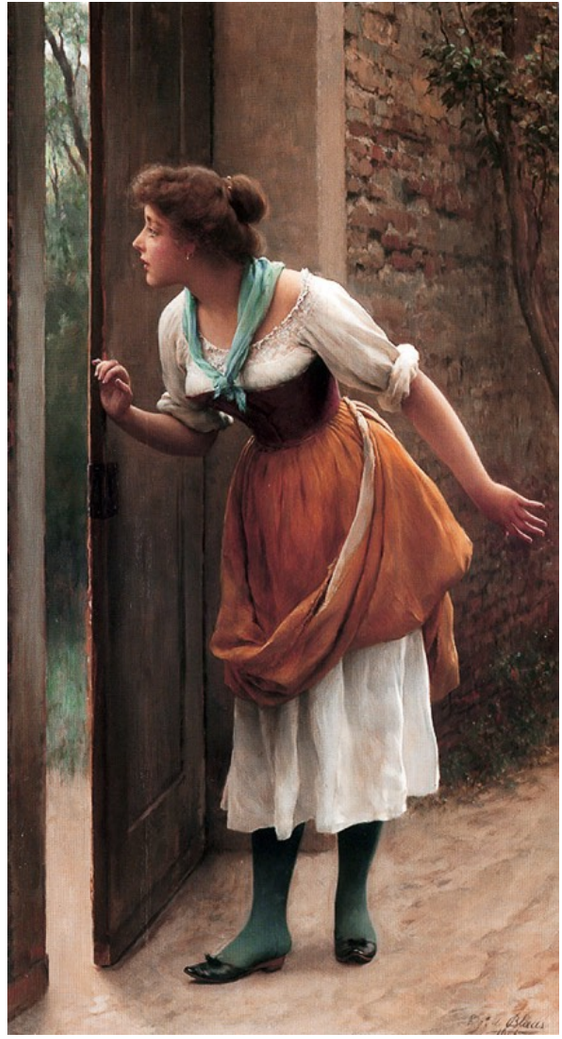


Alice will read the correct qubits with certainty only when Bob, Alice and Eve's apparatuses agree.

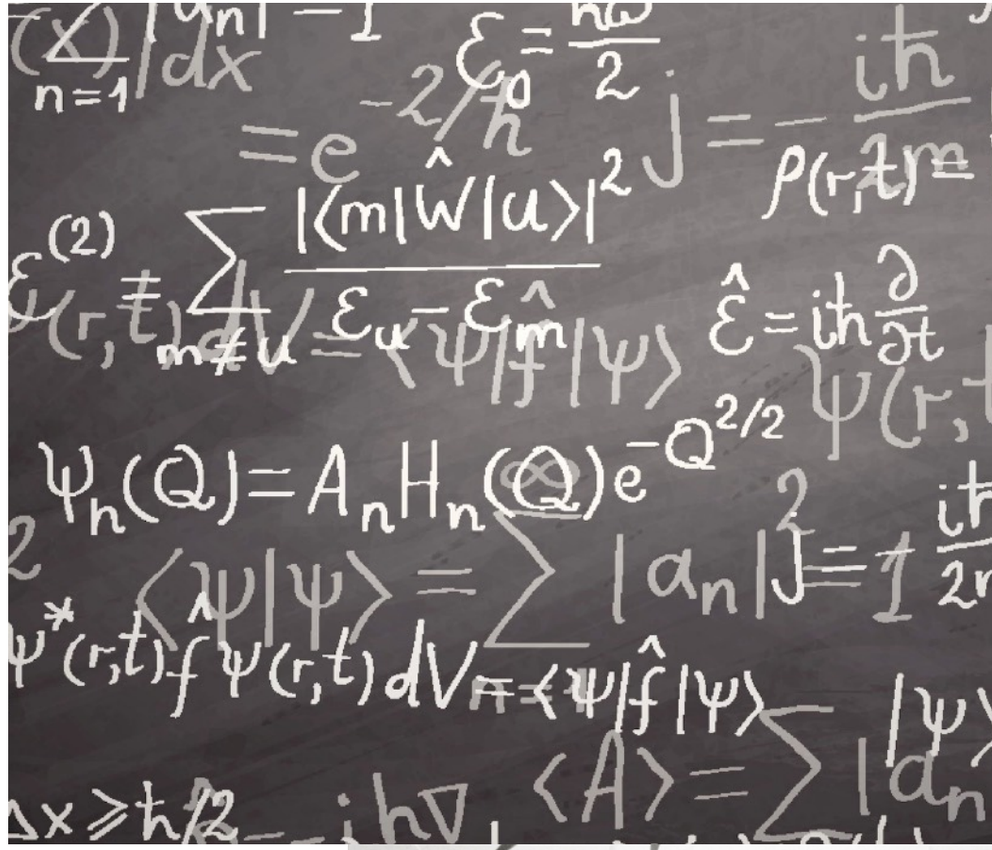
When Eve's apparatus is different, Alice will read the correct qubits only half the time.

