QUANTUM INFORMATION PROCESSING

Jozef Gruska

Faculty of Informatics, Brno, Czech Republic

June 6, 2003

AIM and CONTENTS

AIM: To show what is QUANTUM INFORMATION PROCESSING about and why it is so fascinating, mysterious and interesting.

CONTENTS:

- Why is QIP so important.
- A glimpse on quantum physics
- Classical versus quantum bits, registers and circuits
- Power of quantum parallelism
- Some simple/powerful quantum algorithms
- Quantm entanglement as a new/mysterious computation and communication resource
- Quantum teleportation
- Quantum key-distribution – current state of art
- When we will have a quantum computer?

WHY is QIPC so IMPORTANT?

There are five main reasons why QIPC is increasingly considered as of (very) large importance:

- QIPC is believed to lead to new Quantum Information Processing Technology that could have deep and broad impacts.
- Several sciences and technology are approaching the point at which they badly need expertise with isolation, manipulating and transmition of particles.
- It is increasingly believed that new, quantum information processing based, understanding of quantum phenomena can be developed.
- Quantum cryptography seems to offer new level of security and be soon feasible.
- QIPC has been shown to be more efficient in interesting/important cases.

BASIC OBSERVATION

In quantum computing we witness a merge of two of the most important areas of science of 20th century: quantum physics and informatics.

This merge is bringing new aims, challenges and potentials for informatics and also new approaches to explore quantum world.

In spite of the fact that it is hard to predict particular impacts of quantum computing on computing in general, it is quite safe to expect that the merge will lead to important outcomes.

PHYSICS versus INFORMATICS

Goal of physics is to study laws and limitations of physical world.

Goal of informatics is to study laws and limitations of information world.

QUANTUM PHYSICS

is

is an **excellent theory** to predict probabilities of quantum events.

Quantum physics is an elegant and conceptually simple theory that describes with astounding precission a large spectrum of phenomena of nature.

The predictions made on the base of quantum physics have been experimentally verified to 14 orders of precission. No conflict betwen predictions of theory and experiments is known.

Without quantum physics we cannot explain properties of superfluids, functioning of laser, the substance of chemistry, the structure and function of DNA, the existence and behaviour of solid bodies, color of stars, ...

WHAT QUANTUM PHYSICS TELL US?

Quantum physics

tells us

WHAT happens

but does not tell us

WHY it happens

nor

HOW it happens

nor

HOW MUCH it costs.

QUANTUM PHYSICS

is, from the point of view of explaining quantum phenomena, a very unsatisfactory theory.

Quantum physics is a theory with either some hard to accept principles or a theory leading to mysteries and paradoxes.

> *Quantum theory sems to lead to philosophical standpoints that many find deeply unsatisfying.*
>
> *At best, and taking its descriptions at their most literal, it provides us with a very strange view of the world indeed.*
>
> *At worst, and taking literally the proclamations of some of its most famous protagonists, it provides us with no view of the world at all.*
>
> Roger Penrose

A POPULAR WISDOM

You have nothing to do but mention the quantum theory, and people will take your voice for the voice of science, and believe anything

Bernard Shaw (1938)

CLASSICAL versus QUANTUM COMPUTING

The essence of the difference
between
classical computers and **quantum computers**

is in the way information is stored and processed.

In **classical computers**, information is represented on **macroscopic level** by **bits**, which can take one of the two values

$$0 \quad \text{or} \quad 1$$

In **quantum computers**, information is represented on **microscopic level** using **qubits**, which can take on any from uncountable many values

$$\alpha|0\rangle + \beta|1\rangle$$

where α, β are arbitrary complex numbers such that

$$|\alpha|^2 + |\beta|^2 = 1.$$

PRE-HISTORY

1970 Landauer demonstrated importance of reversibility for minimal energy computation;

1973 Bennett showed the existence of universal reversible Turing machines;

1981 Toffoli-Fredkin designed a universal reversible gate for Boolean logic;

1982 Benioff showed that quantum processes are at least as powerful as Turing machines;

1982 Feynman showed that qunatum physics cannot be simulated effectively on classical computers;

1985 Deutsch showed the existence of a universal quantum Turing machine.

1993 Bernstein-Vazirani-Yao showed the existence of an efficient universal quantum Turing machine;

1994 Shor discovered a polynomial time quantum algorithm for factorization;

1994 Quantum cryptography went through an experimental stage;

1995 DiVincenzo designed a universal gate with two inputs and outputs;

1995 Cirac and Zoller demonstrated a chance to build quantum computers using existing technologies.

WHY von NEUMANN

DID (COULD) NOT DISCOVER QUANTUM COMPUTING?

DEVELOPMENT of BASIC VIEWS

on the role of information in physics:

- Information is information, nor matter, nor energy.

  Norbert Wiener

- Information is physical

  Ralf Landauer

  Should therefore information theory and foundations of computing (complexity theory and computability theory) be a part of physics?

- Physics is informational

  Should (Hilbert space) quantum mechanics be a part of Informatics?

