15. QUANTUM CRYPTOGRAPHY

An important new feauture of quantum cryptography is that security of key generation is based on the laws of nature and not on the unproven assumptions of computational complexity theory.

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

Three main outcomes

- It has been proven that unconditionally secure quantum key generation is possible (in the sense that each eavesdropping is detectable).
- Unconditionally secure basic quantum cryptographic protocols are impossible.
- Quantum cryptography is already in advanced experimental stage.

Before presenting basic schemes of quantum cryptoraphy basic ideas of quantum information procesing will be discussed shortly.

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

is in the way information is stored and processed.

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

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

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

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

where α, β are arbitrary complex numbers such that

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

CLASSICAL EXPERIMENTS

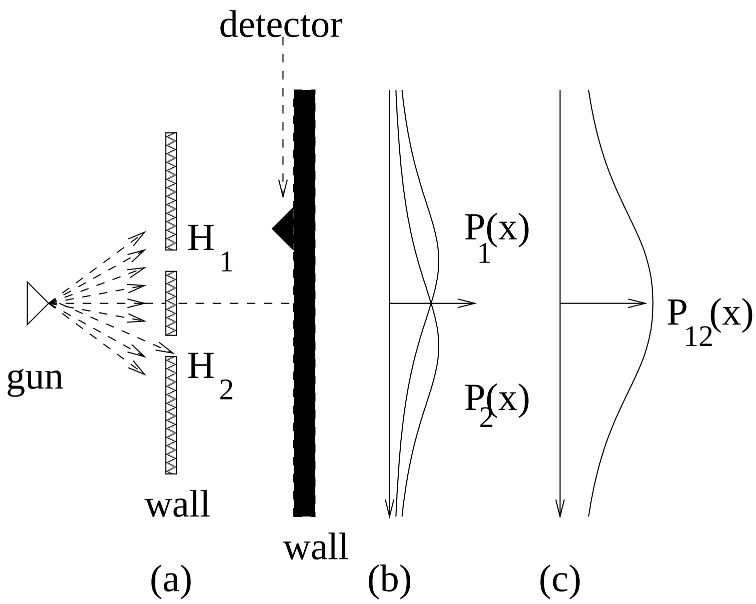


Figure 1: Experiment with bullets

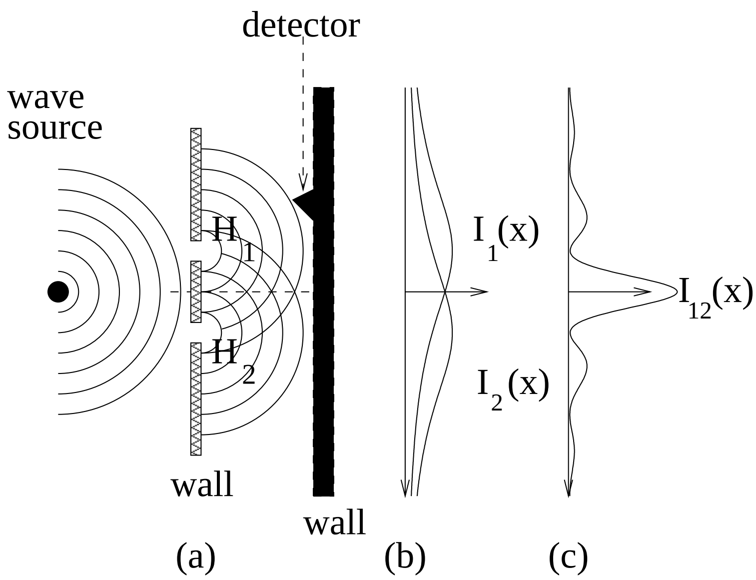


Figure 2: Experiments with waves

QUANTUM EXPERIMENTS

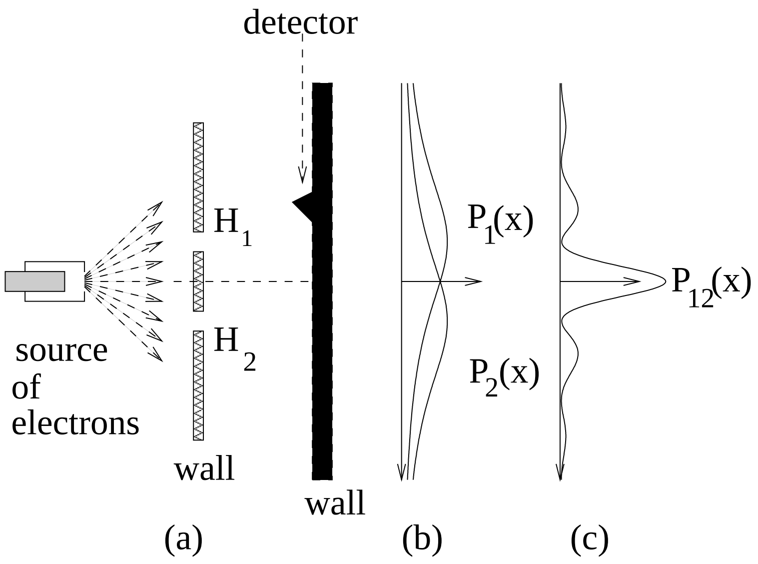


Figure 3: Two-slit experiment

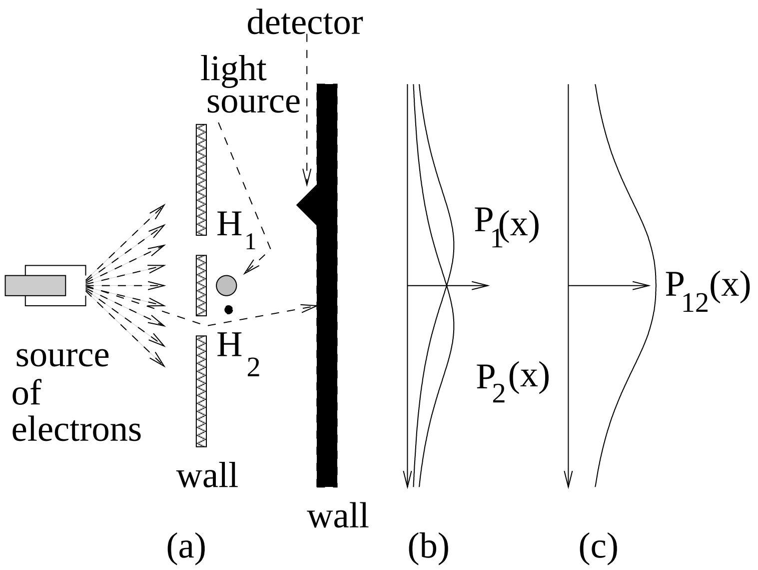


Figure 4: Two-slit experiment with an observation

THREE BASIC PRINCIPLES

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

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

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

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

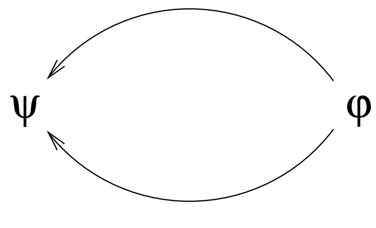
is the **probability** of the transfer.

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

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

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

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



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

QUANTUM SYSTEMS

=

HILBERT SPACE

Hilbert space H_n is n-dimensional complex vector space with

scalar product

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

norm of vectors

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

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

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

Given a basis B, any vector $|\psi\rangle$ from H_n can be uniquelly expressed in the form

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

$\boxed{\text{BRA-KET NOTATION}}$

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

