Quantum Computers and Quantum Cryptography

Giuliano Benenti

Center for Nonlinear and Complex Systems

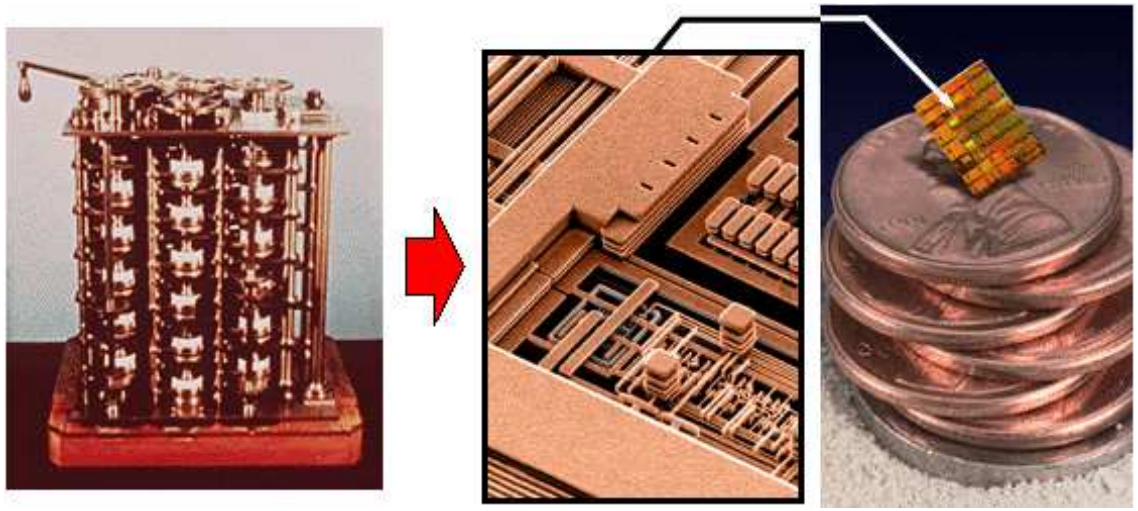
Università degli Studi dell'Insubria

Como, Italy

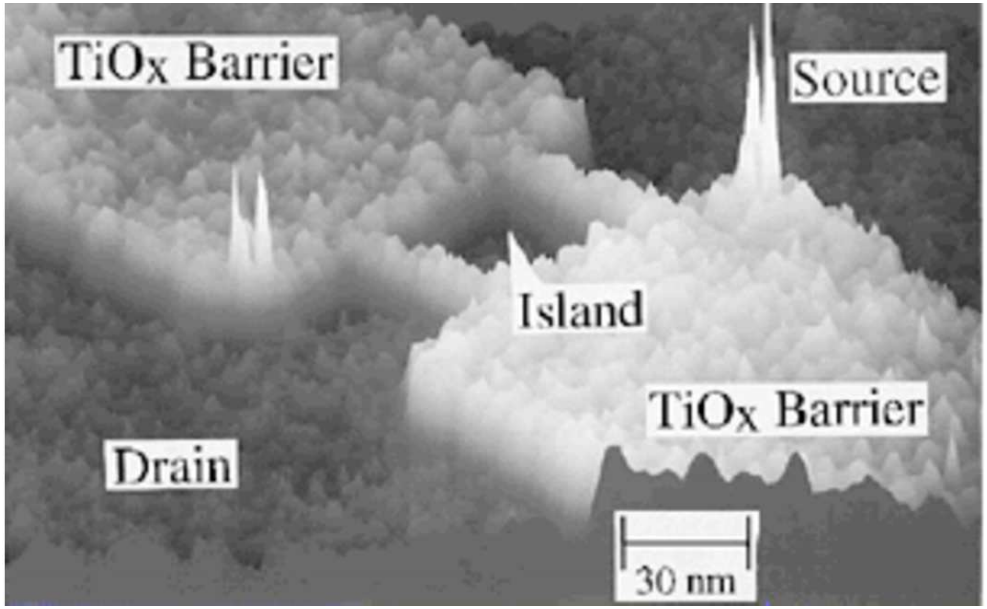
http://scienze-como.uninsubria.it/complexcomo
http://scienze-como.uninsubria.it/benenti

MINIATURIZATION PROBLEM

Smaller and smaller chip size: quantum effects will become dominant (around the year 2020, extrapolating Moore's law)



Development of nanodevices such as quantum dots, single-electron transistors, molecular switches



QUANTUM MACHINES that can process the information taking advantage of the laws of quantum mechanics?

