

## Part I

### Quantum cryptography



Quantum cryptography is an area of science and technology that explores and utilizes potential of quantum phenomena for getting higher quality (security) for cryptography tasks.

Quantum cryptography is an area of science and technology that explores and utilizes potential of quantum phenomena for getting higher quality (security) for cryptography tasks.

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

Quantum cryptography is an area of science and technology that explores and utilizes potential of quantum phenomena for getting higher quality (security) for cryptography tasks.

A new and important feature of quantum cryptography is that security of quantum cryptographical 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 physics laws were directly exploited to bring an essential advantage in information processing.

## MAIN OUTCOMES – so far

- It has been shown that with quantum computers, we could design absolutely secure quantum generation of shared and secret random classical keys.

## MAIN OUTCOMES – so far

- It has been shown that with quantum computers, 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).

## MAIN OUTCOMES – so far

- It has been shown that with quantum computers, 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 cryptography primitives, such as bit commitment and oblivious transfer, are impossible.



## MAIN OUTCOMES – so far

- It has been shown that with quantum computers, 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 cryptography primitives, such as bit commitment and oblivious transfer, are impossible.
- Quantum teleportation and pseudo-telepathy are possible.

## MAIN OUTCOMES – so far

- It has been shown that with quantum computers, 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 cryptography primitives, such as bit commitment and oblivious transfer, are impossible.
- Quantum teleportation and pseudo-telepathy are possible.
- Quantum cryptography and quantum networks are already in the developmental stages. Quantum communication between satellites and ground stations were already demonstrated for 2000 km in 2019 in China. That indicates that quantum internet seems possible.

As an introduction to quantum cryptography

As an introduction to quantum cryptography  
the very basic motivations, experiments, principles,  
concepts and results of quantum information processing  
and communication

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

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.

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

**Quantum physics** deals with fundamental entities of physics – **particles** (waves?) like

- **protons, electrons** and **neutrons** (from which matter is built);

**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)

**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.

**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.
- We call them particles in spite of the fact that some of their properties are totally unlike the properties of what we call particles in our ordinary classical world.

**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.
- We call them particles in spite of the fact that some of their properties are totally unlike the properties of what we call particles in our ordinary classical world.

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

**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.
- We call them particles in spite of the fact that some of their properties are totally unlike the properties of what we call particles in our ordinary classical world.

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 . . .

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

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

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?**

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.

# CLASSICAL versus QUANTUM INFORMATION

Main properties of classical information:

## Main properties of classical information:

- 1 It is easy to store, transmit and process classical information in time and space.

## Main properties of classical information:

- 1 It is easy to store, transmit and process classical information in time and space.
- 2 It is easy to make (unlimited number of) copies of classical information



## Main properties of classical information:

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

## Main properties of classical information:

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

## Main properties of quantum information:

## Main properties of classical information:

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

## Main properties of quantum information:

- 1 It is difficult to store, transmit and process quantum information

## Main properties of classical information:

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

## Main properties of quantum information:

- 1 It is difficult to store, transmit and process quantum information
- 2 There is no way to copy perfectly unknown quantum information

## Main properties of classical information:

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

## Main properties of quantum information:

- 1 It is difficult to store, transmit and process quantum information
- 2 There is no way to copy perfectly unknown quantum information
- 3 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.

**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

**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

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

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

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



## CLASSICAL versus QUANTUM REGISTERS

An  $n$  bit classical register can store at any moment exactly one  $n$ -bit string.

## CLASSICAL versus QUANTUM REGISTERS

An  $n$  bit classical register can store at any moment exactly one  $n$ -bit string.

An  $n$ -qubit quantum register can store at any moment a superposition of all  $2^n$   $n$ -bit strings.

## CLASSICAL versus QUANTUM REGISTERS

An  $n$  bit classical register can store at any moment exactly one  $n$ -bit string.

An  $n$ -qubit quantum register can store at any moment a superposition of all  $2^n$   $n$ -bit strings.

Consequently, on a quantum computer one can "compute" in a single step all  $2^n$  values of a function defined on  $n$ -bit inputs.

## CLASSICAL versus QUANTUM REGISTERS

An  $n$  bit classical register can store at any moment exactly one  $n$ -bit string.

An  $n$ -qubit quantum register can store at any moment a superposition of all  $2^n$   $n$ -bit strings.

Consequently, on a quantum computer one can "compute" in a single step all  $2^n$  values of a function defined on  $n$ -bit inputs.

This enormous massive parallelism is one reason why quantum computing can be so powerful.

# BASIC EXPERIMENTS

# CLASSICAL EXPERIMENTS

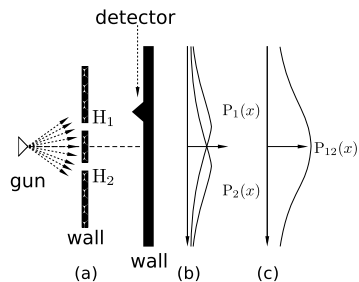


Figure 1: Experiment with bullets

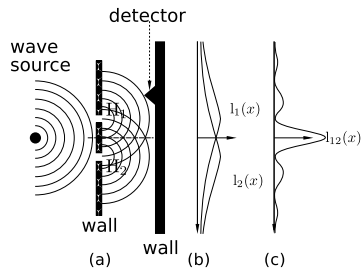
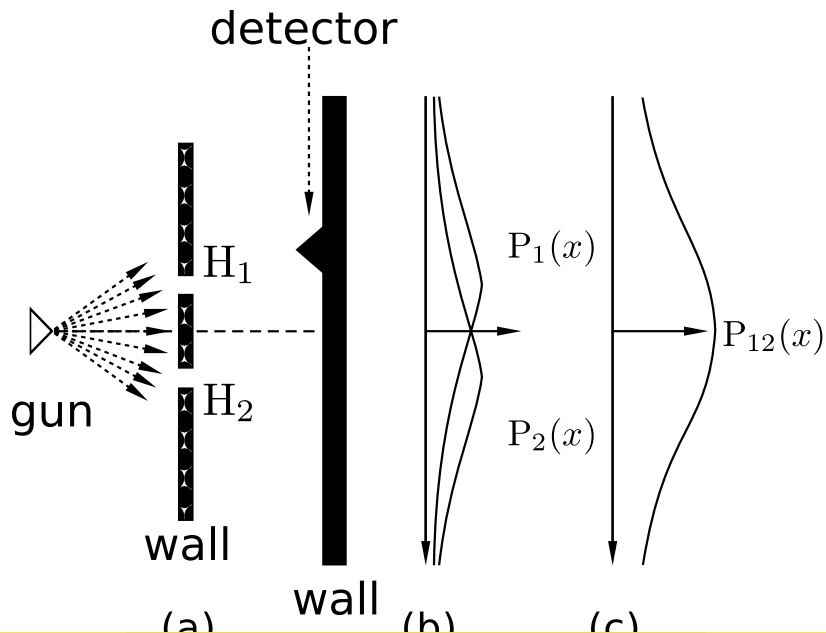
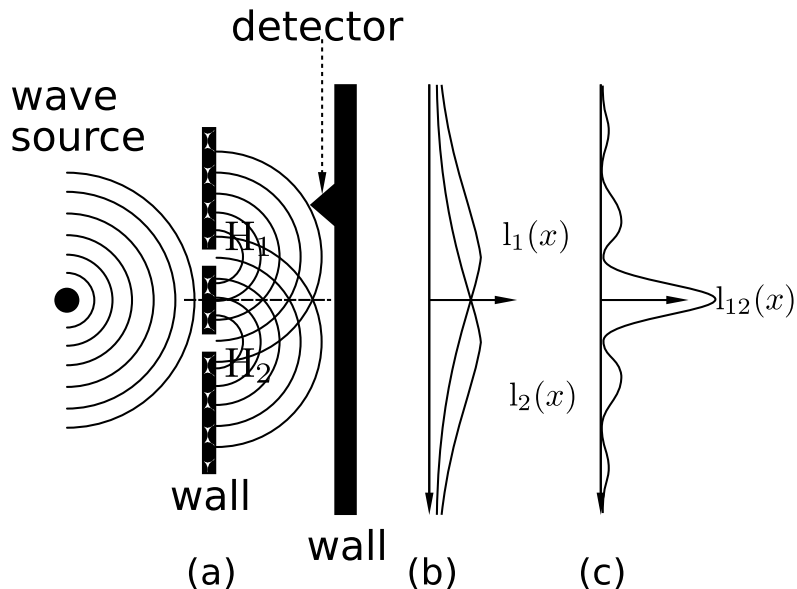


