An important new feature of quantum cryptography is that security of quantum cryptographic protocols is based on the laws of nature – of quantum physics, and not on the unproven assumptions of computational complexity.

Quantum cryptography is the first area of information processing and communication in which quantum particle physics laws are directly exploited to bring an essential advantage in information processing.

MAIN OUTCOMES – so far

- It has been shown that would we have quantum computer, we could design absolutely secure quantum generation of shared and secret random classical keys.
- It has been proven that even without quantum computers unconditionally secure quantum generation of classical secret and shared keys is possible (in the sense that any eavesdropping is detectable).
- Unconditionally secure basic quantum cryptographic primitives, such as bit commitment and oblivious transfer, are impossible.
- Quantum zero-knowledge proofs exist for all NP-complete languages.
- Quantum teleportation and pseudo-telepathy are possible.
- Quantum cryptography and quantum networks are already in advanced experimental stage.

BASICS of QUANTUM INFORMATION PROCESSING

As an introduction to quantum cryptography

the very basic motivations, experiments, principles, concepts and results of quantum information processing and communication will be presented in the next few slides.
In quantum information processing we witness an interaction between the two most important areas of science and technology of 20-th century, between quantum physics and informatics.

This is very likely to have important consequences for 21th century.

Quantum physics deals with fundamental entities of physics – particles (waves?) like protons, electrons and neutrons (from which matter is built); photons (which carry electromagnetic radiation); various “elementary particles” which mediate other interactions in physics.

For example, a quantum particle "can go through two places at the same time" and can interact with itself.

Quantum physics is full of counter-intuitive, weird, mysterious and even paradoxical events.

I am going to tell you what Nature behaves like . . .

However, do not keep saying to yourself, if you can possibly avoid it,

BUT HOW CAN IT BE LIKE THAT?

Because you will get "down the drain" into a blind alley from which nobody has yet escaped

NOBODY KNOWS HOW IT CAN BE LIKE THAT

Richard Feynman (1965): The character of physical law.

Main properties of classical information:
- It is easy to store, transmit and process classical information in time and space.
- It is easy to make (unlimited number of) copies of classical information.
- One can measure classical information without disturbing it.

Main properties of quantum information:
- It is difficult to store, transmit and process quantum information.
- There is no way to copy unknown quantum information.
- Measurement of quantum information destroys it, in general.
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 or 1.

In quantum computers, information is represented on microscopic level using qubits, (quantum bits) which can take on any from the following uncountable many values

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

where $\alpha, \beta$ are arbitrary complex numbers such that

$$|\alpha|^2 + |\beta|^2 = 1.$$
CLASSICAL EXPERIMENT with waves

prof. Jozef Gruska

IV054 13. Quantum cryptography

13/65

QUANTUM EXPERIMENTS

Figure 3: Two-slit experiment

Figure 4: Two-slit experiment with an observation

prof. Jozef Gruska

IV054 13. Quantum cryptography

14/65

TWO-SLIT EXPERIMENT

prof. Jozef Gruska

IV054 13. Quantum cryptography

15/65

TWO-SLIT EXPERIMENT with OBSERVATION

prof. Jozef Gruska

IV054 13. Quantum cryptography

16/65
THREE BASIC PRINCIPLES

P1 To each transfer from a quantum state \( \phi \) to a state \( \psi \) a complex number

\[ \langle \psi | \phi \rangle \]

is associated. This number is called the **probability amplitude** of the transfer and

\[ |\langle \psi | \phi \rangle|^2 \]

is then the **probability** of the transfer.

P2 If a transfer from a quantum state \( \phi \) to a quantum state \( \psi \) 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 a transfer from a state \( \phi \) to a state \( \psi \) has two independent alternatives

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

### BRA-KET NOTATION

Dirac introduced a very handy notation, so called bra-ket notation, to deal with amplitudes, quantum states and linear functionals \( f : H \rightarrow C \).