QUANTUM LOGIC

The elementary unit of quantum information it the qubit

QUBIT: two-level system (spin $1/2$ particle), described by a two-dimensional complex Hilbert space
$\{|0\rangle, |1\rangle\}$ orthonormal (computational) basis
These states represent the values 0 and 1 of a classical bit

From the SUPERPOSITION PRINCIPLE, a generic state of the qubit can be written as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (|\alpha|^2 + |\beta|^2 = 1)$$

QUANTUM REGISTER of size n: a collection of n qubits
Wave function residing in a Hilbert space of dimension 2^n

$$|\psi\rangle = \sum_{k=0}^{2^n-1} c_k |k\rangle, \quad (\sum_k |c_k|^2 = 1)$$

$$|k\rangle = |k_{n-1}\rangle \otimes \cdots |k_1\rangle \otimes |k_0\rangle$$
$$k = k_{n-1}2^{n-1} + \cdots k_1 2 + k_0, \quad k_i \in \{0,1\} \text{ binary digits}$$

While n classical bits can store only a single integer k, the n-qubit quantum register can be prepared in a superposition, including up to 2^n states of the computational basis (quantum parallelism)

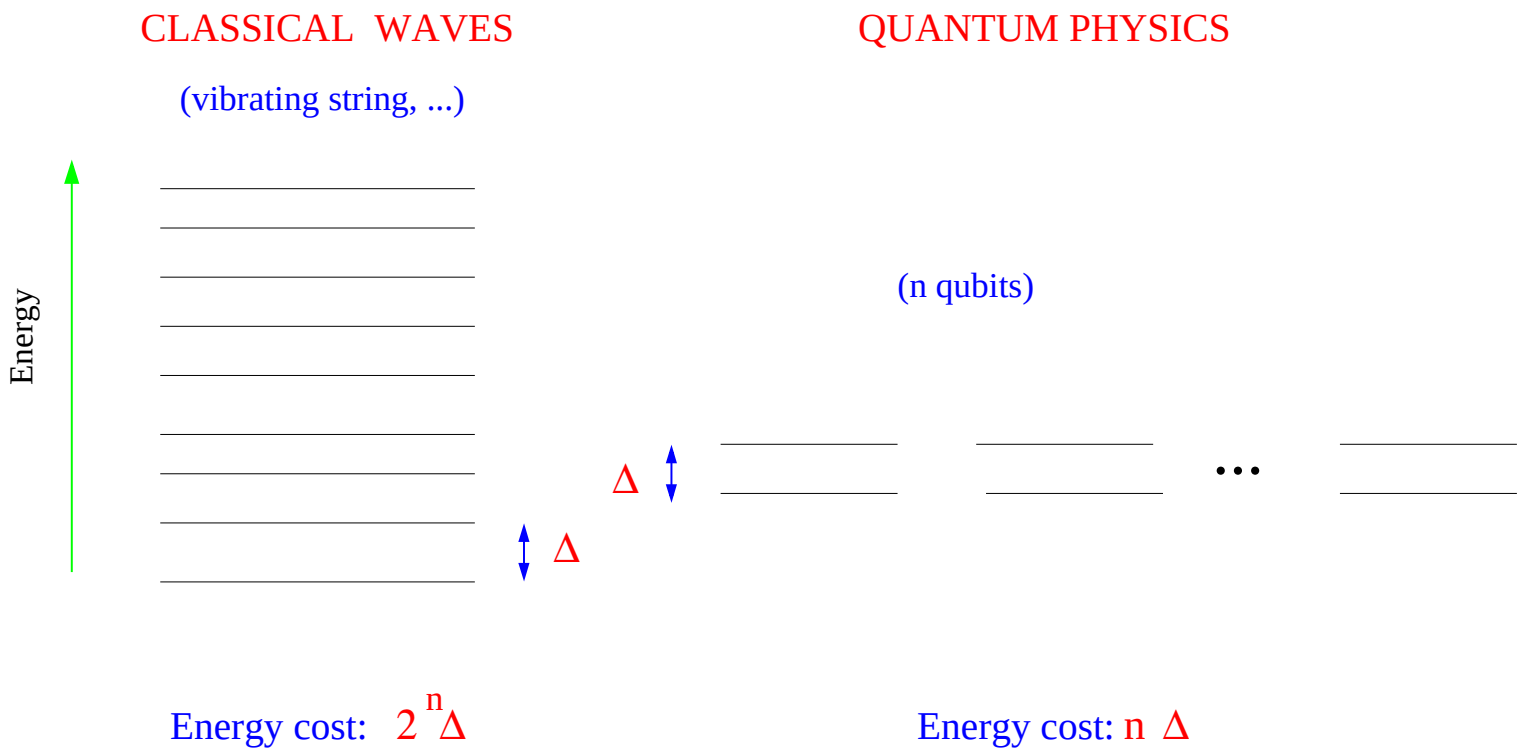
ENTANGLEMENT: after two quantum particles have interacted, they cannot, in general, be described independently of each other