Figure 2: Experiments with waves

# CLASSICAL EXPERIMENT with bullets



# CLASSICAL EXPERIMENT with waves





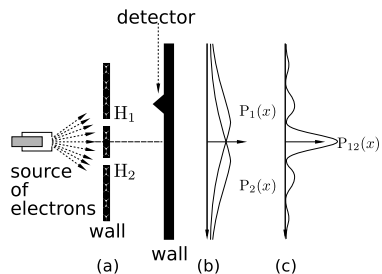


Figure 3: Two-slit experiment

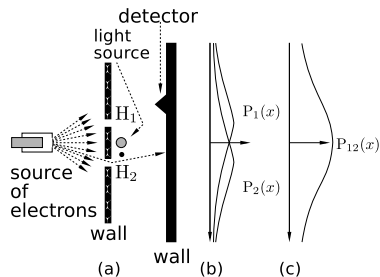
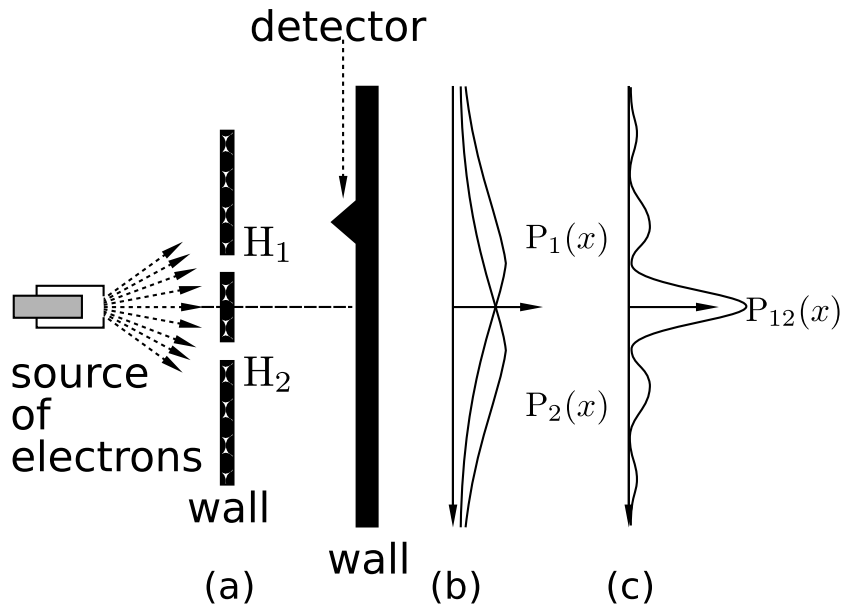
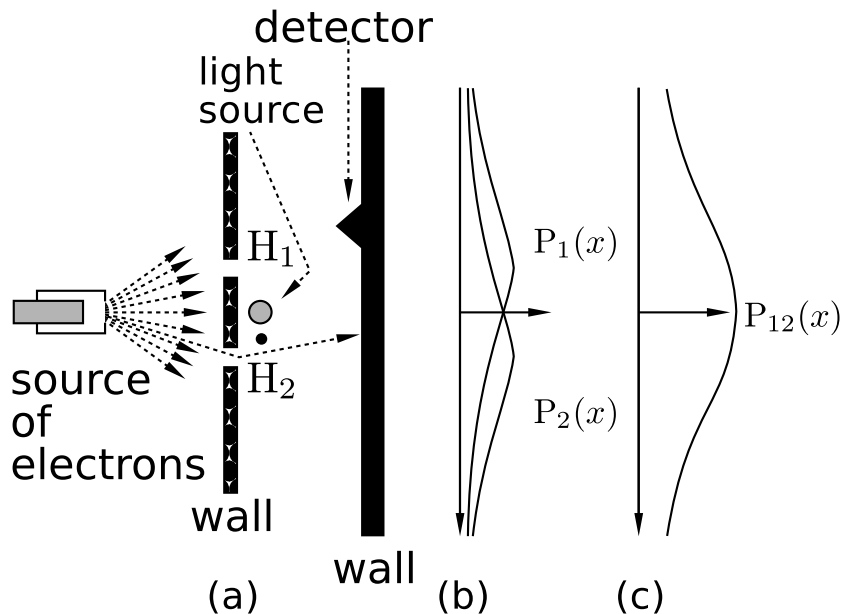


Figure 4: Two-slit experiment with an observation

# TWO-SLIT EXPERIMENT



## TWO-SLIT EXPERIMENT with OBSERVATION



# THREE BASIC PRINCIPLES of QUANTUM WORLD

**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.

# THREE BASIC PRINCIPLES of QUANTUM WORLD

**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:

$$\langle \psi | \phi \rangle = \langle \psi | \phi' \rangle \langle \phi' | \phi \rangle$$

# THREE BASIC PRINCIPLES of QUANTUM WORLD

**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.

# QUANTUM SYSTEMS = HILBERT SPACE

Hilbert space  $H_n$  is an n-dimensional complex vector space with

**scalar product**

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

# QUANTUM SYSTEMS = HILBERT SPACE

Hilbert space  $H_n$  is an n-dimensional complex vector space with

**scalar product**

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

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

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



# QUANTUM SYSTEMS = HILBERT SPACE

Hilbert space  $H_n$  is an n-dimensional complex vector space with

**scalar product**

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

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  $\langle \phi | \psi \rangle = 0$ .

# QUANTUM SYSTEMS = HILBERT SPACE

Hilbert space  $H_n$  is an n-dimensional complex vector space with

**scalar product**

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

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  $|b_1\rangle, |b_2\rangle, \dots, |b_n\rangle$  of the norm 1 which are mutually orthogonal.

# QUANTUM SYSTEMS = HILBERT SPACE

Hilbert space  $H_n$  is an n-dimensional complex vector space with

**scalar product**

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

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  $|b_1\rangle, |b_2\rangle, \dots, |b_n\rangle$  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:

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

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

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

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

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

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

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

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

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

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

$|\phi\rangle$  – ket-vector (a column vector) - an equivalent to  $\phi$

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

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

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

$|\phi\rangle$  – ket-vector (a column vector) - an equivalent to  $\phi$

$\langle \psi |$  – bra-vector (a row vector) a linear functional on  $H$

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



# EXAMPLES

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

$$|\phi\rangle = \begin{pmatrix} \phi_1 \\ \dots \\ \phi_n \end{pmatrix}, \langle\phi| = (\phi_1^*, \dots, \phi_n^*); \langle\phi|\psi\rangle = \sum_{i=1}^n \phi_i^* \psi_i;$$

$$|\phi\rangle\langle\psi| = \begin{pmatrix} \phi_1\psi_1^* & \dots & \phi_1\psi_n^* \\ \vdots & \ddots & \vdots \\ \phi_n\psi_1^* & \dots & \phi_n\psi_n^* \end{pmatrix}$$

EVOLUTION  
in  
QUANTUM SYSTEM

COMPUTATION  
in  
HILBERT SPACE

is described by

**Schrödinger linear equation**

$$i\hbar \frac{\partial |\Phi(t)\rangle}{\partial t} = H(t) |\Phi(t)\rangle$$

where  $\hbar$  is Planck constant,  $H(t)$  is a Hamiltonian (total energy) of the system that can be represented by a Hermitian matrix,

EVOLUTION  
in  
QUANTUM SYSTEM

COMPUTATION  
in  
HILBERT SPACE

is described by

**Schrödinger linear equation**

$$i\hbar \frac{\partial |\Phi(t)\rangle}{\partial t} = H(t) |\Phi(t)\rangle$$

where  $\hbar$  is Planck constant,  $H(t)$  is a Hamiltonian (total energy) of the system that can be represented by a Hermitian matrix, and  $|\Phi(t)\rangle$  is the state of the system in time  $t$ .