BB84 Protocol (quantum key distribution)

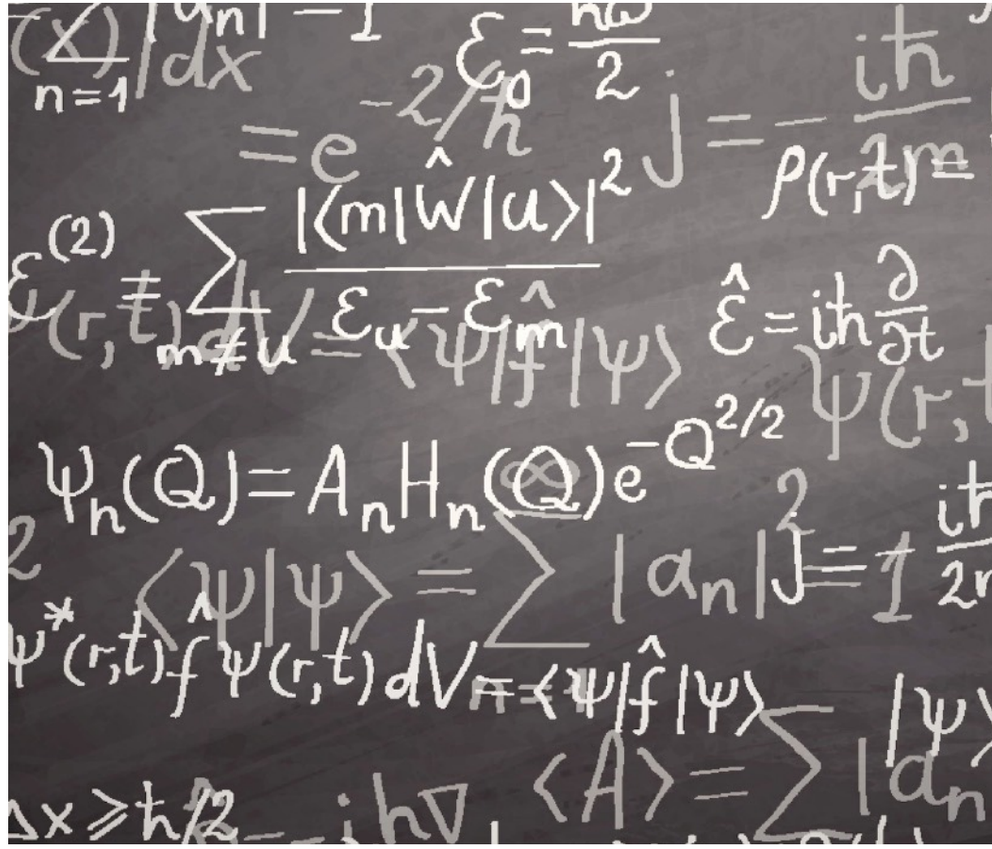
Hence, when Bob and Alice compare n random bits of 0's and 1's in their strings of length 2n, a quarter of the bits will not will match.



They know that they were eavesdropped and need to find another way to communicate!

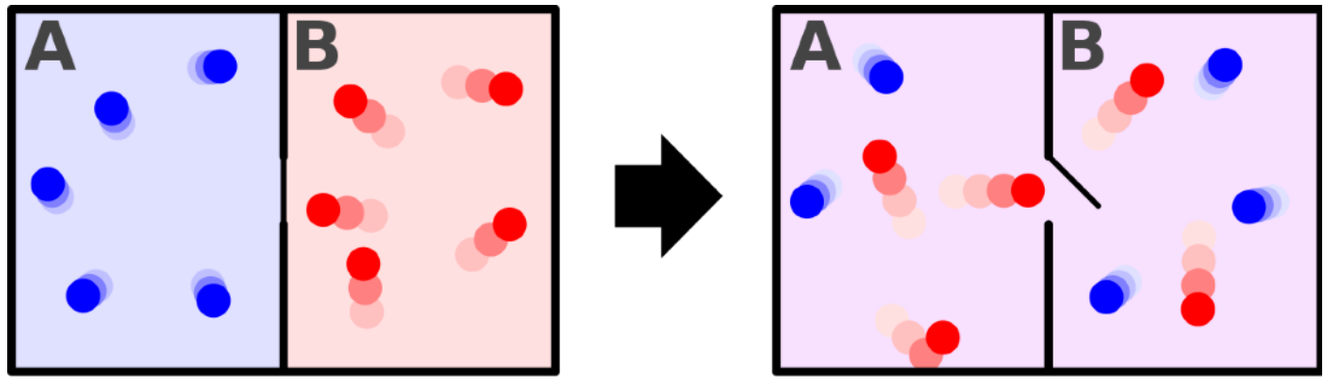


What other unusual properties quantum mechanics has?



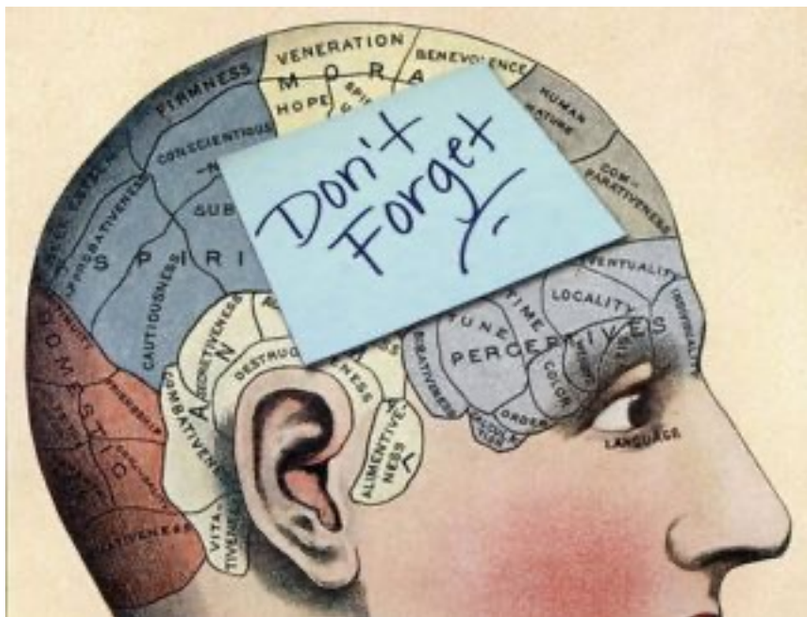
Closed quantum mechanical systems are reversible because time evolution is unitary.