WHEELER's VIEW

I think of my lifetime in physics as divided into three periods

- In the first period ...I was convinced that

  EVERYTHING IS PARTICLE

- I call my second period

  EVERYTHING IS FIELDS

- Now I have new vision, namely that

  EVERYTHING IS INFORMATION

CLASSICAL EXPERIMENTS

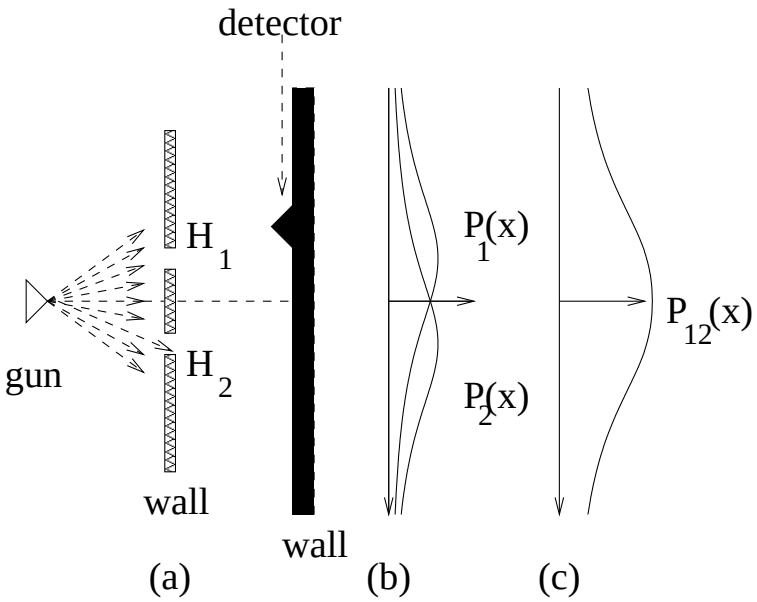


Figure 1: Experiment with bullets

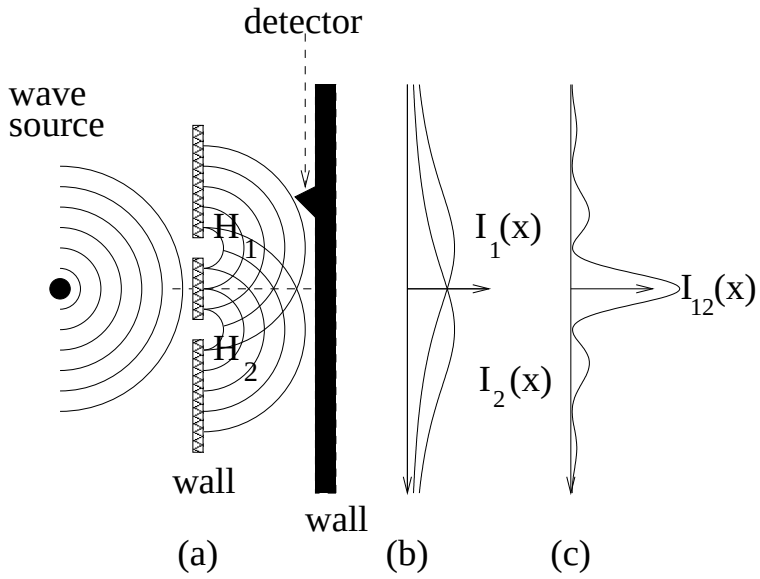


Figure 2: Experiments with waves

QUANTUM EXPERIMENTS

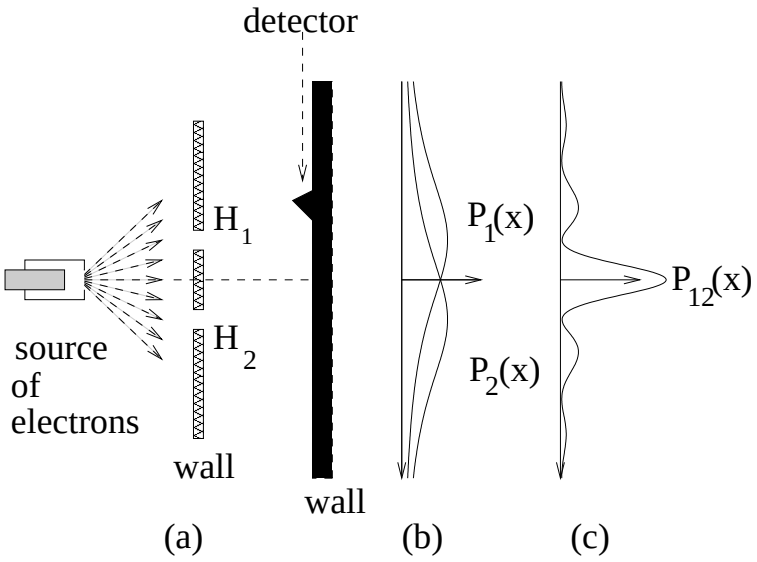


Figure 3: Two-slit experiment

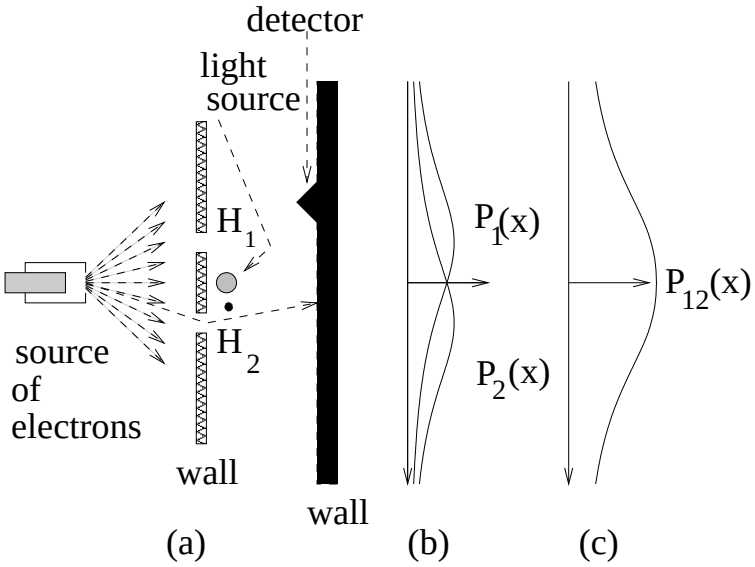


Figure 4: Two-slit experiment with an observation

TWO-SLIT EXPERIMENT – OBSERVATIONS

- Contrary to our intuition, at some places one observes fewer electrons when both slits are open, than in the case only one slit is open.
- Electrons — particles, seem to behave as waves.
- Each electron seems to behave as going through both holes at once.
- Results of the experiment do not depend on frequency with which electrons are shot.
- Quantum physics has no explanation where a particular electron reaches the detector wall. All quantum physics can offer are statements on the probability that an electron reaches a certain position on the detector wall.