EVOLUTION  
in  
QUANTUM SYSTEM

COMPUTATION  
in  
HILBERT SPACE

is described by

**Schrödinger linear equation**

$$i\hbar \frac{\partial |\Phi(t)\rangle}{\partial t} = H(t) |\Phi(t)\rangle$$

where  $\hbar$  is Planck constant,  $H(t)$  is a Hamiltonian (total energy) of the system that can be represented by a Hermitian matrix, and  $|\Phi(t)\rangle$  is the state of the system in time  $t$ .  
If the Hamiltonian is time independent then the above Schrödinger equation has solution

$$|\Phi(t)\rangle = U(t) |\Phi(0)\rangle$$

where

$$U(t) = e^{\frac{iHt}{\hbar}}$$

is the evolution operator that can be represented by a **unitary matrix**.

# QUANTUM EVOLUTION / COMPUTATION

EVOLUTION  
in  
QUANTUM SYSTEM

COMPUTATION  
in  
HILBERT SPACE

is described by

**Schrödinger linear equation**

$$i\hbar \frac{\partial |\Phi(t)\rangle}{\partial t} = H(t) |\Phi(t)\rangle$$

where  $\hbar$  is Planck constant,  $H(t)$  is a Hamiltonian (total energy) of the system that can be represented by a Hermitian matrix, and  $|\Phi(t)\rangle$  is the state of the system in time  $t$ .  
If the Hamiltonian is time independent then the above Schrödinger equation has solution

$$|\Phi(t)\rangle = U(t) |\Phi(0)\rangle$$

where

$$U(t) = e^{\frac{iHt}{\hbar}}$$

is the evolution operator that can be represented by a **unitary matrix**. **A step of such an evolution is therefore a multiplication of a "unitary matrix"  $U$  with a vector  $|\psi\rangle$ , i.e.  $U |\psi\rangle$**

# UNITARY MATRICES

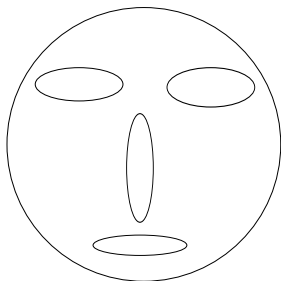
A matrix  $A$  is **unitary** if

$$A \cdot A^\dagger = A^\dagger \cdot A = I$$

where the matrix  $A^\dagger$  is obtained from the matrix  $A$  by revolving  $A$  around the main diagonal and changing all elements by their complex conjugates.

# QUANTUM (PROJECTION) MEASUREMENTS

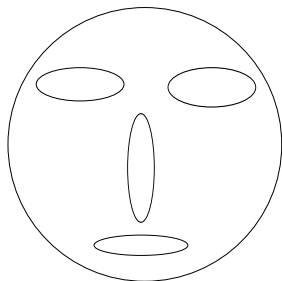
A quantum state is always observed (measured) with respect to an **observable**  $\mathcal{O}$  – a decomposition of a given Hilbert space into orthogonal subspaces (where each vector can be uniquely represented as a sum of vectors of these subspaces).





# QUANTUM (PROJECTION) MEASUREMENTS

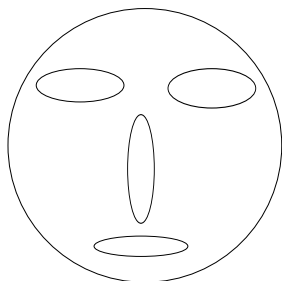
A quantum state is always observed (measured) with respect to an **observable**  $\mathcal{O}$  – a decomposition of a given Hilbert space into orthogonal subspaces (where each vector can be uniquely represented as a sum of vectors of these subspaces).



There are two outcomes of a projection measurement of a state  $|\phi\rangle$  with respect to  $\mathcal{O}$ :

# QUANTUM (PROJECTION) MEASUREMENTS

A quantum state is always observed (measured) with respect to an **observable**  $\mathcal{O}$  – 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).

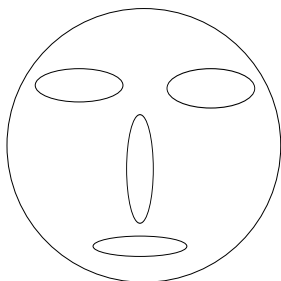


There are two outcomes of a projection measurement of a state  $|\phi\rangle$  with respect to  $\mathcal{O}$ :

- 1 Into classical world comes information into which subspace projection of  $|\phi\rangle$  was made.

# QUANTUM (PROJECTION) MEASUREMENTS

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).

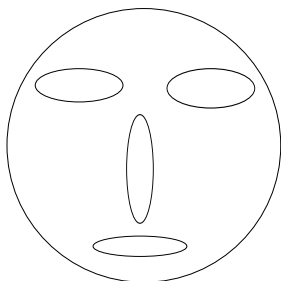


There are two outcomes of a projection measurement of a state  $|\phi\rangle$  with respect to  $O$ :

- 1 Into classical world comes information into which subspace projection of  $|\phi\rangle$  was made.
- 2 In the classical world projection of the measured state (as a new state)  $|\phi'\rangle$  stays in one of the above subspaces.

# QUANTUM (PROJECTION) MEASUREMENTS

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).



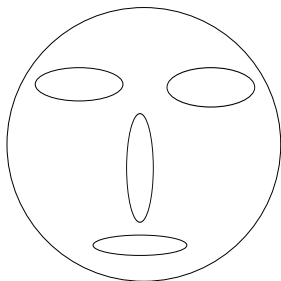
There are two outcomes of a projection measurement of a state  $|\phi\rangle$  with respect to  $O$ :

- 1 Into classical world comes information into which subspace projection of  $|\phi\rangle$  was made.
- 2 In the classical world projection of the measured state (as a new state)  $|\phi'\rangle$  stays in one of the above subspaces.

The subspace into which projection is made is chosen **randomly**

# QUANTUM (PROJECTION) MEASUREMENTS

A quantum state is always observed (measured) with respect to an **observable**  $\mathcal{O}$  – 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  $\mathcal{O}$ :

- 1 Into classical world comes information into which subspace projection of  $|\phi\rangle$  was made.
- 2 In the classical world projection of the measured state (as a new state)  $|\phi'\rangle$  stays 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.

# QUANTUM STATES and PROJECTION MEASUREMENT

# QUANTUM STATES and PROJECTION MEASUREMENT

In case an orthonormal basis  $\{|\beta_i\rangle\}_{i=1}^n$  is chosen in a Hilbert space  $H_n$ , then any state  $|\phi\rangle \in H_n$  can be expressed in the form

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

where

# QUANTUM STATES and PROJECTION MEASUREMENT

In case an orthonormal basis  $\{\beta_i\}_{i=1}^n$  is chosen in a Hilbert space  $H_n$ , then any state  $|\phi\rangle \in H_n$  can be expressed in the form

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

where

$a_i = \langle \beta_i | \phi \rangle$  are called **probability amplitudes**



# QUANTUM STATES and PROJECTION MEASUREMENT

In case an orthonormal basis  $\{\beta_i\}_{i=1}^n$  is chosen in a Hilbert space  $H_n$ , then any state  $|\phi\rangle \in H_n$  can be expressed in the form

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

where

$a_i = \langle \beta_i | \phi \rangle$  are called **probability amplitudes**

and

their squares provide **probabilities**

# QUANTUM STATES and PROJECTION MEASUREMENT

In case an orthonormal basis  $\{|\beta_i\rangle\}_{i=1}^n$  is chosen in a Hilbert space  $H_n$ , then any state  $|\phi\rangle \in H_n$  can be expressed in the form

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

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  $|a_i|^2$ .

# QUANTUM STATES and PROJECTION MEASUREMENT

In case an orthonormal basis  $\{|\beta_i\rangle\}_{i=1}^n$  is chosen in a Hilbert space  $H_n$ , then any state  $|\phi\rangle \in H_n$  can be expressed in the form

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

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.