$$\text{Bell state} \quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \neq |\psi_1\rangle \otimes |\psi_2\rangle$$

There exist non-local correlations between measurements performed on well-separated particles (violation of Bell's inequalities)

Entanglement is a resource for quantum computation and communication

To represent the superposition of 2^n states by means of classical waves we need a single system with 2^n levels



• QUANTUM OPERATIONS:

UNITARY transformations in a Hilbert space of size $N = 2^n$

• Universal set of gates:

each unitary transformation in the Hilbert space can be decomposed into:

a) single qubit unitary transformations

b) a two-qubit gate (qubit-qubit interactions required)

e.g. controlled-NOT

$$\begin{cases} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |11\rangle \\ |11\rangle \to |10\rangle \end{cases}$$

$$\sum_{x,y} c_{x,y}|x\rangle|y\rangle \to \sum_{x,y} c_{x,y}|x\rangle|x \oplus y\rangle$$

($|x\rangle$ control qubit, $|y\rangle$ target qubit, $\oplus$ addition modulo 2)

Due to QUANTUM PARALLELISM, we may obtain $f(k)$ for all k in a single run

$$\sum_{k=0}^{2^n-1} c_k|k\rangle|0\rangle \rightarrow \sum_{k=0}^{2^n-1} c_k|k\rangle|f(k)\rangle$$

The MEASUREMENT PROBLEM: this information is "hidden": we obtain the outcome $|\bar{k}\rangle|f(\bar{k})\rangle$ with probability $|c_{\bar{k}}|^2$

QUANTUM ALGORITHMS

• The prime-factorization problem: given a composite odd positive integer N, find its prime factors
Shor's algorithm: exponential gain in time resources

• Searching for a marked item in an unstructured database of N items
Grover's algorithm: quadratic speedup

• Simulation of complex systems (many-body quantum systems, dynamical systems,...)
Exponential gain in memory resources, the exponential/algebraic gain in time resources depends on the computed observable

Shor's algorithm

Prime factorization problem: given an integer N, find its prime factors

Conjecture: on classical computers, there are no polynomial time algorithms for integer factoring
(at the basis of cryptographic systems like RSA)
With the best known classical algorithm, the number of computational steps is:

$$\#_c = \mathsf{O}(\exp(L^{1/3}(\log L)^{2/3}))$$
$$L = \log N \quad \text{input size}$$

Quantum algorithm (Shor, 1994)

$$\#_q = \mathsf{O}(L^2 \log L \log\log L)$$

$N \sim 10^{130}$: $t_c \approx 30$ days on a nowadays computer
$t_q \approx 7$ hours for $\#_q \approx 2 \times 10^{10}$ gates, switching rate 1MHz
($\sim 10^3$ qubits required)
$N \sim 10^{260}$: $t_c \approx 10^6$ years, $t_q \approx 50$ hours