THREE BASIC PRINCIPLES

P1 To each transfer from a quantum state ϕ to a state ψ a complex number

$$\langle\psi|\phi\rangle$$

is associated, which is called the **probability amplitude** of the transfer, such that

$$|\langle\psi|\phi\rangle|^2$$

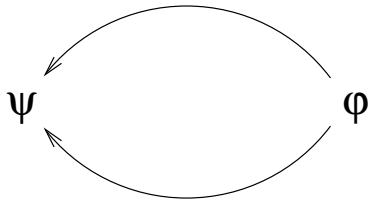
is the **probability** of the transfer.

P2 If a transfer from a quantum state ϕ to a quantum state ψ can be decomposed into two subsequent transfers

$$\psi \leftarrow \phi' \leftarrow \phi$$

then the resulting amplitude of the transfer is the **product** of amplitudes of subtransfers: $\langle\psi|\phi\rangle = \langle\psi|\phi'\rangle\langle\phi'|\phi\rangle$

P3 If the transfer from a state ϕ to a state ψ has two independent alternatives



then the resulting amplitude is the sum of amplitudes of two subtransfers.

QUANTUM SYSTEMS

=

HILBERT SPACE

Hilbert space H_n is n-dimensional complex vector space with

scalar product

$$\langle\psi|\phi\rangle = \sum_{i=1}^{n} \phi_i \psi_i^* \text{ of vectors } |\phi\rangle = \begin{vmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_n \end{vmatrix}, |\psi\rangle = \begin{vmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{vmatrix},$$

norm of vectors

$$||\phi|| = \sqrt{|\langle\phi|\phi\rangle|}$$

and the **metric**

$$\text{dist}(\phi, \psi) = ||\phi - \psi||.$$

BRA-KET NOTATION

Dirack introduced a very handy notation, so called bra-ket notation, to deal with amplitudes, quantum states and linear functionals $f : H \to \mathbf{C}$.

If $\psi, \phi \in H$, then

$\langle\psi|\phi\rangle$ — scalar product of ψ and ϕ
(an amplitude of going from ϕ to ψ).

$|\phi\rangle$ — **ket-vector** — an equivalent to ϕ

$\langle\psi|$ — **bra-vector** a linear functional on H
such that $\langle\psi|(|\phi\rangle) = \langle\psi|\phi\rangle$

QUBITS

A **qubit** is a quantum state in H_2

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where $\alpha, \beta \in \mathbf{C}$ are such that $|\alpha|^2 + |\beta|^2 = 1$ and $\{|0\rangle, |1\rangle\}$ is a (**standard**) **basis** of H_2

EXAMPLE: Representation of qubits by

(a) electron in a Hydrogen atom

(b) a spin-$\frac{1}{2}$ particle

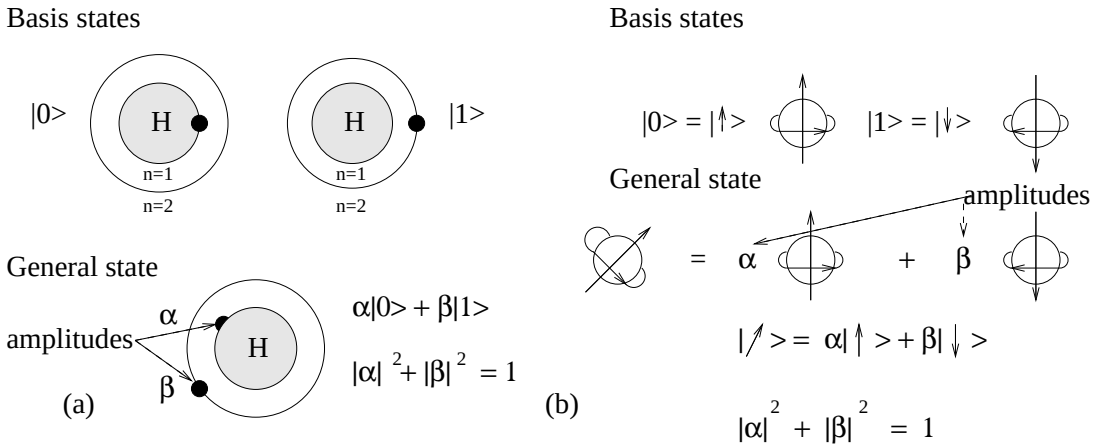


Figure 5: Qubit representations by energy levels of an electron in a hydrogen atom and by a spin-$\frac{1}{2}$ particle. The condition $|\alpha|^2 + |\beta|^2 = 1$ is a legal one if $|\alpha|^2$ and $|\beta|^2$ are to be the probabilities of being in one of two basis states (of electrons or photons).

X

QUANTUM EVOLUTION/COMPUTATION

EVOLUTION in QUANTUM SYSTEM

COMPUTATION in HILBERT SPACE

is described by

Schrödinger linear equation

$$i\hbar\frac{\partial\psi(t)}{\partial t} = H(t)\psi(t),$$

where $H(t)$ is a quantum analogue of a Hamiltonian of the classical system, from which it follows that evolution (computation) of a quantum system is performed by a **unitary operator** and a step of such an evolution we can see as a multiplication of a **unitary matrix** A with a vector $|\psi\rangle$, i.e.

$$A|\psi\rangle$$

A matrix A is **unitary** if

$$A \cdot A^* = A^* \cdot A = I$$

UNITARY MATRICES — EXAMPLES

In the following figure there are examples of unitary matrices of degree 2

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

(a) (b) (c)

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \qquad \frac{1}{2}\begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix}$$

(d) (e)

$$\begin{pmatrix} i\cos\theta & \sin\theta \\ \sin\theta & i\cos\theta \end{pmatrix} \quad \begin{pmatrix} e^{i\alpha}\cos\theta & -ie^{i(\alpha-\theta)}\sin\theta \\ -ie^{i(\alpha+\theta)}\sin\theta & e^{i\alpha}\cos\theta \end{pmatrix}$$

(f) (g)

Figure 6: Examples of unitary matrices of degree 2

Matrices σ_x, σ_y and σ_z are so called **Pauli matrices**. They play an important role in quantum computing and have the following interesting important property.

- Unitary matrix I of degree 2 and Pauli matrices form a basis of all matrices of degree 2. That is each matrix of degree two can be expressed as a linear combination of these matrices.