# QUBITS

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  $H_2$

# QUBITS

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

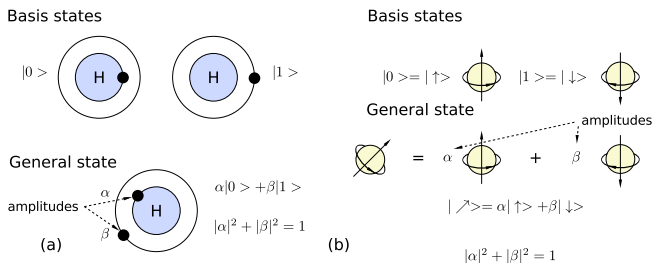


Figure 5: Qubit representations by energy levels of an electron in a hydrogen atom and by a spin-1/2 particle. The condition  $|\alpha|^2 + |\beta|^2 = 1$  is a legal one if  $|\alpha|^2$  and  $|\beta|^2$  are to be the probabilities of being in one of two basis states (of electrons or photons).

STANDARD BASIS

$$\begin{array}{l} |0\rangle, |1\rangle \\ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{array}$$

DUAL BASIS

$$\begin{array}{l} |0'\rangle, |1'\rangle \\ \begin{pmatrix} 1 \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \end{array}$$

STANDARD BASIS

$$\begin{matrix} |0\rangle, |1\rangle \\ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{matrix}$$

DUAL BASIS

$$\begin{matrix} |0'\rangle, |1'\rangle \\ \begin{pmatrix} 1 \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \end{matrix}$$

**Hadamard matrix**

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

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

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

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

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

transforms one of the basis into another one.

STANDARD BASIS

$$\begin{matrix} |0\rangle, |1\rangle \\ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{matrix}$$

DUAL BASIS

$$\begin{matrix} |0'\rangle, |1'\rangle \\ \begin{pmatrix} 1 \\ \frac{1}{\sqrt{2}} \\ 1 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ \frac{1}{\sqrt{2}} \\ 1 \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \end{matrix}$$

**Hadamard matrix**

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

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

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

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

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

transforms one of the basis into another one.

**General form of a unitary matrix of degree 2**

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



Very important one-qubit unary operators are the following **Pauli operators**, expressed in the standard basis as follows;

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

Very important one-qubit unary operators are the following **Pauli operators**, expressed in the standard basis as follows;

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

Observe that Pauli matrices transform a qubit state  $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$  as follows

$$\begin{aligned}\sigma_x(\alpha|0\rangle + \beta|1\rangle) &= \beta|0\rangle + \alpha|1\rangle \\ \sigma_z(\alpha|0\rangle + \beta|1\rangle) &= \alpha|0\rangle - \beta|1\rangle \\ \sigma_y(\alpha|0\rangle + \beta|1\rangle) &= \beta|0\rangle - \alpha|1\rangle\end{aligned}$$

## PAULI MATRICES

Very important one-qubit unary operators are the following **Pauli operators**, expressed in the standard basis as follows;

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

Observe that Pauli matrices transform a qubit state  $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$  as follows

$$\begin{aligned}\sigma_x(\alpha|0\rangle + \beta|1\rangle) &= \beta|0\rangle + \alpha|1\rangle \\ \sigma_z(\alpha|0\rangle + \beta|1\rangle) &= \alpha|0\rangle - \beta|1\rangle \\ \sigma_y(\alpha|0\rangle + \beta|1\rangle) &= \beta|0\rangle - \alpha|1\rangle\end{aligned}$$

Operators  $\sigma_x, \sigma_z$  and  $\sigma_y$  represent therefore a **bit error**, a **sign error** and a **bit-sign error**.

# QUANTUM MEASUREMENT of QUBITS

## of a qubit state

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

# QUANTUM MEASUREMENT of QUBITS

## of a qubit state

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:

# QUANTUM MEASUREMENT of QUBITS

## of a qubit state

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

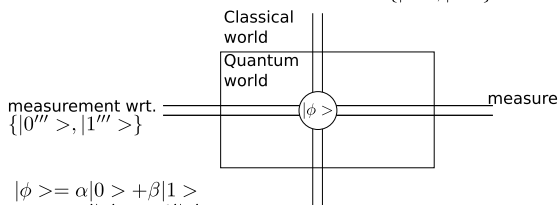
$$\alpha|0\rangle + \beta|1\rangle$$

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  $|\beta|^2$   
measurement wrt.  $\{|0\rangle, |1\rangle\}$



$$\begin{aligned} |\phi\rangle &= \alpha|0\rangle + \beta|1\rangle \\ &= \alpha'|0'\rangle + \beta'|1'\rangle \\ &= \alpha''|0''\rangle + \beta''|1''\rangle \\ &= \alpha'''|0'''\rangle + \beta'''|1'''\rangle \end{aligned}$$

measurement wrt.  $\{|0''\rangle, |1''\rangle\}$

## 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

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

## 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

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

One interpretation of a mixed state  $\{(p_i, |\phi_i\rangle)\}_{i=1}^k$  is that a source  $X$  produces the state  $|\phi_i\rangle$  with probability  $p_i$ .



## 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

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

One interpretation of a mixed state  $\{(p_i, |\phi_i\rangle)\}_{i=1}^k$  is that a source  $X$  produces the state  $|\phi_i\rangle$  with probability  $p_i$ .

Any matrix representing a density operator is called **density matrix**.

## 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

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

One interpretation of a mixed state  $\{(p_i, |\phi_i\rangle)\}_{i=1}^k$  is that a source  $X$  produces the state  $|\phi_i\rangle$  with probability  $p_i$ .

Any matrix representing a density operator is called **density matrix**.

Density matrices are exactly Hermitian, positive matrices with trace 1.

## 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

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

One interpretation of a mixed state  $\{(p_i, |\phi_i\rangle)\}_{i=1}^k$  is that a source  $X$  produces the state  $|\phi_i\rangle$  with probability  $p_i$ .

Any matrix representing a density operator is called **density matrix**.

Density matrices are exactly Hermitian, positive matrices with trace 1.

To two different mixed states can correspond the same density matrix.

**Two mixed states with the same density matrix are physically indistinguishable.**

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

$$\frac{1}{2} \begin{pmatrix} 1 \\ 0 \end{pmatrix} (1, 0) + \frac{1}{2} \begin{pmatrix} 0 \\ 1 \end{pmatrix} (0, 1) = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2} I_2$$

## 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

$$\frac{1}{2} \begin{pmatrix} 1 \\ 0 \end{pmatrix} (1, 0) + \frac{1}{2} \begin{pmatrix} 0 \\ 1 \end{pmatrix} (0, 1) = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2} I_2$$

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 an  $n$ -bit string  $p$

shared key an  $n$ -bit string  $k$

cryptotext an  $n$ -bit string  $c$

encoding  $c = p \oplus k$

decoding  $p = c \oplus k$

# QUANTUM ONE-TIME PAD CRYPTOSYSTEM

## CLASSICAL ONE-TIME PAD cryptosystem

plaintext an n-bit string  $p$

shared key an n-bit string  $k$

cryptotext an n-bit string  $c$

encoding  $c = p \oplus k$

decoding  $p = c \oplus k$

## QUANTUM ONE-TIME PAD cryptosystem

plaintext: an n-qubit string  $|p\rangle = |p_1\rangle \dots |p_n\rangle$

shared key: two n-bit strings  $k, k'$

cryptotext: an n-qubit string  $|c\rangle = |c_1\rangle \dots |c_n\rangle$

encoding:  $|c_i\rangle = \sigma_x^{k_i} \sigma_z^{k'_i} |p_i\rangle$

decoding:  $|p_i\rangle = \sigma_z^{k'_i} \sigma_x^{k_i} |c_i\rangle$

where  $|p_i\rangle = \begin{pmatrix} a_i \\ b_i \end{pmatrix}$  and  $|c_i\rangle = \begin{pmatrix} d_i \\ e_i \end{pmatrix}$  are qubits and  $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  with  $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  are Pauli matrices.