If \( \psi, \phi \in H \), then

\[ \langle \psi | \phi \rangle \quad \text{is the scalar product of } \psi \text{ and } \phi \text{ (an amplitude of going from } \phi \text{ to } \psi) \]

\[ |\phi\rangle \quad \text{is the ket-vector (a column vector) - an equivalent to } \phi \]

\[ \langle \psi | \rangle \quad \text{is the bra-vector (a row vector) a linear functional on } H \]

such that \( \langle \psi | (\phi) \rangle = \langle \psi | \phi \rangle \)

### QUANTUM SYSTEMS = HILBERT SPACE

Hilbert space \( H_n \) is an n-dimensional complex vector space with

**scalar product**

\[ \langle \psi | \phi \rangle = \sum_{i=1}^{n} \phi_i \bar{\psi}_i \quad \text{of vectors } |\phi\rangle = \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_n \end{pmatrix}, \quad |\psi\rangle = \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_n \end{pmatrix} \]

This allows to define the **norm of vectors** as

\[ \| \phi \| = \sqrt{|\langle \phi | \phi \rangle|}. \]

Two vectors \( |\phi\rangle \) and \( |\psi\rangle \) are called **orthogonal** if \( \langle \phi | \psi \rangle = 0 \).

A basis \( B \) of \( H_n \) is any set of \( n \) vectors \( |b_1\rangle, |b_2\rangle, \ldots, |b_n\rangle \) of the norm 1 which are mutually orthogonal.

Given a basis \( B = \{ |b_i\rangle \}_{i=1}^{n} \), any vector \( |\psi\rangle \) from \( H_n \) can be uniquely expressed in the form:

\[ |\psi\rangle = \sum_{i=1}^{n} \alpha_i |b_i\rangle. \]

### EXAMPLES

**Example** For states \( \phi = (\phi_1, \ldots, \phi_n) \) and \( \psi = (\psi_1, \ldots, \psi_n) \) we have

\[ |\phi\rangle = \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_n \end{pmatrix}, \quad \langle \phi | = \begin{pmatrix} \phi_1^* & \ldots & \phi_n^* \end{pmatrix}; \quad \langle \phi | \psi \rangle = \sum_{i=1}^{n} \phi_i^* \psi_i; \]

\[ |\phi\rangle \langle \psi | = \begin{pmatrix} \phi_1 \psi_1^* & \ldots & \phi_1 \psi_n^* \\ \vdots & \ddots & \vdots \\ \phi_n \psi_1^* & \ldots & \phi_n \psi_n^* \end{pmatrix} \]
A quantum state is always observed (measured) with respect to an observable \( O \) – a decomposition of a given Hilbert space into orthogonal subspaces (where each vector can be uniquely represented as a sum of vectors of these subspaces).

There are two outcomes of a projection measurement of a state \( |\phi\rangle \) with respect to \( O \):  
- Classical information into which subspace projection of \( |\phi\rangle \) was made.  
- Resulting quantum projection (as a new state) \( |\phi'\rangle \) in one of the above subspaces.

The subspace into which projection is made is chosen randomly and the corresponding probability is uniquely determined by the amplitudes at the representation of \( |\phi\rangle \) as a sum of states of the subspaces.

\[
|\phi\rangle = \sum_{i=1}^{n} a_i |\beta_i\rangle, \quad \sum_{i=1}^{n} |a_i|^2 = 1
\]

where \( a_i = \langle \beta_i | \phi \rangle \) are called probability amplitudes and their squares provide probabilities.

That if the state \( |\phi\rangle \) is measured with respect to the basis \( \{ |\beta_i\rangle \}_{i=1}^{n} \), then the state \( |\phi\rangle \) collapses into the state \( |\beta_i\rangle \) with probability \( |a_i|^2 \).

The classical "outcome" of the measurement of the state \( |\phi\rangle \) with respect to the basis \( \{ |\beta_i\rangle \}_{i=1}^{n} \) is the index \( i \) of that state \( |\beta_i\rangle \) into which the state \( |\phi\rangle \) collapses.
A qubit is a quantum state in $H_2$

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

where $\alpha, \beta \in \mathbb{C}$ 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-1/2 particle

**QUANTUM MEASUREMENT of QUBITS**

A qubit state can “contain” unboundly large amount of classical information. However, an unknown quantum state cannot be identified.