HILBERT SPACE H_2

STANDARD BASIS

$$|0\rangle, |1\rangle$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

DUAL BASIS

$$|0'\rangle, |1'\rangle$$

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Hadamard matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H|0\rangle = |0'\rangle \qquad H|0'\rangle = |0\rangle$$

$$H|1\rangle = |1'\rangle \qquad H|1'\rangle = |1\rangle$$

General form of a unitary matrix of degree 2

$$U = e^{i\gamma} \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{pmatrix} \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} e^{i\beta} & 0 \\ 0 & e^{-i\beta} \end{pmatrix}$$

QUANTUM REGISTERS

A general state of a 2-qubit register is:

$$|\phi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

where

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

and $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ are vectors of the "standard" basis of H_4, i.e.

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

CNOT GATE

An important unitary matrix of degree 4, to transform states of 2-qubit registers:

$$CNOT = XOR = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

It holds:

$$XOR : |x, y\rangle \Longrightarrow |x, x \oplus y\rangle$$

NO-CLONING THEOREM

INFORMAL VERSION: Unknown quantum state cannot be cloned.

FORMAL VERSION: There is no unitary transformation U such that for any qubit state $|\psi\rangle$

$$U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$$

PROOF: Assume U exists and for two different states $|\alpha\rangle$ and $|\beta\rangle$

$$U(|\alpha\rangle|0\rangle) = |\alpha\rangle|\alpha\rangle \quad U(|\beta\rangle|0\rangle) = |\beta\rangle|\beta\rangle$$

Let

$$|\gamma\rangle = \frac{1}{\sqrt{2}}(|\alpha\rangle + |\beta\rangle)$$

Then

$$U(|\gamma\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle) \neq |\gamma\rangle|\gamma\rangle = \frac{1}{2}(|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle + |\alpha\rangle|\beta\rangle + |\beta\rangle|\alpha\rangle)$$

However, XOR can make copies of basis states $|0\rangle, |1\rangle$:

$$XOR(|x\rangle|0\rangle) = |x\rangle|x\rangle$$

BELL STATES

States

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle, \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle, \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

form an orthogonal (Bell) basis in H_4 and play an important role in quantum computing.

Theoretically, there is an observable for this basis. However, no one has been able to construct a measuring device for Bell measurement using linear elements only.

QUANTUM n-qubit REGISTER

General state of an n-qubit register has the form:

$$|\phi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle = \sum_{i\in\{0,1\}^n} \alpha_i |i\rangle, \quad \text{where} \quad \sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$$

and $|\phi\rangle$ is a vector in H_{2^n}.

Operators on n-qubits registers are unitary matrices of degree 2^n.

Is it difficult to create a superposition of an exponential large number of basis states?

In general yes, in some important special cases not. For example, if n-qubit **Hadamard transformation**

$$H_n = \bigotimes_{i=1}^{n} H.$$

is used then

$$H_n|0^{(n)}\rangle = \bigotimes_{i=1}^{n} H|0\rangle = \bigotimes_{i=1}^{n} |0'\rangle = |0'^{(n)}\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle.$$

MEASUREMENT of n-QUBIT STATES

If the n-qubit state

$$|\phi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle.$$

is measured in the standard basis, then

on quantum level the state $|\phi\rangle$ collapses

into the state $|x_0\rangle$

with probability $|\alpha_i|^2$

and in the classical level information x_0 is obtained to show which collapse took place.

QUANTUM PARALLELISM

If

$$f : \{0, 1, \ldots, 2^n - 1\} \Longrightarrow \{0, 1, \ldots, 2^n - 1\}$$

then the mapping

$$f' : (x, 0) \Longrightarrow (x, f(x))$$

is one-to-one and therefore there is a unitary transformation U_f such that.

$$U_f(|x\rangle|0\rangle) \Longrightarrow |x\rangle|f(x)\rangle$$

Let

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

With a **single application** of the mapping U_f we get

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

IN A SINGLE COMPUTATIONAL STEP 2^n VALUES OF f ARE COMPUTED! We have therefore a really MASSIVE PARALLELISM

IN WHAT LIES POWER OF QUANTUM COMPUTING?

In quantum interference or in quantum parallelism?

NO,

in QUANTUM ENTANGLEMENT.

Let

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

be a (global) state of two very distant particles, then measurement of one of the particles immediately determines state of the other particle – a non-locality effect occurs.

Definition A pure state $|\phi\rangle$ of a bipartite Hilbert spaces $H_1 \otimes \ldots \otimes H_n$ is called **entangled** if it cannot be decomposed in the form

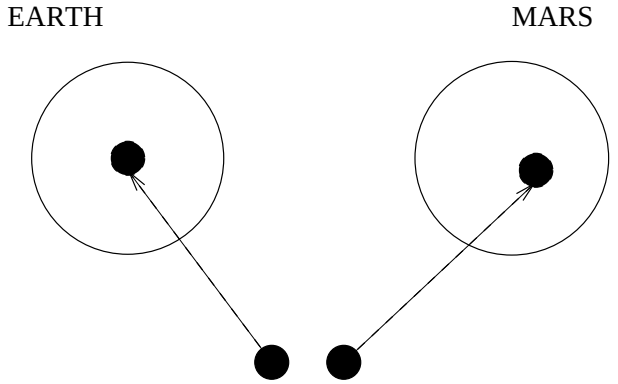
$$|\phi\rangle = |\phi_1\rangle \otimes \ldots \otimes |\phi_n\rangle$$

where $|\phi_i\rangle$ is a pure state of H_i.

ENTANGLEMENT and NON-LOCALITY

Quantum theory implies, and (not fully perfect) experiments confirm, that a set of particles can be in an entangled state even if they are much space separated.

As a consequence, a measurement on one of the entangled particles may uniquely determine the result of measurement on much space separated particles. For example if two particles are in the EPR-state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ as on the following picture:



Einstein called this phenomenon "spooky action at a distance" because measurement in one place seems to have an instantaneous effect at the other (very distant) place.

WHY is QUANTUM ENTANGLEMENT so IMPORTANT?