Therefore the system should retain its memory of the initial conditions.



However, in statistical mechanics, thermalization implies that the system explores every possible configuration before settling down in the most likely one at long times (the system forgets its initial state)!

How do closed quantum systems thermalize?



Eigenstate thermalization hypotesis

$$|\psi(t)\rangle = e^{-i\hat{H}t}|\psi(0)\rangle = \sum_\alpha A_\alpha e^{-iE_\alpha t}|\alpha\rangle$$

$$p_\alpha = |A_\alpha|^2$$

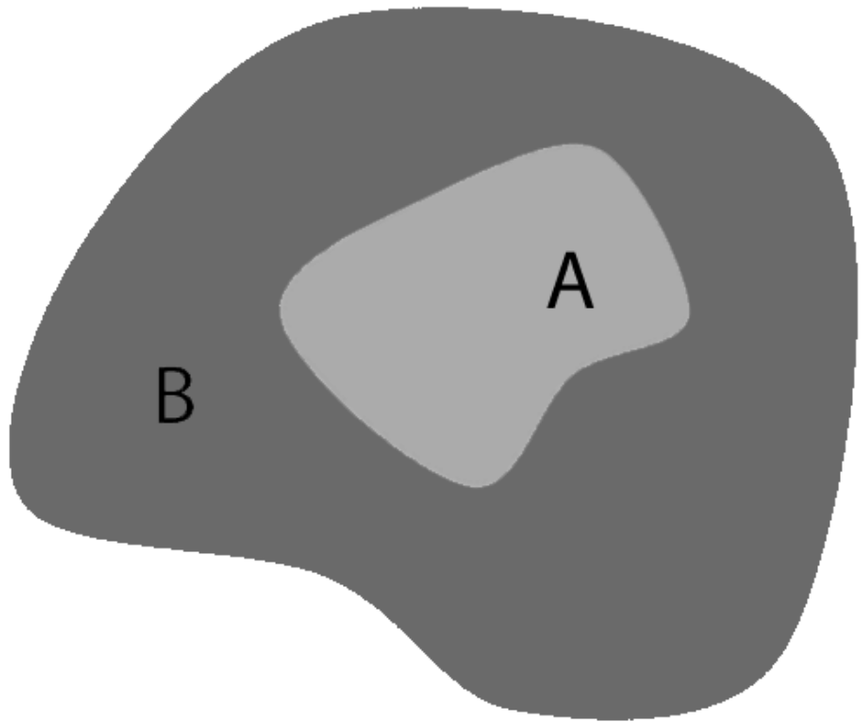
$$\langle \hat{O} \rangle_\infty = \lim_{T\to\infty} \frac{1}{T} \int_0^T \langle\psi(t)|\hat{O}|\psi(t)\rangle dt = \sum_\alpha p_\alpha \langle\alpha|\hat{O}|\alpha\rangle$$

Micro canonical?

At sufficiently long times, in most closed quantum systems, the expectation value of an observable approaches the thermodynamic one in the micro canonical ensemble (thermalization)!

Eigenstate thermalization hypotesis

$$|\psi(t)\rangle = e^{-i\hat{H}t}|\psi(0)\rangle = \sum_{\alpha} A_\alpha e^{-iE_\alpha t}|\alpha\rangle$$

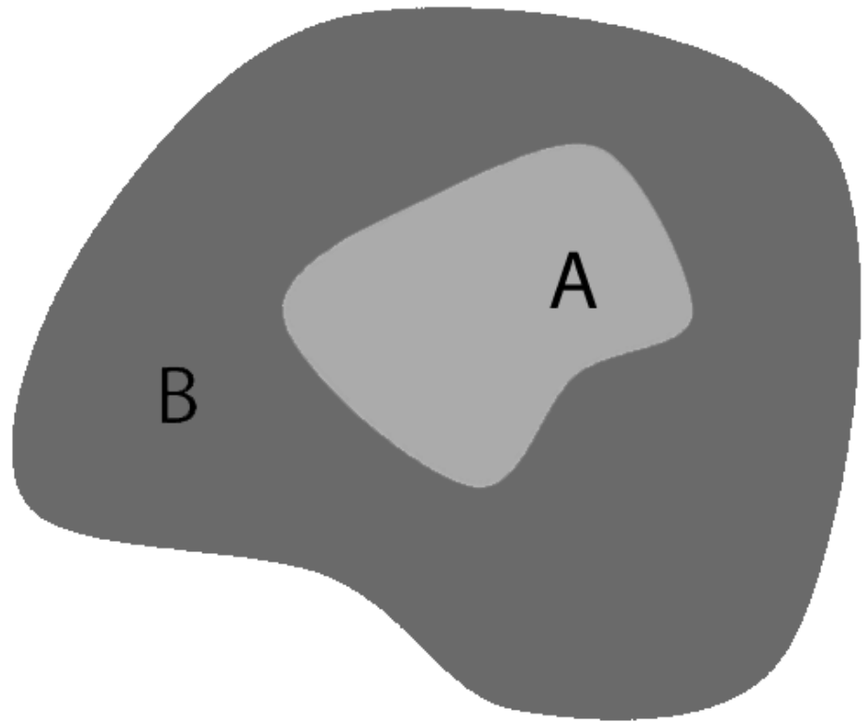


In breaking a quantum system in two subsystems, A and B, the amount of entanglement between them scales with the volume of the system.