By a measurement of the qubit state

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

with respect to the basis

$\{ |0\rangle, |1\rangle \}$

we can obtain only classical information and only in the following random way:

- 0 with probability $|\alpha|^2$
- 1 with probability $|\beta|^2$

**MIXED STATES – DENSITY MATRICES**

A probability distribution $\{(p_i, |\phi_i\rangle)\}_{i=1}^k$ on pure states is called a mixed state to which it is assigned a density operator

$$\rho = \sum_{i=1}^n p_i |\phi_i\rangle \langle \phi_i|.$$
MAXIMALLY MIXED STATES

To the maximally mixed state,
\[ \left( \frac{1}{2}, |0\rangle \right), \left( \frac{1}{2}, |1\rangle \right) \]
representing a random bit, corresponds the density matrix
\[
\frac{1}{2} \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) = \frac{1}{2} \mathbf{I}
\]

Surprisingly, many other mixed states have density matrix that is the same as that of the maximally mixed state.

QUANTUM ONE-TIME PAD CRYPTOSYSTEM

CLASSICAL ONE-TIME PAD cryptosystem
plaintext \( p \) an n-bit string
shared key \( k \) an n-bit string
cryptotext \( c \) an n-bit string
coding \( c = p \oplus k \)
decoding \( p = c \oplus k \)

QUANTUM ONE-TIME PAD cryptosystem
plaintext: an n-qubit string \( |p\rangle \)
shared key: two n-bit strings \( k, k' \)
cryptotext: an n-qubit string \( |c\rangle \)
encoding: \( |c_i\rangle = \sigma_{x}^{k_i} \sigma_{y}^{k'_i} |p_i\rangle \)
decoding: \( |p_i\rangle = \sigma_{y}^{k'_i} \sigma_{x}^{k_i} |c_i\rangle \)

where \( |p_i\rangle = \left( \frac{a_i}{b_i} \right) \) and \( |c_i\rangle = \left( \frac{d_i}{e_i} \right) \) are qubits and \( \sigma_x = \left( \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right) \) with \( \sigma_y = \left( \begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right) \) are Pauli matrices.

UNCONDITIONAL SECURITY of QUANTUM ONE-TIME PAD

In the case of encryption of a qubit \( |\phi\rangle = \alpha |0\rangle + \beta |1\rangle \) by QUANTUM ONE-TIME PAD cryptosystem, what is being transmitted is the mixed state
\[
\left( \frac{1}{2}, |\phi\rangle \right), \left( \frac{1}{4}, \sigma_x |\phi\rangle \right), \left( \frac{1}{4}, \sigma_x \sigma_z |\phi\rangle \right), \left( \frac{1}{4}, \sigma_z |\phi\rangle \right)
\]
whose density matrix is
\[
\frac{1}{2} \mathbf{I}
\]

This density matrix is identical to the density matrix corresponding to that of a random bit, that is to the maximally mixed state
\[ \left( \frac{1}{2}, |0\rangle \right), \left( \frac{1}{2}, |1\rangle \right) \]

SHANNON’s THEOREMS

Shannon classical encryption theorem says that \( n \) bits are necessary and sufficient to encrypt securely \( n \) bits.

Quantum version of Shannon encryption theorem says that \( 2n \) classical bits are necessary and sufficient to encrypt securely \( n \) qubits.
**COMPOSED QUANTUM SYSTEMS (1)**

Tensor product of vectors

\[(x_1, \ldots, x_n) \otimes (y_1, \ldots, y_m) = (x_1 y_1, \ldots, x_1 y_m, \ldots, x_n y_1, \ldots, x_n y_m)\]

Tensor product of matrices \(A \otimes B = \begin{pmatrix} a_{11} B & \ldots & a_{1n} B \\ \vdots & \ddots & \vdots \\ a_{n1} B & \ldots & a_{nn} B \end{pmatrix}\)

where \(A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}\)

Example

\[
\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 \\ 0 & 0 & a_{11} & a_{12} \\ 0 & 0 & a_{21} & a_{22} \end{pmatrix}
\]

**COMPOSED QUANTUM SYSTEMS (II)**

Tensor product of Hilbert spaces \(H_1 \otimes H_2\) is the complex vector space spanned by tensor products of vectors from \(H_1\) and \(H_2\). That corresponds to the quantum system composed of the quantum systems corresponding to Hilbert spaces \(H_1\) and \(H_2\).