- Entanglement is seen as having a potential to provide a new gold mine for science and technology.
- Entanglement is main resource giving edge to quantum versus classical information processing.
- Entanglement is seen as a way to better understanding of various important physics phenomena.

POWER of ENTANGLEMENT

Power of entanglement as a resource has been demonstrated for:

- performing tasks that are impossible to peform without quantum entanglement;
- speeding-up (quantum) algorithms;
- making communication more efficient;
- making communication more secure;
- making quantum games strategies more efficient;
- enlarging capacities of (quantum) channels

GROVER's SEARCH PROBLEM

Grover's method seems to apply to problems for which it is hard to find a solution, but it is easy to check a to-be-solution.

> **Problem:** In an unsorted database of N items there is one, x_0, satisfying an easy to verify condition P. Find x_0.

Classical algorithms need in average $\frac{N}{2}$ checks.
Quantum algorithm exists that needs $\mathcal{O}(\sqrt{N})$ steps.

Modified problem: Given an easy to compute black-box function

$$f : \{0,1\}^n \to \{0,1\}$$

find an x_0 such that $f(x_0) = 1$ (let there is single such x_0).

Basic idea of the algorithm

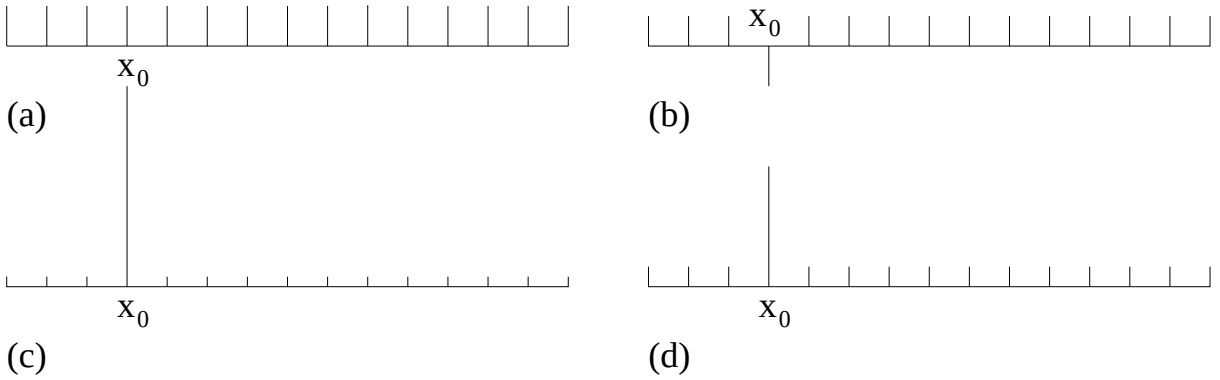


Figure 7: "Cooking" the solution with Grover's algorithm

We shall deal also with a more general problem. Namely that there is more than one solution, especially the case that the number

$$t = |\{x \mid f(x) = 1\}|$$

is known.

GROVER's SEARCH ALGORITHM

Start in the state

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

and iterate $\lfloor \frac{\pi}{4}\sqrt{2^n} \rfloor$ times the transformation

$$-\underbrace{H_n V_0^n H_n V_f}|\phi\rangle \rightarrow |\phi\rangle.$$

Grover's iterate

Finally, measure the register to get x_0 and check whether $f(x_0) = 1$. If not, repeat the procedure.

It has been shown that the above algorithm is optimal for finding the solution with probability $> \frac{1}{2}$.

In the case that there are t solutions, repeat the above iteration

$$\left\lfloor \frac{\pi}{4}\sqrt{\frac{2^n}{t}} \right\rfloor \quad \text{times}$$

ANALYSIS of GROVER's ALGORITHM

Denote

$$X_1 = \{x \mid f(x) = 1\} \quad X_0 = \{x \mid f(x) = 0\}$$

and denote the state after jth iteration of Grover's iterate $-H_n V_0^n H_N V_f$ as

$$|\phi_j\rangle = k_j \sum_{x \in X_1} |x\rangle + l_j \sum_{x \in X_0} |x\rangle$$

with

$$k_0 = \frac{1}{\sqrt{2^n}} = l_0.$$

Since

$$|\phi_{j+1}\rangle = -H_n V_0^n H_n V_f |\phi_j\rangle,$$

it holds

$$k_{j+1} = \frac{2^n - 2t}{2^n} k_j + \frac{2(2^n - t)}{2^n} l_j$$

$$l_{j+1} = \frac{2^n - 2t}{2^n} l_j - \frac{2t}{2^n} k_j$$

what yields

$$k_j = \frac{1}{\sqrt{t}} \sin((2j+1)\theta)$$

$$l_j = \frac{1}{\sqrt{2^n - t}} \cos((2j+1)\theta)$$

where

$$\sin^2\theta = \frac{t}{2^n}.$$

Recurrence relations therefore provide

$$k_j = \frac{1}{\sqrt{t}}\sin((2j+1)\theta)$$

$$l_j = \frac{1}{\sqrt{2^n - t}}\cos((2j+1)\theta)$$

where

$$\sin^2\theta = \frac{t}{2^n}.$$

The aim now is to find such an j which maximizes k_j and minimizes l_j.

Take j such that $\cos((2j+1)\theta) = 0$, that is $(2j+1)\theta = (2m+1)\frac{\pi}{2}$.

Hence

$$j = \frac{\pi}{4\theta} - \frac{1}{2} + \frac{m\pi}{2\theta}$$

what yields

$$j_0 = \lceil \frac{\pi}{4\theta} \rceil,$$

and because

$$\sin^2\theta = \frac{t}{2^n}$$

we have

$$0 \leq \sin\theta \leq \sqrt{\frac{t}{2^n}}$$

and therefore

$$j_0 = \mathcal{O}\left(\sqrt{\frac{2^n}{t}}\right).$$

POWERFUL QUANTUM ALGORITHMS

- Shor has shown the existence of polynomial time quantum algorithms to factorize integers and to compute discrete algorithms.
- Several other polynomial time algorithms have been developed that can brake modern cryptosystems (for example elliptic curves cryptosystems).
- It has been show that polynomial time algorithms exist for so called hidden subgroup problem for all Abelian groups and some non-Abelian groups.
- Using the ideas behind Grover's algorithms in a variety of cases it has been shown that using quantum means a square root time improvement can be obtained.