The quantum system can explore all possible states (superposition).

Eigenstate thermalization hypotesis

$$|\psi(t)\rangle = e^{-i\hat{H}t}|\psi(0)\rangle = \sum_{\alpha} A_\alpha e^{-iE_\alpha t}|\alpha\rangle$$

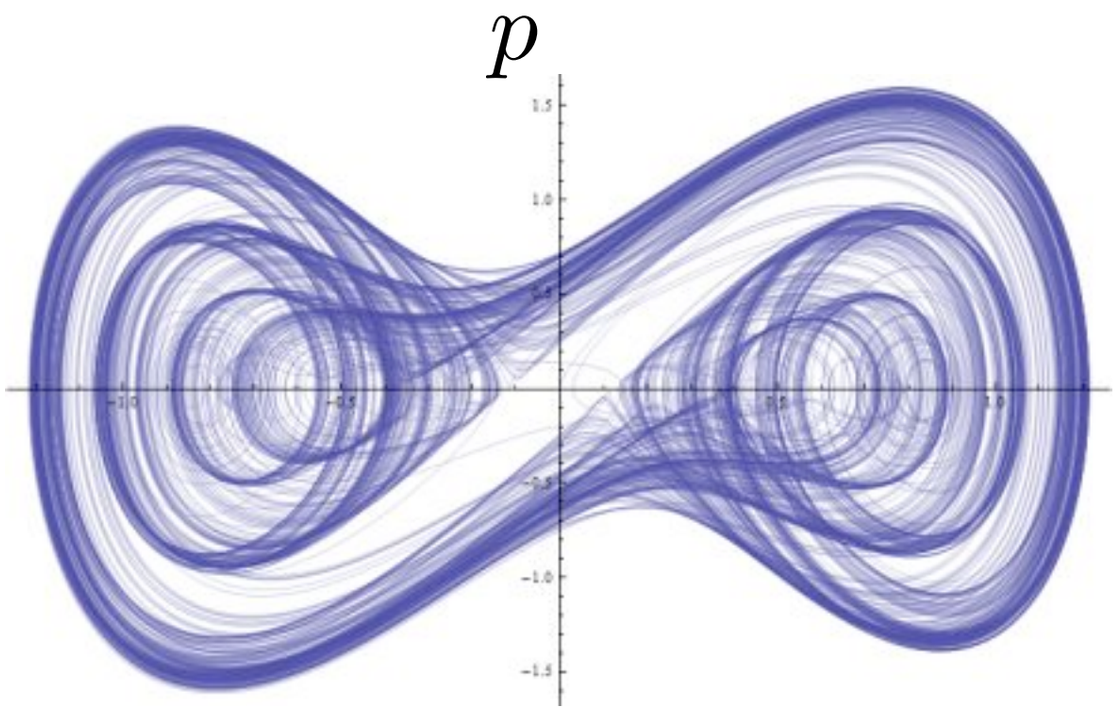


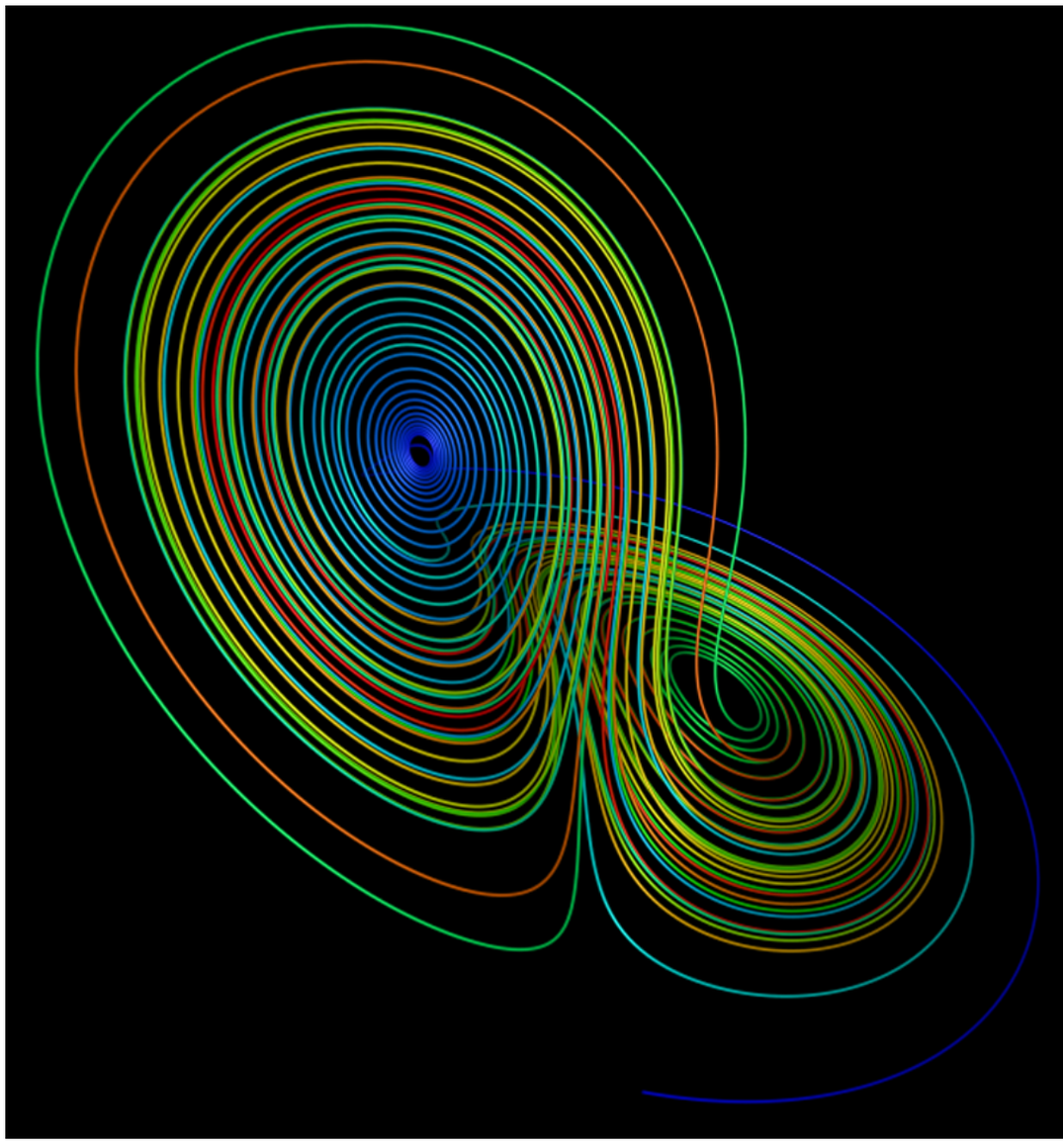
If one performs a local measurement, the expectation value of the observable appears to be the thermodynamic one.