An important difference between classical and quantum systems

A state of a compound classical (quantum) system can be (cannot be) always composed from the states of the subsystem.

**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 \(H_2\), i.e.

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

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

\[\text{CNOT} = \text{XOR} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\]

It holds:

\[\text{CNOT} : |x, y\rangle \Rightarrow |x, x \oplus y\rangle\]

**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

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

However, CNOT can make copies of the basis states \(|0\rangle, |1\rangle\): Indeed, for \(x \in \{0, 1\}, \)

\[\text{CNOT}(|x\rangle|0\rangle) = |x\rangle|x\rangle\]
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 (so called 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 device for Bell measurement using linear elements only.

QUANTUM n-qubit REGISTERS

A 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 state of an n-qubit register?

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

\[ H_n = \otimes_{i=1}^n H. \]

is used then

\[ H_n |0^@\rangle = \otimes_{i=1}^n H |0\rangle = \otimes_{i=1}^n |0\rangle = |0^@\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \]

and, in general, for \( x \in \{0,1\}^n \)

\[ H_n |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle. \]

\[ 1 \] The dot product is defined as follows: \( x \cdot y = \otimes_{i=1}^n x_i y_i \).

QUANTUM PARALLELISM

If

\[ f : \{0,1,…,2^n − 1\} \rightarrow \{0,1,…,2^n − 1\} \]

then the mapping

\[ f' : (x,0) \rightarrow (x,f(x)) \]

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

\[ U_f(|x\rangle|0\rangle) \rightarrow |x\rangle|f(x)\rangle \]

Let us now have the state

\[ |\Psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|0\rangle \]

With a single application of the mapping \( U_f \) we then get

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

OBSERVE THAT IN A SINGLE COMPUTATIONAL STEP \( 2^n \) VALUES OF \( f \) ARE COMPUTED!

IN WHAT LIES POWER OF QUANTUM COMPUTING?

In quantum superposition or in quantum parallelism?

\[ \text{NOT,} \]

in QUANTUM ENTANGLEMENT!

Let

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

be a state of two very distant particles, for example on two planets

Measurement of one of the particles, with respect to the standard basis, makes the above state to collapse to one of the states

\[ |00\rangle \text{ or } |11\rangle. \]

This means that subsequent measurement of other particle (on another planet) provides the same result as the measurement of the first particle. This indicate that in quantum world non-local influences, correlations, exist.
POWER of ENTANGLEMENT

Quantum state $|\Psi\rangle$ of a composed bipartite quantum system $A \otimes B$ is called entangled if it cannot be decomposed into tensor product of the states from $A$ and $B$.

Quantum entanglement is an important quantum resource that allows

- To create phenomena that are impossible in the classical world (for example teleportation)
- To create quantum algorithms that are asymptotically more efficient than any classical algorithm known for the same problem.
- To create communication protocols that are asymptotically more efficient than classical communication protocols for the same task
- To create, for two parties, shared secret binary keys
- To increase capacity of quantum channels

CLASSICAL versus QUANTUM CRYPTOGRAPHY

Security of classical cryptography is based on unproven assumptions of computational complexity (and it can be jeopardize 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.

QUANTUM KEY GENERATION

Quantum protocols for using quantum systems to achieve unconditionally secure generation of secret (classical) keys by two parties are one of the main theoretical achievements of quantum information processing and communication research.

Moreover, experimental systems for implementing such protocols are one of the main achievements of experimental quantum information processing research.