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

$$\left(\frac{1}{4}, |\phi\rangle\right), \left(\frac{1}{4}, \sigma_x|\phi\rangle\right), \left(\frac{1}{4}, \sigma_z|\phi\rangle\right), \left(\frac{1}{4}, \sigma_x\sigma_z|\phi\rangle\right)$$

whose density matrix is

$$\frac{1}{2}I_2$$



# 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

$$\left(\frac{1}{4}, |\phi\rangle\right), \left(\frac{1}{4}, \sigma_x|\phi\rangle\right), \left(\frac{1}{4}, \sigma_z|\phi\rangle\right), \left(\frac{1}{4}, \sigma_x\sigma_z|\phi\rangle\right)$$

whose density matrix is

$$\frac{1}{2}I_2$$

This density matrix is identical to the density matrix corresponding to that of a random bit, that is to the 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.

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

$$(x_1, \dots, x_n) \otimes (y_1, \dots, y_m) = (x_1 y_1, \dots, x_1 y_m, x_2 y_1, \dots, x_2 y_m, \dots, x_2 y_m, \dots, x_n y_1, \dots, x_n y_m)$$

Tensor product of matrices  $A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & & \vdots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix}$

where  $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$

# COMPOSED QUANTUM SYSTEMS (1)

## Tensor product of vectors

$$(x_1, \dots, x_n) \otimes (y_1, \dots, y_m) = (x_1 y_1, \dots, x_1 y_m, x_2 y_1, \dots, x_2 y_m, \dots, x_2 y_m, \dots, x_n y_1, \dots, x_n y_m)$$

$$\text{Tensor product of matrices } A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & & \vdots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix}$$

$$\text{where } A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$$

$$\text{Example } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 \\ 0 & 0 & a_{11} & a_{12} \\ 0 & 0 & a_{21} & a_{22} \end{pmatrix}$$

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

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  $H_2$ .

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  $H_4$ , i.e.

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

# 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.

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

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

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

# 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.

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

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:

$$CNOT : |x, y\rangle \Rightarrow |x, x \oplus y\rangle$$

# NO-CLONING THEOREM

**INFORMAL VERSION:** Unknown quantum state cannot be cloned.

# 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  $|\psi\rangle$

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

# 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  $|\beta\rangle$

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

# 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

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

# 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

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



# 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

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), & |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), & |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned}$$

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

States

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), & |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), & |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned}$$

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:

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

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

---

<sup>1</sup>The dot product is defined as follows:  $x \cdot y = \sum_{i=1}^n x_i y_i$ .

# QUANTUM n-qubit REGISTERS

A general state of an n-qubit register has the form:

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

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

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

---

<sup>1</sup>The dot product is defined as follows:  $x \cdot y = \sum_{i=1}^n x_i y_i$ .

# QUANTUM n-qubit REGISTERS

A general state of an n-qubit register has the form:

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

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?

---

<sup>1</sup>The dot product is defined as follows:  $x \cdot y = \sum_{i=1}^n x_i y_i$ .

# QUANTUM n-qubit REGISTERS

A general state of an n-qubit register has the form:

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

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.

---

<sup>1</sup>The dot product is defined as follows:  $x \cdot y = \sum_{i=1}^n x_i y_i$ .

# QUANTUM n-qubit REGISTERS

A general state of an n-qubit register has the form:

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

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

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

---

<sup>1</sup>The dot product is defined as follows:  $x \cdot y = \otimes_{i=1}^n x_i y_i$ .



# QUANTUM n-qubit REGISTERS

A general state of an n-qubit register has the form:

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

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

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

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

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

---

<sup>1</sup>The dot product is defined as follows:  $x \cdot y = \sum_{i=1}^n x_i y_i$ .

# QUANTUM PARALLELISM

If

$$f : \{0, 1, \dots, 2^n - 1\} \Rightarrow \{0, 1, \dots, 2^n - 1\}$$

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.

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

# QUANTUM PARALLELISM

If

$$f : \{0, 1, \dots, 2^n - 1\} \Rightarrow \{0, 1, \dots, 2^n - 1\}$$

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

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

# QUANTUM PARALLELISM

If

$$f : \{0, 1, \dots, 2^n - 1\} \Rightarrow \{0, 1, \dots, 2^n - 1\}$$

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

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

# QUANTUM PARALLELISM

If

$$f : \{0, 1, \dots, 2^n - 1\} \Rightarrow \{0, 1, \dots, 2^n - 1\}$$

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 WHAT LIES POWER OF QUANTUM COMPUTING?

In quantum superposition or in quantum parallelism?

# IN WHAT LIES POWER OF QUANTUM COMPUTING?

In quantum superposition or in quantum parallelism?

NOT,



# IN WHAT LIES POWER OF QUANTUM COMPUTING?

In quantum superposition or in quantum parallelism?

NOT,

in **QUANTUM ENTANGLEMENT!**

# IN WHAT LIES POWER OF QUANTUM COMPUTING?

In quantum superposition or in quantum parallelism?

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

$|00\rangle$  or  $|11\rangle$ .

# IN WHAT LIES POWER OF QUANTUM COMPUTING?

In quantum superposition or in quantum parallelism?

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

$|00\rangle$  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  $B$ .

## 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

## 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)

## 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.

## 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



# 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

# 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

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

## CLASSICAL versus QUANTUM CRYPTOGRAPHY

- Security of 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.

# CLASSICAL versus QUANTUM CRYPTOGRAPHY

- Security of 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.

## CLASSICAL versus QUANTUM CRYPTOGRAPHY

- Security of 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.

# 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.

## 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.



# 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)

# 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)

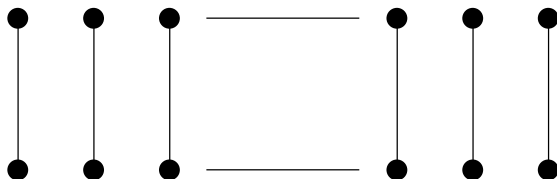
where one can expect the first

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.

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

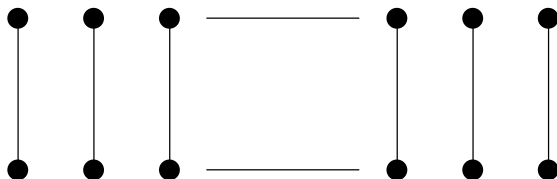


$n$  pairs of particles in EPR state

## 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  $n$ .

# POLARIZATION of PHOTONS

Polarized photons are currently mainly used for experimental quantum key generation.

# POLARIZATION of PHOTONS

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.

# POLARIZATION of PHOTONS

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.

# POLARIZATION of PHOTONS

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.



# LINEAR POLARIZATION - visualization

## LINEAR POLARIZATION - visualization

You can think of light as traveling in waves.

## LINEAR POLARIZATION - visualization

You can think of light as traveling in waves. One way to visualize these waves is to imagine taking a long rope and tying one end in a fixed place and to move the free end in some way.

## LINEAR POLARIZATION - visualization

You can think of light as traveling in waves. One way to visualize these waves is to imagine taking a long rope and tying one end in a fixed place and to move the free end in some way.

Moving the free end of the rope up and down sets up a "wave" along the rope which also moves up and down.

## LINEAR POLARIZATION - visualization

You can think of light as traveling in waves. One way to visualize these waves is to imagine taking a long rope and tying one end in a fixed place and to move the free end in some way.

Moving the free end of the rope up and down sets up a "wave" along the rope which also moves up and down. If you think of the rope as representing a beam of light, the light would be a "vertically polarized".

## LINEAR POLARIZATION - visualization

You can think of light as traveling in waves. One way to visualize these waves is to imagine taking a long rope and tying one end in a fixed place and to move the free end in some way.

Moving the free end of the rope up and down sets up a "wave" along the rope which also moves up and down. If you think of the rope as representing a beam of light, the light would be a "vertically polarized".

If the free end of the rope is moved from side to side a wave that moves from side to side is set up.

## LINEAR POLARIZATION - visualization

You can think of light as traveling in waves. One way to visualize these waves is to imagine taking a long rope and tying one end in a fixed place and to move the free end in some way.

Moving the free end of the rope up and down sets up a "wave" along the rope which also moves up and down. If you think of the rope as representing a beam of light, the light would be a "vertically polarized".