The information of the initial state is spread all over the system (scrambled) and appears lost!

Subsystem B behaves as a thermal bath for A, allowing it to thermalize and vice versa.

Dynamical systems





In nature, the universe of possible dynamic configurations of an isolated system can be mapped into semiclassical orbits inside the phase space.

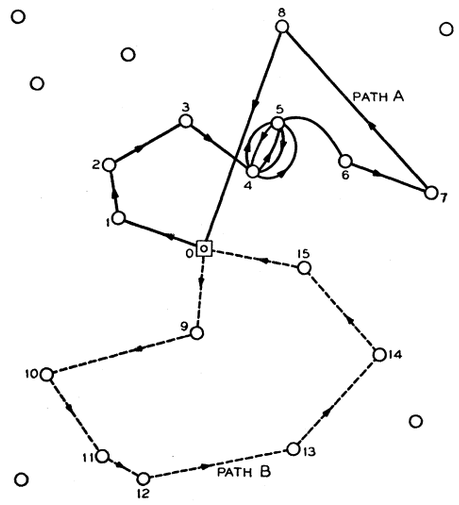
PHYSICAL REVIEW VOLUME 109, NUMBER 5 MARCH 1, 1958

Absence of Diffusion in Certain Random Lattices

P. W. ANDERSON
Bell Telephone Laboratories, Murray Hill, New Jersey

(Received October 10, 1957)

This paper presents a simple model for such processes as spin diffusion or conduction in the "impurity band." These processes involve transport in a lattice which is in some sense random, and in them diffusion is expected to take place via quantum jumps between localized sites. In this simple model the essential randomness is introduced by requiring the energy to vary randomly from site to site. It is shown that at low enough densities no diffusion at all can take place, and the criteria for transport to occur are given.

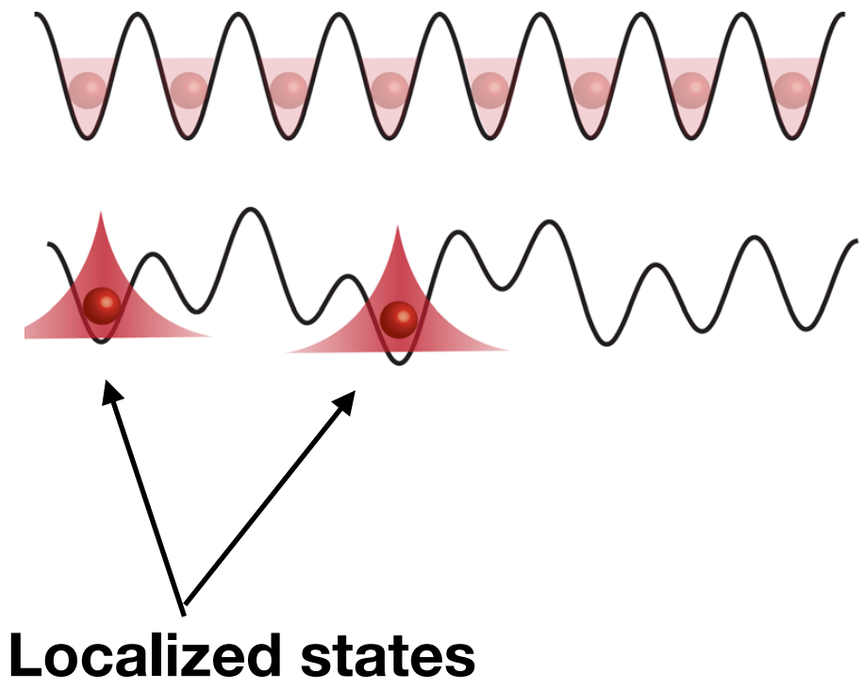


In 1958, Philip Anderson realized that some metals become insulators when disordered.