It is believed and hoped that it will be quantum key generation (QKG)

another term is quantum key distribution (QKD)

where one can expect the first transfer from the experimental to the application stage.

QUANTUM KEY GENERATION – EPR METHOD

Let Alice and Bob share $n$ pairs of particles in the entangled EPR-state.

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

$n$ pairs of particles in EPR state

If both of them measure their particles in the standard basis, then they get, as the classical outcome of their measurements the same random, shared and secret binary key of length $n$. 
Polarized photons are currently mainly used for experimental quantum key generation.

Photon, or light quantum, is a particle composing light and other forms of electromagnetic radiation.

Photons are electromagnetic waves and their electric and magnetic fields are perpendicular to the direction of propagation and also to each other.

An important property of photons is polarization – it refers to the bias of the electric field in the electromagnetic field of the photon.

If the electric field vector is always parallel to a fixed line we have linear polarization (see Figure).

There is no way to determine exactly polarization of a single photon. However, for any angle \( \theta \) there are \( \theta \)-polarizers – “filters” – that produce \( \theta \)-polarized photons from an incoming stream of photons and they let \( \theta_1 \)-polarized photons to get through with probability \( \cos^2(\theta - \theta_1) \).

For any two orthogonal polarizations there are generators that produce photons of two given orthogonal polarizations. For example, a calcite crystal, properly oriented, can do the job.

**Figure 6:** Electric and magnetic fields of a linearly polarized photon

Generation of orthogonally polarized photons.

Photons whose electronic fields oscillate in a plane at either 0° or 90° to some reference line are called usually rectilinearly polarized and those whose electric field oscillates in a plane at 45° or 135° as diagonally polarized. Polarizers that produce only vertically or horizontally polarized photons are depicted in Figure 6 a, b.
**Quantum Key Generation – Prologue**

Very basic setting: Alice tries to send a quantum system to Bob and an eavesdropper tries to learn, or to change, as much as possible, without being detected.

Eavesdroppers have this time especially hard time, because quantum states cannot be copied and cannot be measured without causing, in general, a disturbance.

**Key problem:** If Alice prepares a quantum system in a specific way, unknown fully to the eavesdropper Eve, and sends it to Bob

then the question is how much information can Eve extract of that quantum system and how much it costs in terms of the disturbance of the system.

Three special cases

- Eve has no information about the state $|\psi\rangle$ Alice sends.
- Eve knows that $|\psi\rangle$ is one of the states of an orthonormal basis $\{|\phi_i\rangle\}_{i=1}^n$.
- Eve knows that $|\psi\rangle$ is one of the states $|\phi_1\rangle, \ldots, |\phi_n\rangle$ that are not mutually orthonormal and that $p_i$ is the probability that $|\psi\rangle = |\phi_i\rangle$.

**BB84 Quantum Key Generation Protocol II**

Due to the laws of quantum physics, there is no detector that could distinguish between unorthogonal polarizations.

In a more formal setting, Bob can measure the incoming photons either in the standard basis $B = \{|0\rangle, |1\rangle\}$ or in the dual basis $D = \{|0\rangle', |1\rangle'\}$.

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⟩ or |1⟩'), i.e., in the standard or dual basis.

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

**BB84 Quantum Key Generation Protocol III**

An example of an encoding – decoding process is in the Figure 10.

Raw key extraction

Bob makes public the sequence of bases 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 measurement as she did for encoding. The corresponding bits then form the basic raw key.

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

---

**BB84 Quantum Key Generation of Classical Random Key**

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

**Preparation phase**

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

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).
**BB84 QUANTUM KEY GENERATION PROTOCOL III**

**Test for eavesdropping**

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 admissible error of the channel (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 raw keys after the key generation phase.

A way out is to use a special error correction techniques and at the end of this stage both Alice and Bob share identical keys.

**BB84 QUANTUM KEY GENERATION PROTOCOL IV**

**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 i-th bit of $S_i$, 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 $2^{-\left( n-k-1 \right) \ln 2}$.