If the free end of the rope is moved from side to side a wave that moves from side to side is set up. If this way moves a light beam, it is called "horizontally polarized".

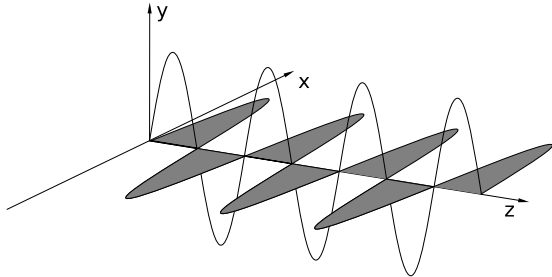


Figure: Linearly polarized photons - visualization

Both vertical and horizontal polarizations are examples of "linear polarizations".

If the free end of the rope is moved around in a circle, then we would get a wave that looks like a corkscrew. This would visualize **circular polarization**"



# POLARIZATION of PHOTONS III

Generation of orthogonally polarized photons.

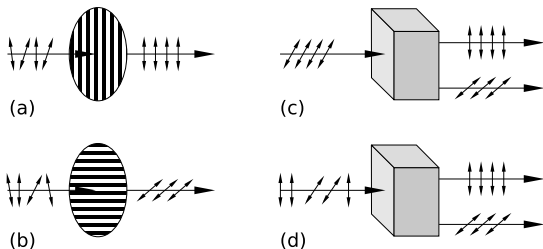


Figure: Photon polarizers and measuring devices

For any polarizations there are generators that produce photons only of a given polarizations. For example, calcite crystals, shown in Fig. a and b can do the job.

# POLARIZATION of PHOTONS III

Generation of orthogonally polarized photons.

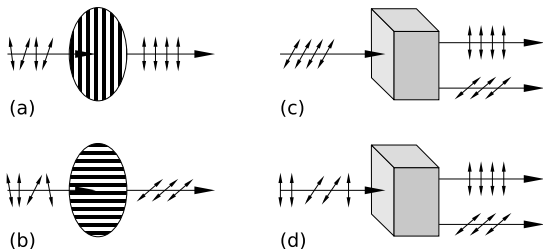


Figure: Photon polarizers and measuring devices

For any polarizations there are generators that produce photons only of a given polarizations. For example, calcite crystals, shown in Fig. a and b can do the job.

Fig. c – a calcite crystal that makes  $\theta$ -polarized photons to be horizontally (vertically) polarized with probability  $\cos^2\theta(\sin^2\theta)$ .

# POLARIZATION of PHOTONS III

Generation of orthogonally polarized photons.

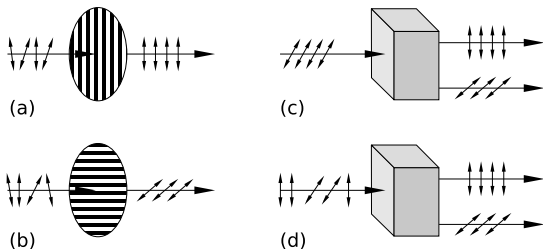


Figure: Photon polarizers and measuring devices

For any polarizations there are generators that produce photons only of a given polarizations. For example, calcite crystals, shown in Fig. a and b can do the job.

Fig. c – a calcite crystal that makes  $\theta$ -polarized photons to be horizontally (vertically) polarized with probability  $\cos^2\theta(\sin^2\theta)$ .

Fig. d – a calcite crystal can be used to separate horizontally and vertically polarized photons.

# QUANTUM GENERATION of CLASSICAL KEYS – 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.

# QUANTUM GENERATION of CLASSICAL KEYS – 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.

# QUANTUM GENERATION of CLASSICAL KEYS – 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.

# QUANTUM GENERATION of CLASSICAL KEYS – 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

# QUANTUM GENERATION of CLASSICAL KEYS – 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

- 1 Eve has no information about the state  $|\psi\rangle$  Alice sends.



# QUANTUM GENERATION of CLASSICAL KEYS – 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

- 1 Eve has no information about the state  $|\psi\rangle$  Alice sends.
- 2 Eve knows that  $|\psi\rangle$  is one of the states of an orthonormal basis  $\{|\phi_i\rangle\}_{i=1}^n$ .

# QUANTUM GENERATION of CLASSICAL KEYS – 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

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

## BB84 QUANTUM 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:

# BB84 QUANTUM 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

# BB84 QUANTUM 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

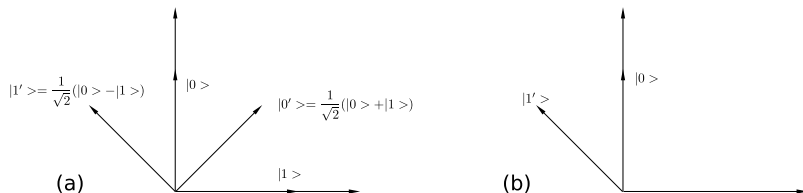


Figure 8: Polarizations of photons for BB84 and B92 protocols

# BB84 QUANTUM 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

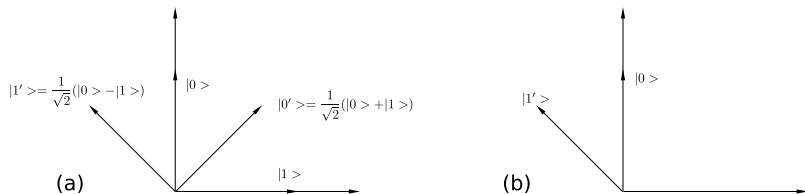


Figure 8: Polarizations of photons for BB84 and B92 protocols

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

# BB84 QUANTUM 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

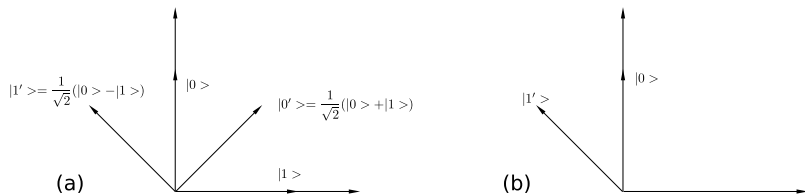


Figure 8: Polarizations of photons for BB84 and B92 protocols

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).

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**.



# 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**.

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
B	D	D	D	B	B	D	B	B	D	B	Bob's observable
1	0	R	0	1	R	0	0	0	R	R	outcomes

# 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**.

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
B	D	D	D	B	B	D	B	B	D	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.

## 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.

## 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.

## 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.

## 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.

## 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.

Privacy amplification phase



## 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 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  $S_1, \dots, S_n$  of bits of  $s'$  and let  $s_i$ , the  $i$ -th 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  $s'$ .

## 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  $S_1, \dots, S_n$  of bits of  $s'$  and let  $s_i$ , the  $i$ -th 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  $\frac{2^{-(n-k-1)}}{\ln 2}$ .

## Successes

- 1 Transmissions using optical fibers to the distance of 200 km.

## 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 in 2014).

## 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 in 2014).
- 3 Next goal: earth to satellite transmissions was met in 2019.

## 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 in 2014).
- 3 Next goal: earth to satellite transmissions was met in 2019.

All current systems use optical means for quantum state transmissions

## 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 in 2014).
- 3 Next goal: earth to satellite transmissions was met in 2019.

All current systems use optical means for quantum state transmissions

## Problems and tasks



## 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 in 2014).
- 3 Next goal: earth to satellite transmissions was met in 2019.

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.

## 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 in 2014).
- 3 Next goal: earth to satellite transmissions was met in 2019.

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%)

## 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 in 2014).
- 3 Next goal: earth to satellite transmissions was met in 2019.