The factorization problem can be reduced to a period finding problem:
find the period r of the function

$$f(x) = m^x (\text{mod. } N), \quad m < N \text{ randomly chosen}$$

$$f(x + r) = f(x)$$

Step 1. Prepare two registers of $n = 2\log N$ qubits in their ground state

$$|x\rangle|y\rangle = |0\rangle|0\rangle = |00...0\rangle|00...0\rangle$$

Step 2. Prepare the $|x\rangle$ register in the uniform superposition of the computational basis states

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|0\rangle$$

Step 3. Perform the unitary transformation
$U_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$, with $f(x) = m^x$ (mod. N)

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle$$

After Step 3 the two registers are entangled

Step 4. Measurement of the y register: collapse of the y register state onto $|u\rangle$

$$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |d_u + jr\rangle |u\rangle$$

$f(d_u + jr) = u \quad (j = 0, 1, ..., M-1)$
r period of $f(x)$, $M = 2^n/r$

Step 5. Apply (efficiently) the discrete Fourier transform to the first register

$$\frac{1}{\sqrt{r}} \sum_k \hat{f}(k) |k\rangle$$

$$|\hat{f}(k)| = \begin{cases} 1 & \text{if } k \text{ multiple of } 2^n/r \\ 0 & \text{otherwise} \end{cases}$$

Step 6. Measure the x register and get r (The algorithm succeeds with probability arbitrarily close to one after $O(\log \log r)$ runs)

Algorithm's key ingredients:
- quantum interference effects,
- exponentially large number of states,
- quantum entanglement

FIRST EXPERIMENTAL IMPLEMENTATIONS

The great challenge of quantum computation is to experimentally realize a quantum computer

Requirements: a collection of (many) two-level quantum systems that can be prepared, manipulated and measured at will

Main obstacle: decoherence, that is, the uncontrolled coupling to the environment, introduces errors in the computation

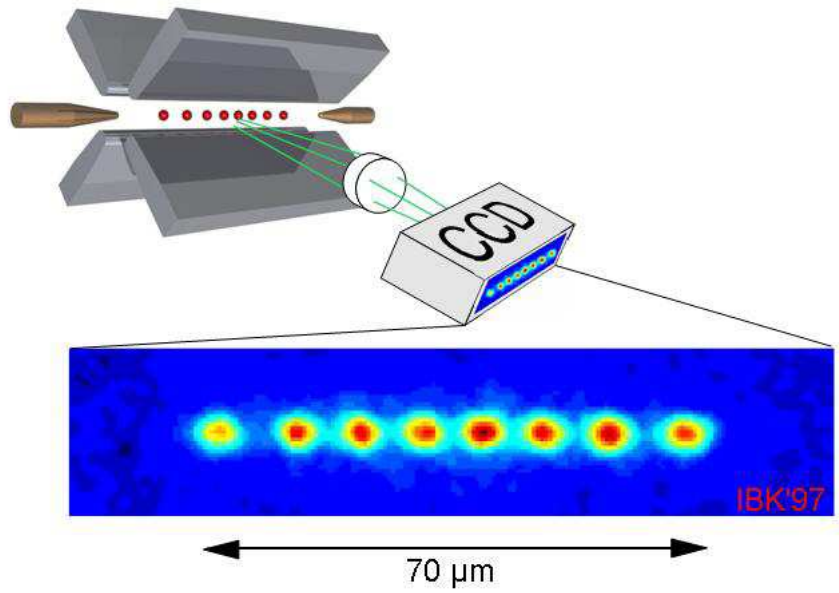
• Liquid state Nuclear Magnetic Resonance quantum processors:
A qubit is the spin of a nucleus in a molecule and quantum gates are implemented by means of resonant oscillating magnetic fields
Demonstrate several quantum algorithms, including Grover's algorithm, the quantum Fourier transform and the Shor's algorithm, using from three- to seven-qubit molecules
Problem: non scalable

• Cavity quantum electrodynamics: A single atom interacts with a single mode or a few modes of the electromagnetic field inside a cavity: the two states of a qubit can be represented by the polarization states of a single photon or by two excited states of an atom
Implemented one- and two-qubit gates