Deutsch-Jozsa problem

Problem Given a **black-box** function

$$f : \{0, 1, \ldots, 2_1^n\} \rightarrow \{0, 1\}$$

and a **promise** that f is either **constant** or **balanced**. Detrmine which if this properties f has.

Classsical solution; requires in the worst casee $2^{n-1} + 1$ queries.

Quantum solution can be obtained using a single query (with a superposition of inputs)

Improvement is from $2^{n-1} + 1$ to 1.

CLASSICAL versus QUANTUM TELEPORTATION I

The so called **No-teleportation theorem** says that **(classical) teleportation is impossible**.

This means that there is **no way** to use

classical channels

to transmit faithfully

quantum information.

CLASSICAL versus QUANTUM TELEPORTATION II

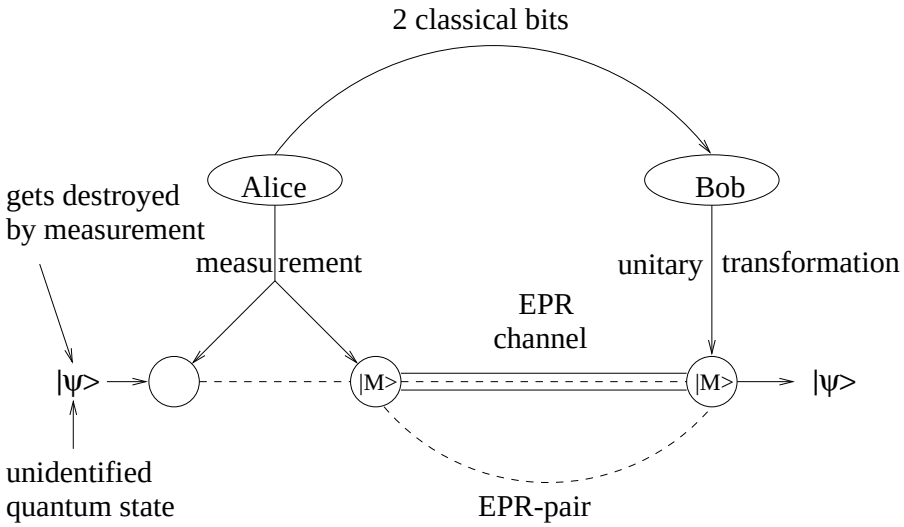
In contrast to the classical no-teleportation theorem, quantum teleportation is possible.

Indeed, let us assume that two parties, Alice and Bob, share two particles P_A and P_B in the EPR state and Alice gets a new particle P_u, in an unknown state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$.

State $|\phi\rangle$ can be teleported to Bob by the following actions:

- Alice performs Bell measurement on particles P_u and P_A to receive two classical bits.
- Alice sends the two bits to Bob.
- Depending on two bits received, Bob performs one of four Pauli operators on his particle to get Bob's particle P_B to the state $|\phi\rangle$.

QUANTUM TELEPORTATION - DETAILS



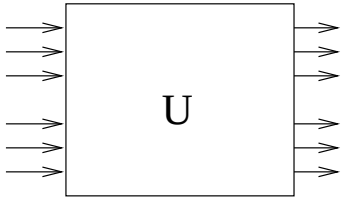
In case the (unknown) state to be teleported is $\alpha|0\rangle + \beta|1\rangle$ and Alice and Bo b share the EPR state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$, then total state can be written in the form

$$|\psi\rangle|\text{EPR}\rangle = |\Phi^+\rangle\frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle) + |\Psi^+\rangle\frac{1}{\sqrt{2}}(\beta|0\rangle + \alpha|1\rangle)$$
$$+|\Phi^-\rangle\frac{1}{\sqrt{2}}(\alpha|0\rangle - \beta|1\rangle) + |\Psi^-\rangle\frac{1}{\sqrt{2}}(-\beta|0\rangle + \alpha|1\rangle))$$

and therefore the measurement of the first two particles projects the state of the Bob's particle into a "small modification " $|\psi_1\rangle$ of the unknown state $|\psi\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)$

QUANTUM GATES — CIRCUITS

Unitarity is the main new requirement quantum gates have to satisfy.



Definition 0.1 *A* **quantum gate** *with n inputs and n outputs is specified by a unitary operator $U : \mathcal{H}_{2^n} \to \mathcal{H}_{2^n}$, and it is represented by a unitary matrix A_U of degree 2^n.*

Definition A quantum circuit is a circuit consisting of quantum gates

POWER of QUANTUM ENTANGLEMENT for CRYPTOGRAPHY

There are several ways how quantum entanglement has an impact on quantum cryptography.

Positive way:

- Unconditionally secure quantum key-generation is possible.
- Unconditionally secure encryption is possible.

Negative way:

Due to the existence of entanglement, unconditional secure quantum bit commitment is believed to be impossible, in non-relativistic quantum setting.

TWO SHANNON THEOREMS

- **Classical Shannon Theorem** says that n bits are necessary and sufficient to hide perfectly n bits.

  Consequently: ONE-TIME-PAD CRYPTOSYSTEM is perfectly secure if parties always share new n random secret bits.

- **Quantum Shannon Theorem** says that $2n$ bits are necessary and sufficient to hide perfectly n qubits.

  Consequently: QUANTUM ONE-TIME-PAD CRYPTOSYSTEM is perfectly secure if parties always share either new

  – $2n$ secret bits or

  – $2n$ maximally entangled (Bell) states.

PERFECT HIDING of QUBITS

Let b_1, b_2 be two shared secret bits and $|\phi\rangle$ a qubit to be hidden.

- Encoding

$$E_{b_1 b_2}|\phi\rangle = \sigma_x^{b_1}\sigma_z^{b_2}|\phi\rangle = |\psi\rangle$$

- Decoding

$$D_{b_1 b_2}|\psi\rangle = \sigma_z^{b_2}\sigma_x^{b_1}|\psi\rangle = |\phi\rangle$$

QUANTUM KEY GENERATION

Security of many cryptographic systems is such how secure is their secret key distribution.