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

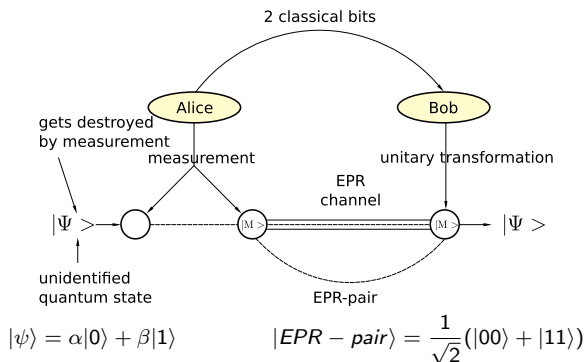
$$|EPR_{pair}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

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



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

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

Total state

$$|\psi\rangle|EPR - pair\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

Alice measures her two qubits with respect to the "Bell basis":

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

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

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

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

## QUANTUM TELEPORTATION 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:

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

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

$$|\Psi_1\rangle = \text{either } |\Psi\rangle \text{ or } \sigma_x|\Psi\rangle \text{ or } \sigma_z|\Psi\rangle \text{ or } \sigma_x\sigma_z|\psi\rangle$$

## QUANTUM TELEPORTATION 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:

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

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

$$|\Psi_1\rangle = \text{either } |\Psi\rangle \text{ or } \sigma_x|\Psi\rangle \text{ or } \sigma_z|\Psi\rangle \text{ or } \sigma_x\sigma_z|\psi\rangle$$

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.

## QUANTUM TELEPORTATION 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:

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

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

$$|\Psi_1\rangle = \text{either } |\Psi\rangle \text{ or } \sigma_x|\Psi\rangle \text{ or } \sigma_z|\Psi\rangle \text{ or } \sigma_x\sigma_z|\psi\rangle$$

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).



## QUANTUM TELEPORTATION III.

If the first two particles of the state

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

are measured with respect to the Bell basis then Bob's particle gets into the mixed state

$$\left(\frac{1}{4}, \alpha|0\rangle + \beta|1\rangle\right) \oplus \left(\frac{1}{4}, \alpha|0\rangle - \beta|1\rangle\right) \oplus \left(\frac{1}{4}, \beta|0\rangle + \alpha|1\rangle\right) \oplus \left(\frac{1}{4}, \beta|0\rangle - \alpha|1\rangle\right)$$

to which corresponds the density matrix

$$\frac{1}{4} \begin{pmatrix} \alpha^* \\ \beta^* \end{pmatrix} (\alpha, \beta) + \frac{1}{4} \begin{pmatrix} \alpha^* \\ -\beta^* \end{pmatrix} (\alpha, -\beta) + \frac{1}{4} \begin{pmatrix} \beta^* \\ \alpha^* \end{pmatrix} (\beta, \alpha) + \frac{1}{4} \begin{pmatrix} \beta^* \\ -\alpha^* \end{pmatrix} (\beta, -\alpha) = \frac{1}{2} I$$

## QUANTUM TELEPORTATION III.

If the first two particles of the state

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

are measured with respect to the Bell basis then Bob's particle gets into the mixed state

$$\left(\frac{1}{4}, \alpha|0\rangle + \beta|1\rangle\right) \oplus \left(\frac{1}{4}, \alpha|0\rangle - \beta|1\rangle\right) \oplus \left(\frac{1}{4}, \beta|0\rangle + \alpha|1\rangle\right) \oplus \left(\frac{1}{4}, \beta|0\rangle - \alpha|1\rangle\right)$$

to which corresponds the density matrix

$$\frac{1}{4} \begin{pmatrix} \alpha^* \\ \beta^* \end{pmatrix} (\alpha, \beta) + \frac{1}{4} \begin{pmatrix} \alpha^* \\ -\beta^* \end{pmatrix} (\alpha, -\beta) + \frac{1}{4} \begin{pmatrix} \beta^* \\ \alpha^* \end{pmatrix} (\beta, \alpha) + \frac{1}{4} \begin{pmatrix} \beta^* \\ -\alpha^* \end{pmatrix} (\beta, -\alpha) = \frac{1}{2} I$$

The resulting density matrix is identical to the density matrix for the mixed state

$$\left(\frac{1}{2}, |0\rangle\right) \oplus \left(\frac{1}{2}, |1\rangle\right)$$

Indeed, the density matrix for the last mixed state has the form

$$\frac{1}{2} \begin{pmatrix} 1 \\ 0 \end{pmatrix} (1, 0) + \frac{1}{2} \begin{pmatrix} 0 \\ 1 \end{pmatrix} (0, 1) = \frac{1}{2} I$$

# QUANTUM TELEPORTATION – COMMENTS

- Alice can be seen as dividing information contained in  $|\psi\rangle$  into
  - quantum information – transmitted through EPR channel

# 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

# 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.

# 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.

# 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).

# 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.





## WHY IS QUANTUM INFORMATION PROCESSING SO IMPORTANT

- QIPC is believed to lead to new Quantum Information Processing Technology that could have broad impacts.

# 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.

# 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.

# 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.

# 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  $U$ .

## 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.

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



## FUNDAMENTAL RESULTS

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

# 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:

# 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**

$$R_{\alpha}(\theta) = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} \sigma_{\alpha} \quad \text{for } \alpha \in \{x, y, z\}$$

**form a universal set of gates.**

# DESIGN of QUANTUM PROCESSORS

- For years attempts to implement a quantum processor ended at 8 to 10 qubits processors.
- Canadian company D-WAVE? offered in 2007 a 16-qubit processor,

# DESIGN of QUANTUM PROCESSORS

- For years attempts to implement a quantum processor ended at 8 to 10 qubit processors.
- Canadian company D-WAVE offered in 2007 a 16-qubit processor, later, step by step, a 28-qubits, then 128-qubits later 128-qubits and finally a 512-qubit processor.

- For years attempts to implement a quantum processor ended at 8 to 10 qubits processors.
- Canadian company D-WAVE offered in 2007 a 16-qubit processor, later, step by step, a 28-qubits, then 128-qubits later 128-qubits qubits and finally a 512-qubit processor. In 2008 they offered 1024-qubits processor and in 2018 2048 qubits processors. They also claimed superiority of their processors for solving optimization problem in comparison with current classical processors. However, there was a lot of controversy how much are their processors fully quantum.
- In 2016 IBM announced a 49-qubits processor, in 2018 IBM 53-qubits processors and in 2019 GOOGLE a 72-qubits processors. All of them had to be superior with respect to classical supercomputers in solving a variety of optimization problems.

# DESIGN of QUANTUM PROCESSORS

- For years attempts to implement a quantum processor ended at 8 to 10 qubit processors.
- Canadian company D-WAVE offered in 2007 a 16-qubit processor, later, step by step, a 28-qubits, then 128-qubits later 128-qubits qubits and finally a 512-qubit processor. In 2008 they offered 1024-qubits processor and in 2018 2048 qubits processors. They also claimed superiority of their processors for solving optimization problem in comparison with current classical processors. However, there was a lot of controversy how much are their processors fully quantum.
- In 2016 IBM announced a 49-qubits processor, in 2018 IBM 53-qubits processors and in 2019 GOOGLE a 72-qubits processors. All of them had to be superior with respect to classical supercomputers in solving a variety of optimization problems. In 100-authors paper from Google they claimed the existence of 53 qubit processor (with qubits arranged in a net where each qubit was connected with 4 neighbour). They claim to be compatible with current supercomputers for solving a variety of optimization problems.

# QUANTUM ALGORITHMS

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



# 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.

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;

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;

# 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;

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.

# EXAMPLES of QUANTUM ALGORITHMS

**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

## EXAMPLES of QUANTUM ALGORITHMS

**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

## EXAMPLES of QUANTUM ALGORITHMS

**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



## EXAMPLES of QUANTUM ALGORITHMS

**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

In the following we present the basic idea behind a polynomial time algorithm for quantum computers to factorize integers.

In the following we present the basic idea behind a polynomial time algorithm for quantum computers to factorize integers.

Quantum computers works with superpositions of basic quantum states on which very special (unitary) operations are applied and and very special quantum features (non-locality) are used.

In the following we present the basic idea behind a polynomial time algorithm for quantum computers to factorize integers.

Quantum computers works with superpositions of basic quantum states on which very special (unitary) operations are applied and and very special quantum features (non-locality) are used.

Quantum computers work not with **bits**, that can take on any of two values 0 and 1, but with **qubits** (quantum bits) that can take on any of infinitely many states  $\alpha|0\rangle + \beta|1\rangle$ , where  $\alpha$  and  $\beta$  are complex numbers such that  $|\alpha|^2 + |\beta|^2 = 1$ .