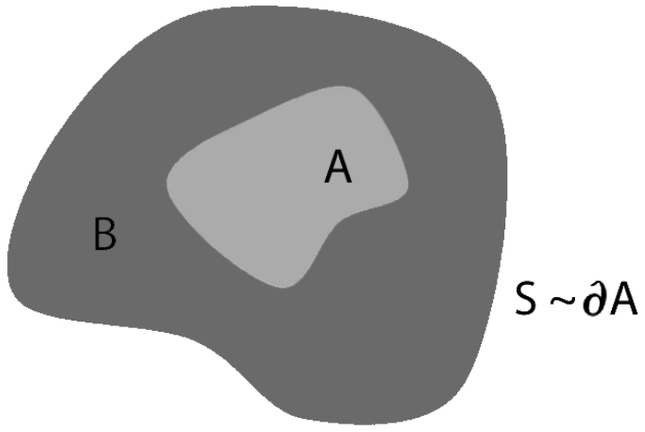
Due to quantum mechanical interference, the electrons stop diffusing across the lattice and become localized wave-functions.

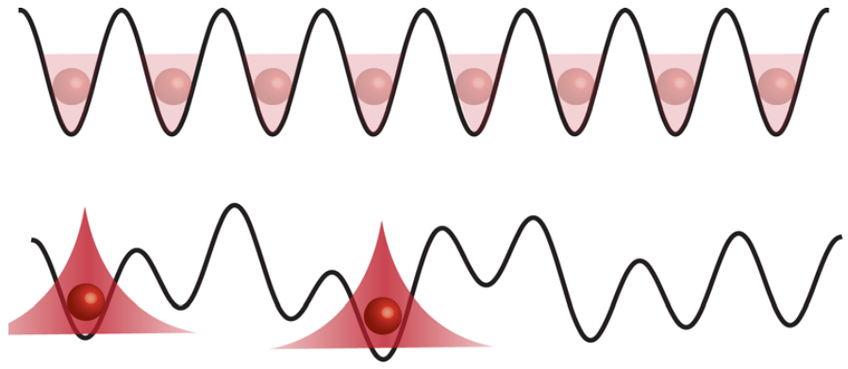
Anderson localization

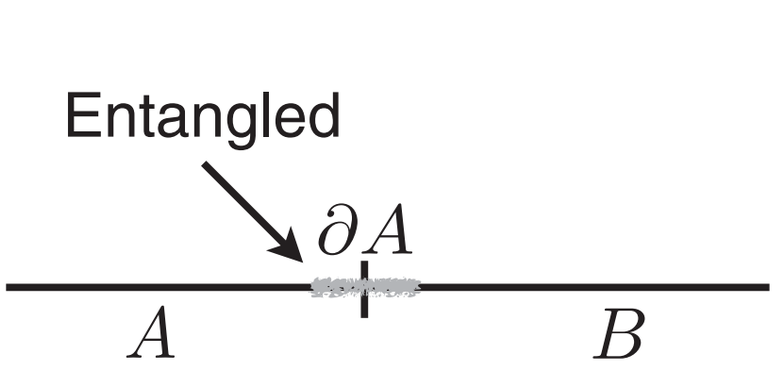
The Nobel Prize in Physics 1977 was awarded jointly to Philip Warren Anderson, Sir Nevill Francis Mott and John Hasbrouck Van Vleck "for their fundamental theoretical investigations of the electronic structure of magnetic and disordered systems."

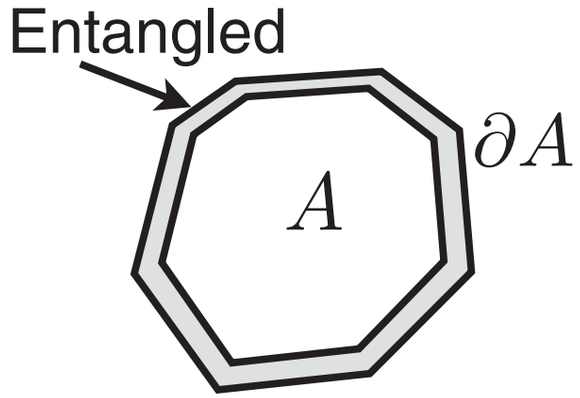


Because the electrons are localized, they cannot explore the phase space and therefore may fail to thermalize even at very long times!