• Linear optics plus repeated measurements
Implemented controlled-NOT

Ion-trap quantum processors

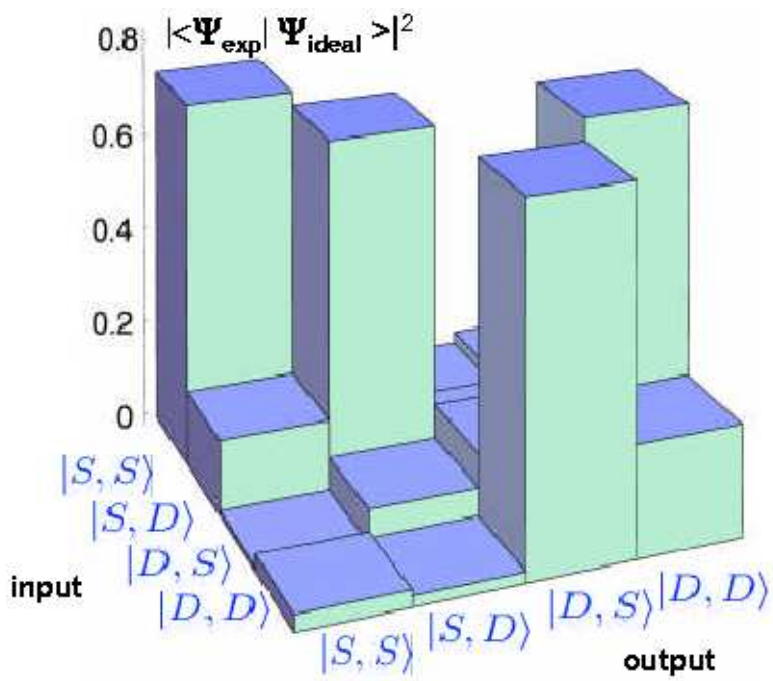
The quantum hardware: a string of ions is confined by a combination of static and oscillating electric fields in a linear trap



Single-qubit gates: addressing individual ions with laser pulses of appropriate frequency, intensity and duration

Two-qubit gates: qubit-qubit interactions mediated by the collective vibrational motion of the trapped string of ions

Implemented the controlled-NOT gate, quantum teleportation and controlled entanglement of four ions