**EXPERIMENTAL CRYPTOGRAPHY**

**Successes**

1. Transmissions using optical fibers to the distance of 200 km.
2. Open air transmissions to the distance 144 km at day time (from one pick of Canary Islands to another).
3. Next goal: earth to satellite transmissions.

All current systems use optical means for quantum state transmissions.

**Problems and tasks**

1. No single photon sources are available. Weak laser pulses currently used contains in average 0.1 - 0.2 photons.
2. Loss of signals in the fiber. (Current error rates: 0.5 - 4%)  
3. To move from the experimental to the developmental stage.

**QUANTUM TELEPORTATION - BASIC SETTING**

Quantum teleportation allows to transmit unknown quantum information to a very distant place in spite of impossibility to measure or to broadcast information to be transmitted.

Alice and Bob share two particles in the EPR-state

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

and then Alice receives another particle in an unknown qubit state

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

Alice then measure her two particles in the Bell basis.
QUANTUM TELEPORTATION - BASIC SETTING I

\[ |\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{and} \quad |EPR - pair\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \]

Total state
\[ |\psi\rangle|EPR - pair\rangle = \frac{1}{\sqrt{2}}(\alpha|00\rangle + \alpha|01\rangle + \beta|10\rangle + \beta|11\rangle) \]

Alice measures her two qubits with respect to the “Bell basis”:
\[ |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad \text{and} \quad |\Phi^\rightarrow\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \]
\[ |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad \text{and} \quad |\Psi^\rightarrow\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \]

QUANTUM TELEPORTATION III.

If the first two particles of the state
\[ |\psi\rangle|EPR - pair\rangle = |\Phi^+\rangle \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle) + |\Psi^+\rangle \frac{1}{\sqrt{2}}(\beta|0\rangle + \alpha|1\rangle) + |\Phi^\rightarrow\rangle \frac{1}{\sqrt{2}}(\alpha|0\rangle - \beta|1\rangle) + |\Psi^\rightarrow\rangle \frac{1}{\sqrt{2}}(-\beta|0\rangle + \alpha|1\rangle) \]

are measured with respect to the Bell basis then Bob’s particle gets into the mixed state
\[ \left( \frac{1}{4} |\psi\rangle + \frac{1}{4} |\phi\rangle \right) \oplus \left( \frac{1}{4} |\psi\rangle - \frac{1}{4} |\phi\rangle \right) \oplus \left( \frac{1}{4} |\psi\rangle \right) \oplus \left( \frac{1}{4} |\psi\rangle \right) \]

to which corresponds the density matrix
\[ \frac{1}{4} \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix} + \frac{1}{4} \begin{pmatrix} \alpha & -\beta \\ -\beta & \alpha \end{pmatrix} + \frac{1}{4} \begin{pmatrix} \beta & \alpha \\ \alpha & -\beta \end{pmatrix} = \frac{1}{2} I \]

The resulting density matrix is identical to the density matrix for the mixed state
\[ \begin{pmatrix} 1/2 & |0\rangle \\ |0\rangle & 1/2 \end{pmatrix} \]

Indeed, the density matrix for the last mixed state has the form
\[ \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2} I \]

QUANTUM TELEPORTATION – COMMENTS

- Alice can be seen as dividing information contained in |\psi\rangle into
  - quantum information – transmitted through EPR channel
  - classical information – transmitted through a classical channel
- In a quantum teleportation an unknown quantum state |\phi\rangle can be disassembled into, and later reconstructed from, two classical bit-states and an maximally entangled pure quantum state.
- Using quantum teleportation an unknown quantum state can be teleported from one place to another by a sender who does not need to know – for teleportation itself – neither the state to be teleported nor the location of the intended receiver.
- The teleportation procedure can not be used to transmit information faster than light but it can be argued that quantum information presented in unknown state is transmitted instantaneously (except two random bits to be transmitted at the speed of light at most).
- EPR channel is irreversibly destroyed during the teleportation process.

\[ |\phi\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} |0\rangle + \begin{pmatrix} 0 \\ 1 \end{pmatrix} |1\rangle \]