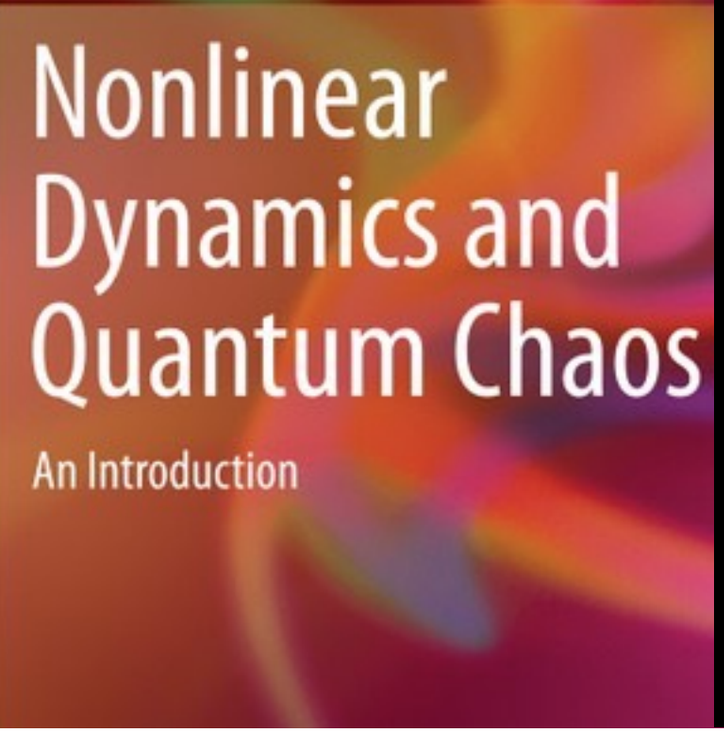


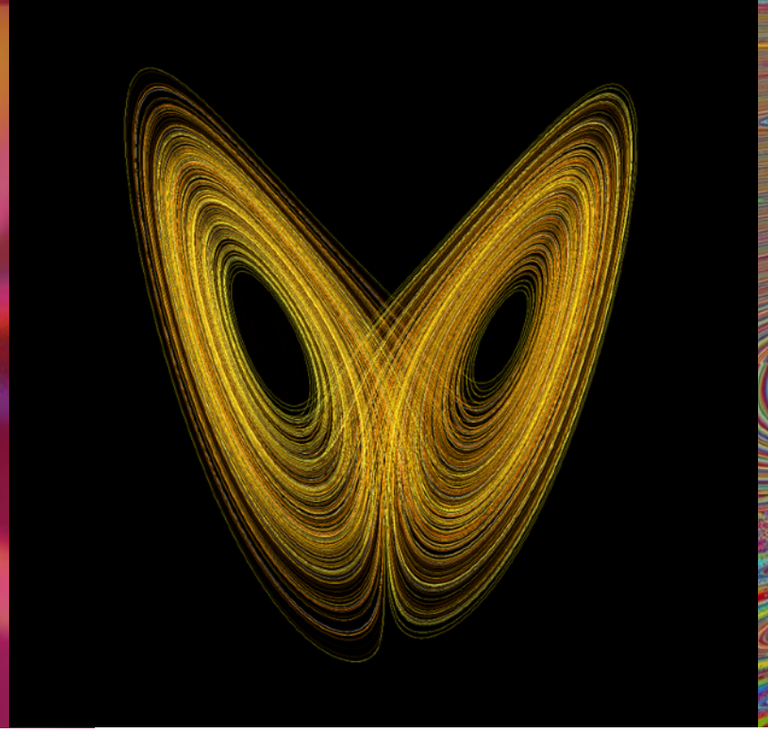


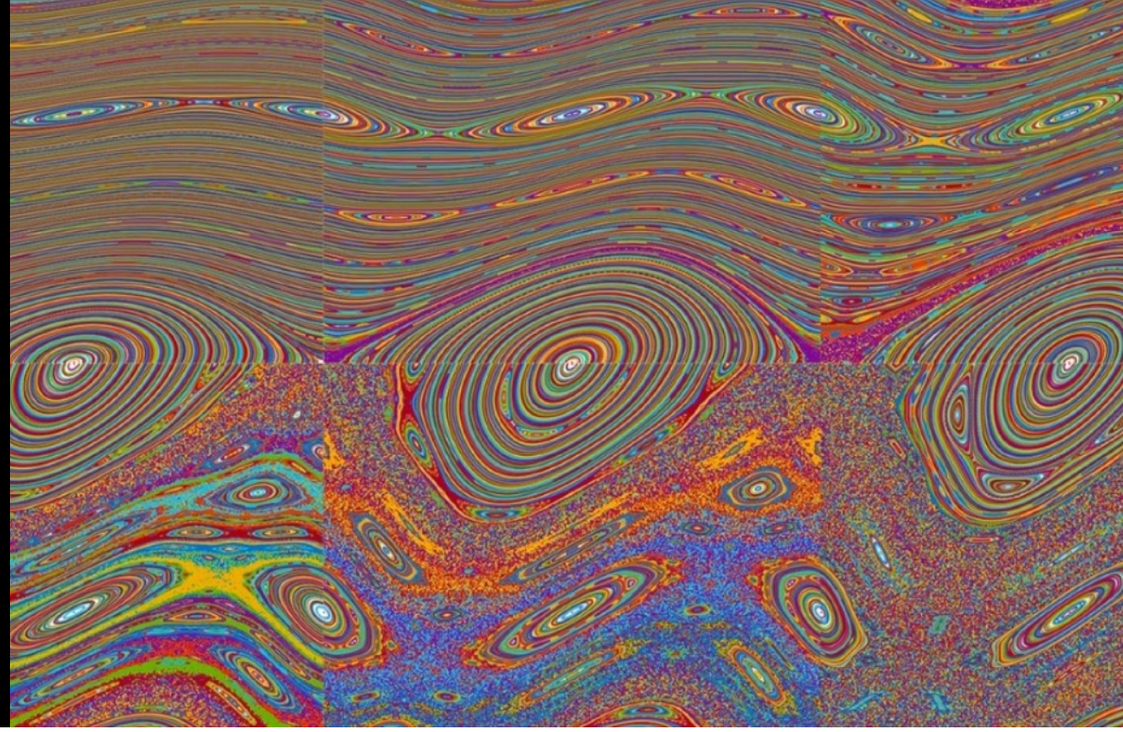


The system does not thermalize!