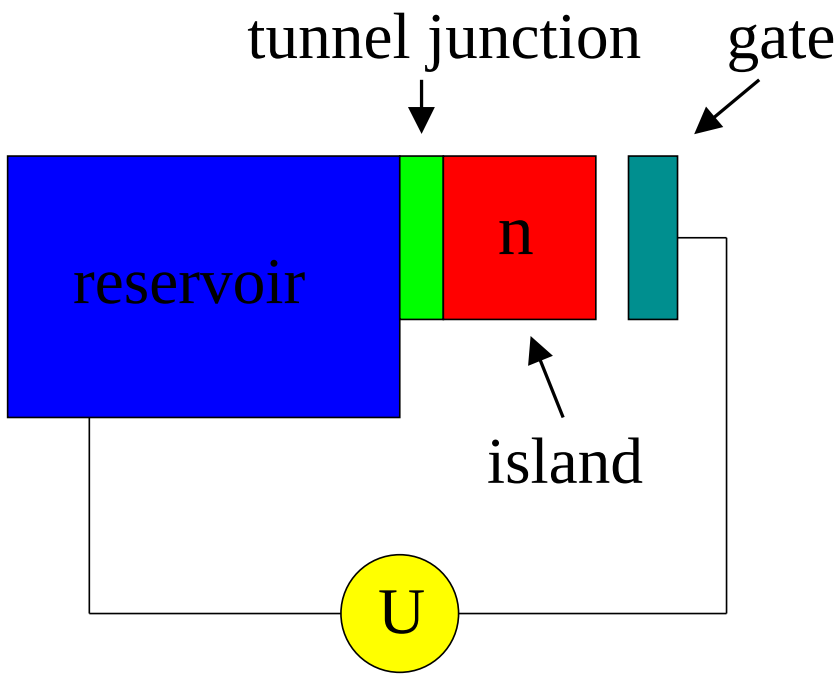


Superconducting circuits

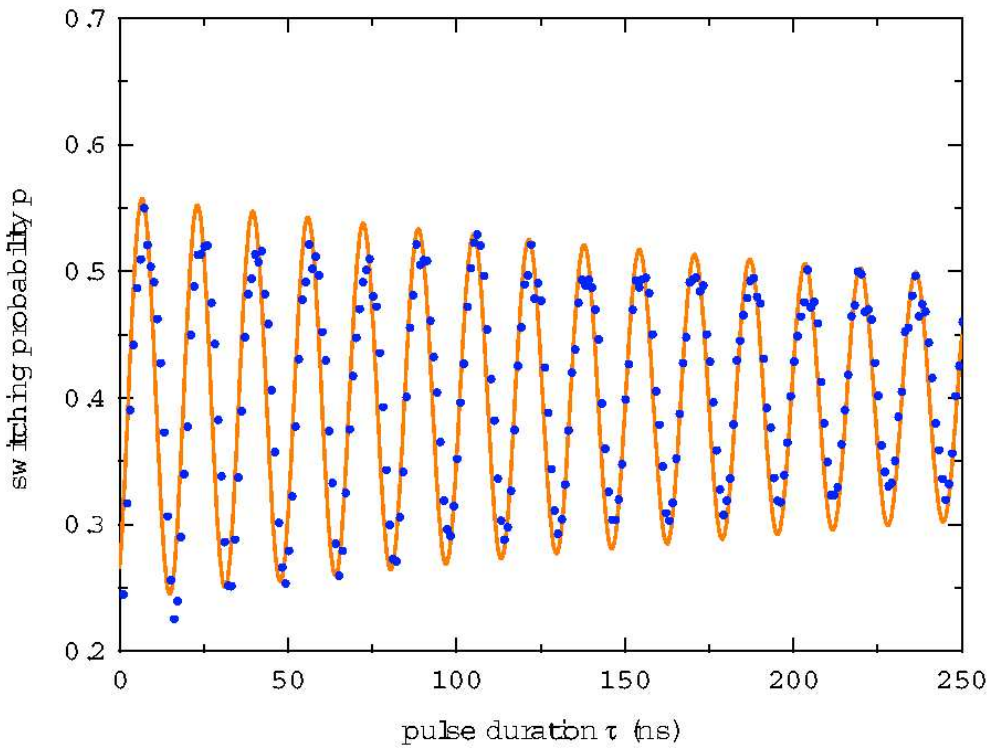
In a Josephson junction a Cooper pair box, known as the island, is connected by a thin insulator (tunnel junction) to a superconducting reservoir

Cooper pairs can move from the island to the reservoir and vice versa by quantum tunneling effect

The two lowest energy states $|0\rangle$ and $|1\rangle$ of the island form a qubit

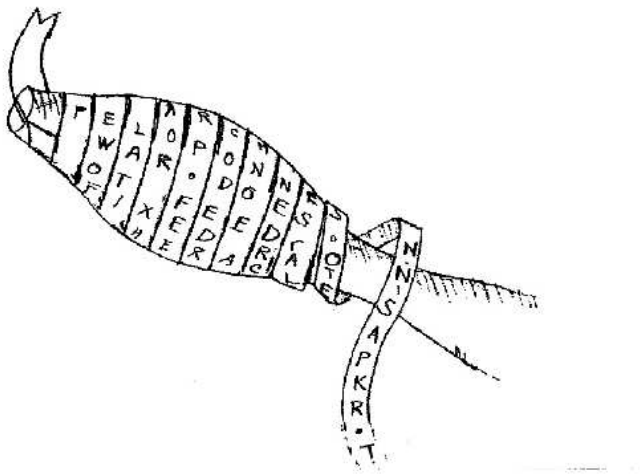


Implemented single-qubit gates and controlled-NOT gate, using a pair of capacitively coupled superconducting qubits