Security (unconditional) of quantum key generation protocols is based on the fact that, on the basis of physical laws, undectable eavesdropping is not possible.

This security is based on quantum laws, on Heisenberg's uncertainty principle, and the fact that quantum information cannot be copied and cannot be measured without causing detectable disturbances.

Experimentally, secure quantum key distribution has been tested, using polarization or phase of photons, for distance of 64 km using standard optical fibres and for the distance of 23 km in open air. Earth-to-satelite quantum bit transmissions are considered as feasible. Quantum cryptography is therefore in the advanced experimental and development stage.

FUNDAMENTAL DIFFERENCES

between classical and quantum cryptography

- Security of (public key) classical cryptography is based on unproven assumptions of computational complexity (and it can be jeopardized by progress in algorithms and/or technology).

  Security of quantum cryptography is based on laws of quantum physics that allow to build systems where undetectable eavesdropping is impossible.

- Since classical cryptography is vulnerable to technological improvements it has to be designed in such a way that a secret is secure with respect to **future technology**, during the whole period in which the secrecy is required.

  Quantum key generation, on the other hand, needs to be designed only to be secure against technology available at the moment of key generation.

BB84 QUANTUM KEY GENERATION PROTOCOL

Quantum key generation protocol BB84 (due to Bennett and Brassard), for generation of a key of length n, has several phases:

Preparation phase

Alice generates two private random binary sequences of bits of length $m \gg n$ bits and Bob generates one such private random sequence.

Quantum transmission

Alice is assumed to have four transmitters of photons in one of the following four polarizations $0, 45, 90$ and 135 degrees

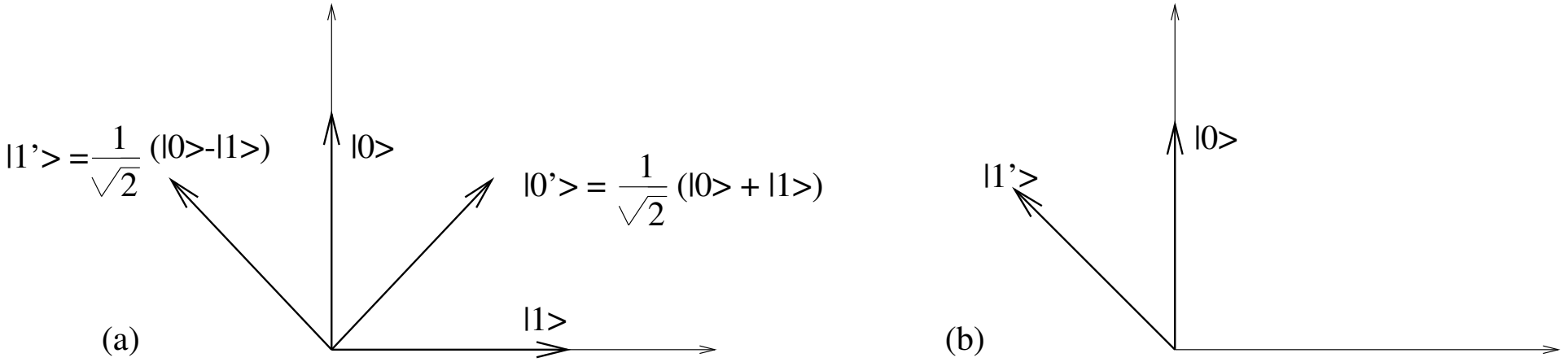


Figure 8: Polarizations of photons for BB84 and B92 protocols

Expressed in a more general form, Alice uses for encoding states from the set $\{|0\rangle, |1\rangle, |0'\rangle, |1'\rangle\}$.)

Bob has a detector that can be set up to distinguish between rectilinear polarizations (0 and 90 degrees) or can be quickly reset to distinguish between diagonal polarizations (45 and 135 degrees).

However, in accordance with the laws of quantum physics, there is no detector that could distinguish between unorthogonal polarizations.

(In a more formal setting, Bob can use either the standard observable $\mathcal{B} = \{|0\rangle, |1\rangle\}$ or the dual observable $\mathcal{D} = \{|0'\rangle, |1'\rangle\}$, to measure the incoming photon.

Transmissions

To send a bit 0 (1) of her first random sequence through a quantum channel Alice chooses, on the basis of her second random sequence, one of the encodings $|0\rangle$ or $|0'\rangle$ ($|1\rangle$ or $|1'\rangle$), i.e., in the standard or dual basis,

Bob chooses, each time on the base of his private random sequence, one of the observables $\mathcal{B}$ or $\mathcal{D}$ to measure the photon he is to receive and he records the results of his measurements and keeps them secret.

Alice's encodings	Bob's observables	Alice's state relative to Bob	the result and its probability	correctness
$0 \rightarrow \|0\rangle$	$0 \rightarrow \mathcal{B}$	$\|0\rangle$	0 (prob. 1)	correct
	$1 \rightarrow \mathcal{D}$	$\frac{1}{\sqrt{2}}(\|0'\rangle + \|1'\rangle)$	$0/1$ (prob. $\frac{1}{2}$)	random
$0 \rightarrow \|0'\rangle$	$0 \rightarrow \mathcal{B}$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$0/1$ (prob. $\frac{1}{2}$)	random
	$1 \rightarrow D$	$\|0'\rangle$	0 (prob. 1)	correct
$1 \rightarrow \|1\rangle$	$0 \rightarrow \mathcal{B}$	$\|1\rangle$	1 (prob. 1)	correct
	$1 \rightarrow \mathcal{D}$	$\frac{1}{\sqrt{2}}(\|0'\rangle - \|1'\rangle)$	$0/1$ (prob. $\frac{1}{2}$)	random
$1 \rightarrow \|1'\rangle$	$0 \rightarrow \mathcal{B}$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$0/1$ (prob. $\frac{1}{2}$)	random
	$1 \rightarrow D$	$\|1'\rangle$	1 (prob. 1)	correct

Figure 9: Quantum cryptography with BB84 protocol

Figure 9 shows the possible results of the measurements and their probabilities.