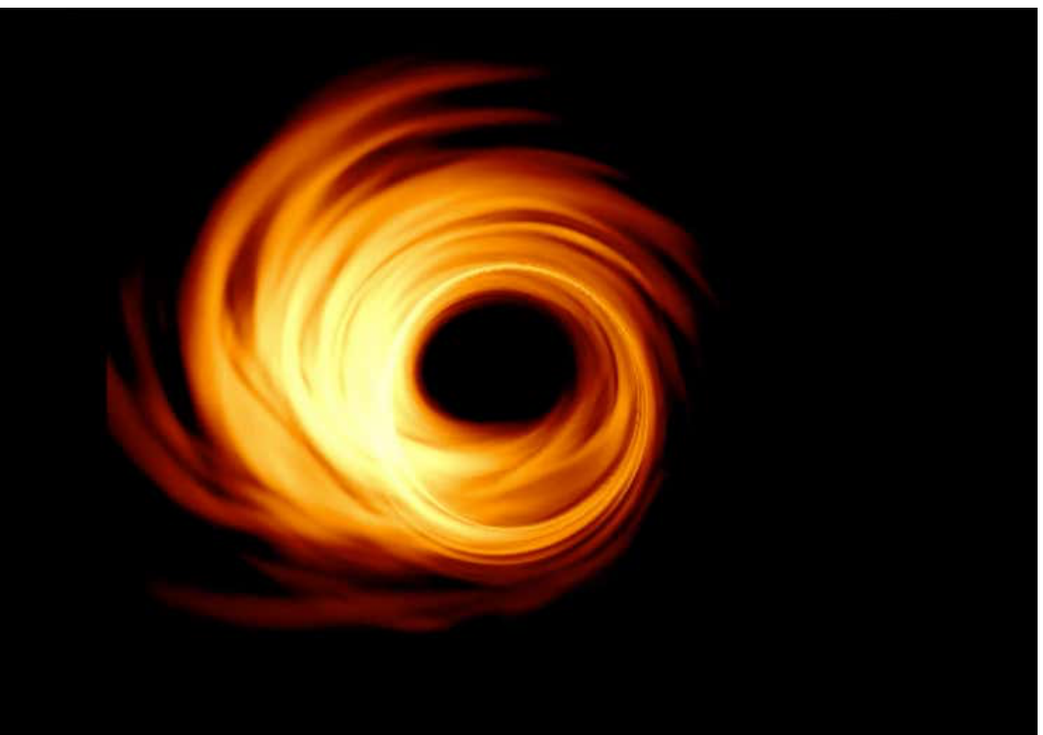
A and B are very weakly entangled. The information of the initial conditions in A stays in A and is detectable by a local measurement.



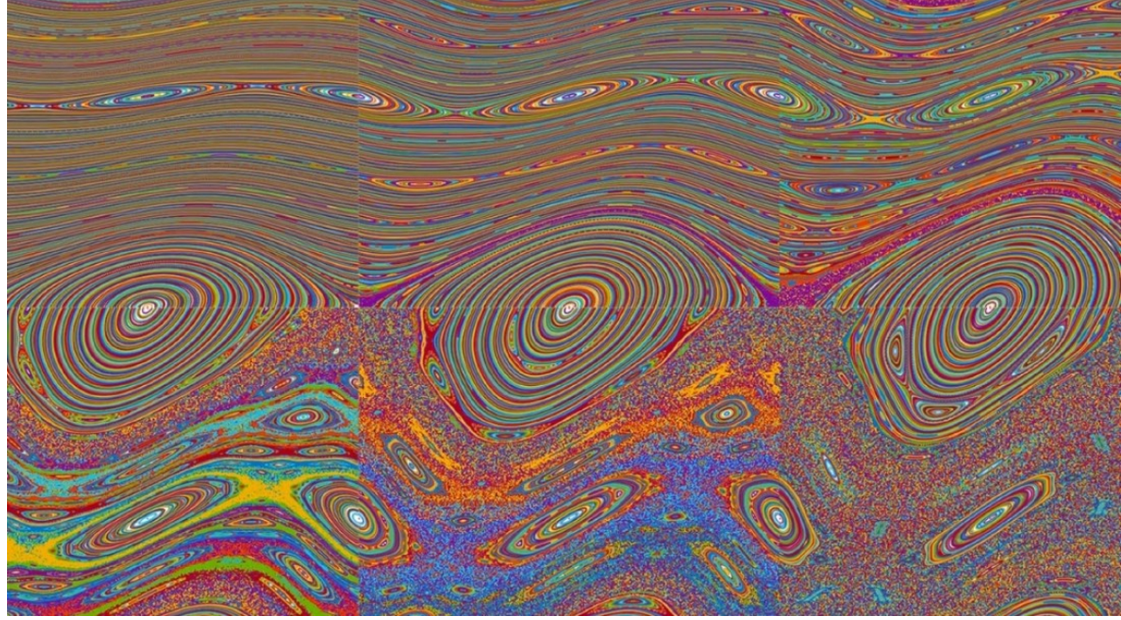




On the other hand, there are classes of closed quantum systems that thermalize extremely fast at the Plank scale (fast scramblers)!



Black-holes are the fastest scramblers we know!



The are quantum materials that seem to behave as fast scramblers (strange metals). Could this unusual phase of matter be the secret behind high temperature superconductivity?