Classical cryptography

The scital



The Vernam cipher

01011000 plain text

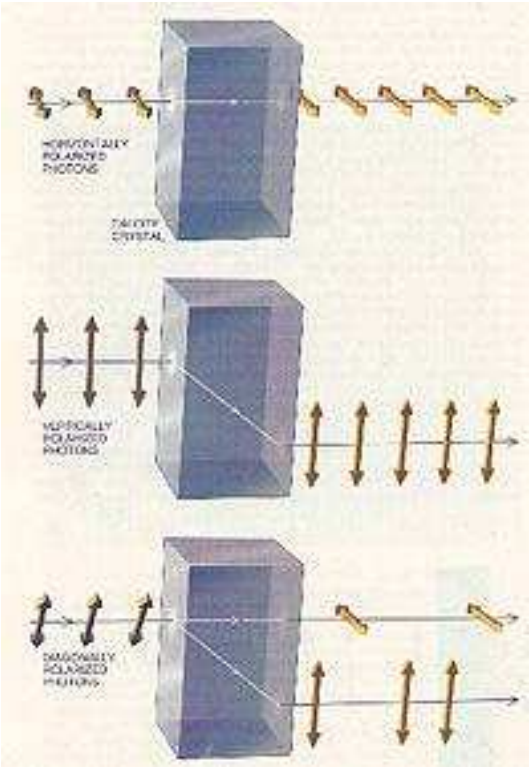
01100101 secret key

00111101 cipher text

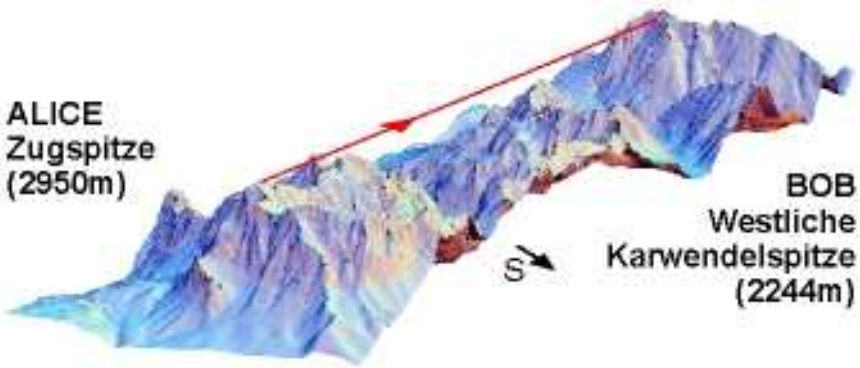
The RSA public key cryptosystem (no secret key is exchanged) would be broken by a large-scale quantum computer

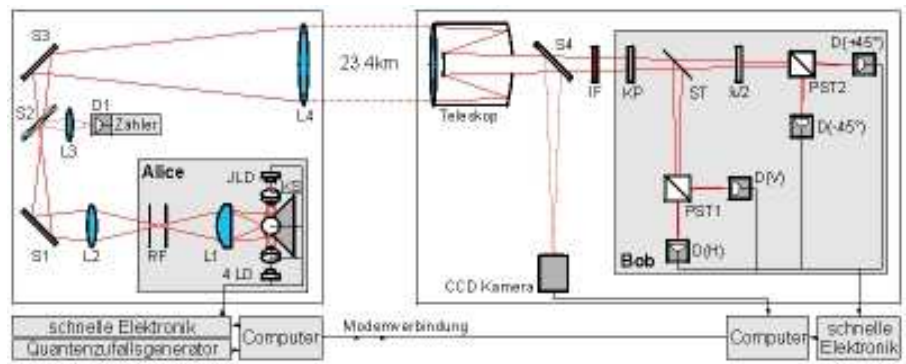
QUANTUM CRYPTOGRAPHY

Quantum key distribution (intrusion detection): in quantum mechanics the measurement process disturbs the system



Experimental implementations





Transmission of qubits (photons) over a few tens of kilometres via optical fibres or through free-space

Satellite-based links foreseen

PROSPECTS

Quantum cryptography: from fundamental science to commercial applications

Quantum computation:
- The difficulties to build a large-scale quantum computer are huge
- What class of problems could be solved efficiently using a quantum computer?

Even the first, demonstrative experiments are remarkable, not only for quantum computation but also for testing the theoretical principles of quantum mechanics

Such experiments stimulate the control of individual quantum systems (atoms, electrons, photons,...)
Applications: single-ion clocks more precise than standard atomic clocks
Foreseen applications: use of entangled states to improve the resolution of optical lithography and interferometric measurements