An example of an encoding–decoding

process is in the Figure 11.

1	0	0	0	1	1	0	0	0	1	1	Alice's random sequence
$\|1\rangle$	$\|0'\rangle$	$\|0\rangle$	$\|0'\rangle$	$\|1\rangle$	$\|1'\rangle$	$\|0'\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1'\rangle$	Alice's polarizations
0	1	1	1	0	0	1	0	0	1	0	Bob's random sequence
$\mathcal{B}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{B}$	Bob's observable
1	0	R	0	1	R	0	0	0	R	R	outcomes

Figure 10: Quantum transmissions in the BB84 protocol—R stands for the case that the result of the measurement is random

Raw key extraction

Bob makes public the sequence of observables he used to measure the photons he received—but not the results of the measurements —and Alice tells Bob, through a classical channel, in which cases he has chosen the same basis for observable as she did for encoding. The corresponding bits then form the basic **raw key** both parties agree on.

1	0	0	0	1	1	0	0	0	1	1	Alice's random sequence
$\|1\rangle$	$\|0'\rangle$	$\|0\rangle$	$\|0'\rangle$	$\|1\rangle$	$\|1'\rangle$	$\|0'\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1'\rangle$	Alice's polarizations
0	1	1	1	0	0	1	0	0	1	0	Bob's random sequence
$\mathcal{B}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{B}$	Bob's observable
1	0	R	0	1	R	0	0	0	R	R	outcomes

Figure 11: Quantum transmissions in the BB84 protocol—R stands for the case that the result of the measurement is random

Test for evesdropping

Alice and Bob agree on a sequence of indices of the raw key and make the corresponding bits of their raw keys public.

Case 1. Noiseless channel. If the subsequences chosen by Alice and Bob are not completely identical eavesdropping is detected. Otherwise, the remaining bits are taken as creating the final key.

Case 2. Noisy channel. If the subsequences chosen by Alice and Bob contains more errors than the admitable error (that has to be determined from channel characteristics), then eavesdropping is assumed. Otherwise, the remaining bits are taken as the next result of the raw key generation process.

Error correction phase

In the case of a noisy channel for transmission it may happen that Alice and Bob have different keys after the key generation phase.

A way out is that before sending choosen sequence of bits Alice encodes them using some classical error correcting code.

During error correcting phase Alice sends Bob information about encoding and so Bob can use corresponding decoding procedures.

At the end of this stage both Alice and Bob share identical keys.

Privacy amplification phase

One problem remains. Eve can still have quite a bit of information about the key both Alice and Bob share. Privacy amplification is a tool to deal with such a case.

Privacy amplification is a method how to select a short and **very secret** binary string s from a longer but **less secret** string s'.
The main idea is simple. If $|s| = n$, then one picks up n random subsets $S_1, \ldots, S_n$ of bits of s' and let s_i, the ith bit of S, be the parity of S_i. One way to do it is to take a random binary matrix of size $|s| \times |s'|$ and to perform multiplication Ms'^T, where s'^T is the binary column vector corresponding to s'.

The point is that even in the case where an eavesdropper knows quite a few bits of s', she will have almost no information about s.

More exactly, if Eve knows parity bits of k subsets of s', then if a random subset of bits of s' is chosen, then the probability that Eve has any information about its parity bit is less than $2^{-(n-k-1)}/\ln 2$.

CONCLUSIONS

OVERCOMMING PESSIMISM

- Till 1995 there was strong pessimis due to destructive impacts of environment called decoherence whether powerful QIP is possible.
- It was believed that quantum error-correcting codes are impossible.
- In 1995-96 P. Shor has shown the existence of quantum error-correcting codes and quantum fault-tolerant computations.
- A threshold has been derived for errors of quantum gates such that if nthis threshold is reached arbitrarily long in time and space quantum computations/transmission are possible.

QIPC SCEPTICS

It will need more than rain to stop this parade

Ralf Landauer

OPTIMISTS versus PESSIMISTS

- Progress in science is often done by pessimists.
- Progress in technology is always done by optimists.

QUANTUM COMPUTING TECHNOLOGIES

With respect to the underlying technologies that has been explored in order to perform some rudimentary quantum opertaions we can talk about the following types of quantum computing:

- NMR quantum computing
- Solid state and ionic quantum computing
- Neutral-atom quantum computing
- Quantum computing with superconductors
- Photonic quantum computing
- Cavite-QEF quantum computing
- Molecular quantum computing

ROAD MAP

Research community recently established the following research goal for next ten years concerning experimental research.

To develope by 2012 a suite of viable emerging quantum computing technologies of sufficient complexity to function as computer science test-beds in which architectural and algorithmic issues can be explored.

MOORE LAW

It is nowadays accepted that information processing technology has been developing for the last 30 years according to so-called Moore law. This law can be seen as having the following forms.

Economic form: Computer power doubles, for constant cost, every two years or so.

Physical form: The number of atoms needed to represent one bit of information should halves every two years or so.

Quantum form: for certain applications, quantum computers need to increase in the size only by one qubit every two years or so, in order to keep pace with the classical computers performance increase.

UNSCRAMBELING of OMELETTE

Todays we are beginning to realize how much of all physical science is really only *information, organized in a particular way*.

But we are far from unraveling the knotty question: *To what extent does this information reside in us, and to what extent is it a property of nature?*

Our present quantum mechanics formalism is a peculiar mixture describing in part laws of Nature, in part incomplete human information about Nature – all scrambled up together by Bohr into an omelette that nobody has seen how to unscramble,

Yet we think the unscrambeling is a prerequisite for any further advances in basic physical theory...

Edwin T. Jaynes, 1990

CLOSING MOTTO

If we knew what we are doing,
it wouldn't be called research, would it?

Albert Einstein

TRY TO BELIEVE IMPOSSIBLE

There's no use in trying, she said: one can't believe impossible things

I daresay you haven't had much practice said the Queen.

When I was your age, I always did it for half-an-hour a day.

Why sometimes I've believed as many as six impossible things before breakfast.

Lewis Carol: *Through the Looking-glass, 1872*