QUANTUM TELEPORTATION – BASIC SETTING II

Since the total state of all three particles is:
\[ |\psi\rangle|EPR - pair\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle) \]

and can be expressed also as follows:
\[ |\psi\rangle|EPR - pair\rangle = |\Phi^+\rangle \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle) + |\Psi^+\rangle \frac{1}{\sqrt{2}}(\beta|0\rangle + \alpha|1\rangle) + |\Phi^\rightarrow\rangle \frac{1}{\sqrt{2}}(\alpha|0\rangle - \beta|1\rangle) + |\Psi^\rightarrow\rangle \frac{1}{\sqrt{2}}(-\beta|0\rangle + \alpha|1\rangle) \]

then the Bell measurement of the first two particles projects the state of Bob’s particle into a “small modification” |\psi_1\rangle of the state |\psi\rangle = \alpha|0\rangle + \beta|1\rangle.
\[ |\psi_1\rangle = \begin{pmatrix} |\psi\rangle \text{ or } |\sigma_x|\psi\rangle \text{ or } |\sigma_y|\psi\rangle \text{ or } |\sigma_z\sigma_x|\psi\rangle \end{pmatrix} \]

The unknown state |\psi\rangle can therefore be obtained from |\psi_1\rangle by applying one of the four operations
\[ \sigma_x, \sigma_y, \sigma_z, I \]

and the result of the Bell measurement provides two bits specifying which of the above four operations should be applied.

These four bits Alice needs to send to Bob using a classical channel (by email, for example).
WHY IS QUANTUM INFORMATION PROCESSING SO IMPORTANT

- QIPC is believed to lead to new Quantum Information Processing Technology that could have broad impacts.
- Several areas of science and technology are approaching such points in their development where they badly need expertise with storing, transmission and processing of particles.
- It is increasingly believed that new, quantum information processing based, understanding of (complex) quantum phenomena and systems 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.

UNIVERSAL SETS of QUANTUM GATES

The main task at quantum computation is to express solution of a given problem $P$ as a unitary matrix $U$ and then to construct a circuit $C_U$ with elementary quantum gates from a universal sets of quantum gates to realize $U$.

A simple universal set of quantum gates consists of gates.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \sigma_\alpha^\frac{\pi}{4} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i} \end{pmatrix}$$

FUNDAMENTAL RESULTS

The first really satisfactory results, concerning universality of gates, have been due to Barenco et al. (1995)

Theorem 0.1 CNOT gate and all one-qubit gates form a universal set of gates.

The proof is in principle a simple modification of the RQ-decomposition from linear algebra. Theorem 0.1 can be easily improved:

Theorem 0.2 CNOT gate and elementary rotation gates

$$R_\alpha(\theta) = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} \sigma_\alpha$$

for $\alpha \in \{x, y, z\}$ form a universal set of gates.

QUANTUM ALGORITHMS

Quantum algorithms are methods of using quantum circuits and processors to solve algorithmic problems.

On a more technical level, a design of a quantum algorithm can be seen as a process of an efficient decomposition of a complex unitary transformation into products of elementary unitary operations (or gates), performing simple local changes.

The four main features of quantum mechanics that are exploited in quantum computation:

- Superposition;
- Interference;
- Entanglement;
- Measurement.
Deutsch problem: Given is a black-box function $f : \{0, 1\} \rightarrow \{0, 1\}$, how many queries are needed to find out whether $f$ is constant or balanced:
Classically: 2
Quantumly: 1

Deutsch-Jozsa Problem: Given is a black-box function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ and a promise that $f$ is either constant or balanced, how many queries are needed to find out whether $f$ is constant or balanced.
Classically: $n$
Quantumly 1

Factorization of integers: all classical algorithms are exponential.
Peter Shor developed polynomial time quantum algorithm

Search of an element in an unordered database of $n$ elements:
Classically $n$ queries are needed in the worst case
Lov Grover showed that quantumly $\sqrt{n}$ queries are enough