Shor's polynomial time quantum factorization algorithm is based on an understanding that factorization problem can be reduced

- 1 first on the problem of solving a simple modular quadratic equation;
- 2 second on the problem of finding periods of functions  $f(x) = a^x \bmod n$ .

# FIRST REDUCTION

**Lemma** If there is a polynomial time deterministic (randomized) [quantum] algorithm to find a nontrivial solution of the modular quadratic equations

$$a^2 \equiv 1 \pmod{n},$$

then there is a polynomial time deterministic (randomized) [quantum] algorithm to factorize integers.

# FIRST REDUCTION

**Lemma** If there is a polynomial time deterministic (randomized) [quantum] algorithm to find a nontrivial solution of the modular quadratic equations

$$a^2 \equiv 1 \pmod{n},$$

then there is a polynomial time deterministic (randomized) [quantum] algorithm to factorize integers.

**Proof.** Let  $a \neq \pm 1$  be such that  $a^2 \equiv 1 \pmod{n}$ . Since

$$a^2 - 1 = (a + 1)(a - 1),$$

if  $n$  is not prime, then a prime factor of  $n$  has to be a prime factor of either  $a + 1$  or  $a - 1$ . By using Euclid's algorithm to compute

$$\gcd(a + 1, n) \quad \text{and} \quad \gcd(a - 1, n)$$

we can find, in  $O(\lg n)$  steps, a prime factor of  $n$ .

## SECOND REDUCTION

The second key concept is that of the **period** of functions

$$f_{n,x}(k) = x^k \bmod n.$$



## SECOND REDUCTION

The second key concept is that of the **period** of functions

$$f_{n,x}(k) = x^k \bmod n.$$

Period is the smallest integer  $r$  such that

$$f_{n,x}(k+r) = f_{n,x}(k)$$

for any  $k$ , i.e. the smallest  $r$  such that

$$x^r \equiv 1 \pmod{n}.$$

## SECOND REDUCTION

The second key concept is that of the **period** of functions

$$f_{n,x}(k) = x^k \bmod n.$$

Period is the smallest integer  $r$  such that

$$f_{n,x}(k+r) = f_{n,x}(k)$$

for any  $k$ , i.e. the smallest  $r$  such that

$$x^r \equiv 1 \pmod{n}.$$

**AN ALGORITHM TO SOLVE EQUATION  $x^2 \equiv 1 \pmod{n}$ .**

- 1 Choose randomly  $1 < a < n$ .
- 2 Compute  $\gcd(a, n)$ . If  $\gcd(a, n) \neq 1$  we have a factor.
- 3 Find period  $r$  of function  $a^k \bmod n$ .
- 4 If  $r$  is odd or  $a^{r/2} \equiv \pm 1 \pmod{n}$ , then go to step 1; otherwise stop.

If this algorithm stops, then  $a^{r/2}$  is a non-trivial solution of the equation

$$x^2 \equiv 1 \pmod{n}.$$

## EXAMPLE

Let  $n = 15$ . Select  $a < 15$  such that  $\gcd(a, 15) = 1$ .  
{The set of such  $a$  is  $\{2, 4, 7, 8, 11, 13, 14\}$ }

Choose  $a = 11$ . Values of  $11^x \bmod 15$  are then

$$11, 1, 11, 1, 11, 1$$

which gives  $r = 2$ .

Hence  $a^{r/2} = 11 \pmod{15}$ . Therefore

$$\gcd(15, 12) = 3, \quad \gcd(15, 10) = 5$$

## EXAMPLE

Let  $n = 15$ . Select  $a < 15$  such that  $\gcd(a, 15) = 1$ .  
{The set of such  $a$  is  $\{2, 4, 7, 8, 11, 13, 14\}$ }

Choose  $a = 11$ . Values of  $11^x \bmod 15$  are then

$$11, 1, 11, 1, 11, 1$$

which gives  $r = 2$ .

Hence  $a^{r/2} = 11 \pmod{15}$ . Therefore

$$\gcd(15, 12) = 3, \quad \gcd(15, 10) = 5$$

For  $a = 14$  we get again  $r = 2$ , but in this case

$$14^{2/2} \equiv -1 \pmod{15}$$

and the following algorithm fails.

- 1 Choose randomly  $1 < a < n$ .
- 2 Compute  $\gcd(a, n)$ . If  $\gcd(a, n) \neq 1$  we have a factor.
- 3 Find period  $r$  of function  $a^k \bmod n$ .
- 4 If  $r$  is odd or  $a^{r/2} \equiv \pm 1 \pmod{n}$ , then go to step 1; otherwise stop.

## EFFICIENCY of REDUCTION

**Lemma** If  $1 < a < n$  satisfying  $\gcd(n, a) = 1$  is selected in the above algorithm randomly and  $n$  is not a power of prime, then

$$\Pr\{r \text{ is even and } a^{r/2} \not\equiv \pm 1\} \geq \frac{9}{16}.$$

- 1 Choose randomly  $1 < a < n$ .
- 2 Compute  $\gcd(a, n)$ . If  $\gcd(a, n) \neq 1$  we have a factor.
- 3 Find period  $r$  of function  $a^k \bmod n$ .
- 4 If  $r$  is odd or  $a^{r/2} \equiv \pm 1 \pmod{n}$ , then go to step 1; otherwise stop.

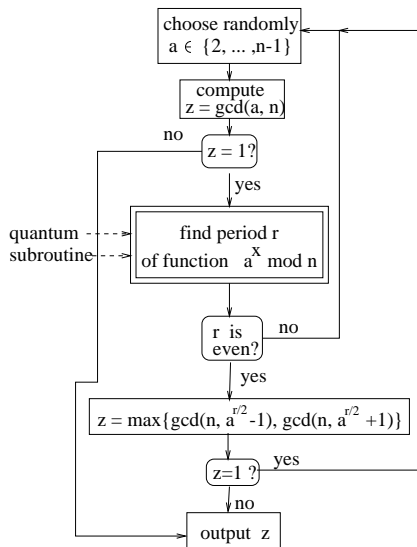
**Corollary** If there is a polynomial time randomized [quantum] algorithm to compute the period of the function

$$f_{n,a}(k) = a^k \bmod n,$$

then there is a polynomial time randomized [quantum] algorithm to find non-trivial solution of the equation  $a^2 \equiv 1 \pmod{n}$  (and therefore also to factorize integers).

# A GENERAL SCHEME for Shor's ALGORITHM

The following flow diagram shows the general scheme of Shor's quantum factorization algorithm



# SHOR'S QUANTUM FACTORIZATION ALGORITHM I.

- 1 For given  $n, q = 2^d, a$  create states

$$\frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |n, a, q, x, \mathbf{0}\rangle \text{ and } \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |n, a, q, x, a^x \bmod n\rangle$$

- 2 By measuring the last register the state collapses into the state

$$\frac{1}{\sqrt{A+1}} \sum_{j=0}^A |n, a, q, jr + l, y\rangle \text{ or, shortly } \frac{1}{\sqrt{A+1}} \sum_{j=0}^A |jr + l\rangle,$$

where  $A$  is the largest integer such that  $l + Ar \leq q$ ,  $r$  is the period of  $a^x \bmod n$  and  $l$  is the offset.

$$\sqrt{\frac{r}{q}} \sum_{j=0}^{\frac{q}{r}-1} |jr + l\rangle$$

- 3 By applying quantum Fourier transformation we get then the state

$$\frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{2\pi i j l / r} |j \cdot \frac{q}{r}\rangle.$$

- 4 By measuring the resulting state we get  $c = \frac{jq}{r}$  and if  $\gcd(j, r) = 1$ , what is very likely, then from  $c$  and  $q$  we can determine the period  $r$ .

Indeed, since

$$c = \frac{jq}{r}$$

for randomly chosen  $j$  and still unknown period  $r$  and very likely  $\gcd(j, r) = 1$   
we have

$$\frac{c}{j} = \frac{q}{r}$$

and therefore

$$r = \frac{q}{\gcd(c, q)}$$