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

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

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

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

QUANTUM EVOLUTION/COMPUTATION

EVOLUTION	COMPUTATION
in	in
QUANTUM SYSTEM	HILBERT SPACE

is described by

Schrödinger linear equation

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

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

$$A|\psi\rangle$$

A matrix A is **unitary** if

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

QUANTUM (PROJECTION) MEASUREMENTS

A quantum state is observed (measured) with respect to an **observable** — a decomposition of a given Hilbert space into orthogonal subspaces (such that 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 $|\phi\rangle$:

1. Information into which subspace projection of $|\phi\rangle$ was made.
2. Resulting projection (a new state) $|\phi'\rangle$.

The subspace into which projection is made is chosen **randomly** and the corresponding probability is uniquely determined by the amplitudes at the representation of $|\phi\rangle$ at the basis states of the subspace.

QUBITS

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

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

where $\alpha, \beta \in \mathbf{C}$ are such that $|\alpha|^2 + |\beta|^2 = 1$ and

$\{|0\rangle, |1\rangle\}$ is a **(standard) basis** of H_2

EXAMPLE: Representation of qubits by

(a) electron in a Hydrogen atom

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

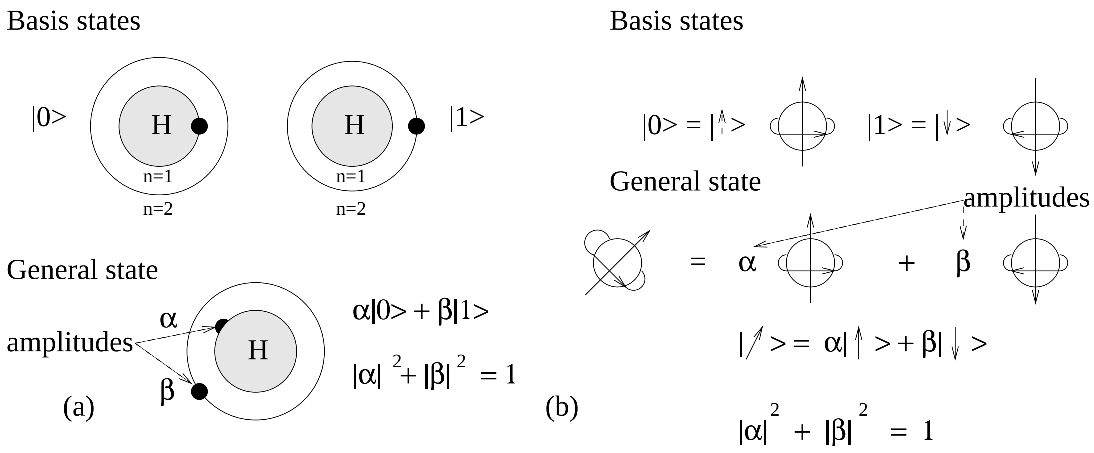


Figure 5: Qubit representations by energy levels of an electron in a hydrogen atom and by a spin-$\frac{1}{2}$ particle. The condition $|\alpha|^2 + |\beta|^2 = 1$ is a legal one if $|\alpha|^2$ and $|\beta|^2$ are to be the probabilities of being in one of two basis states (of electrons or photons).

HILBERT SPACE H_2

STANDARD BASIS | **DUAL BASIS**

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

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad\qquad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Hadamard matrix

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

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

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

transforms
one of the basis into another one.

General form of a unitary matrix of degree 2

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

QUANTUM MEASUREMENT

of a qubit state

A qubit state can "contain" unboundly large amount of information. However, **a quantum state cannot be identified**.

By a **measurement** of the qubit state

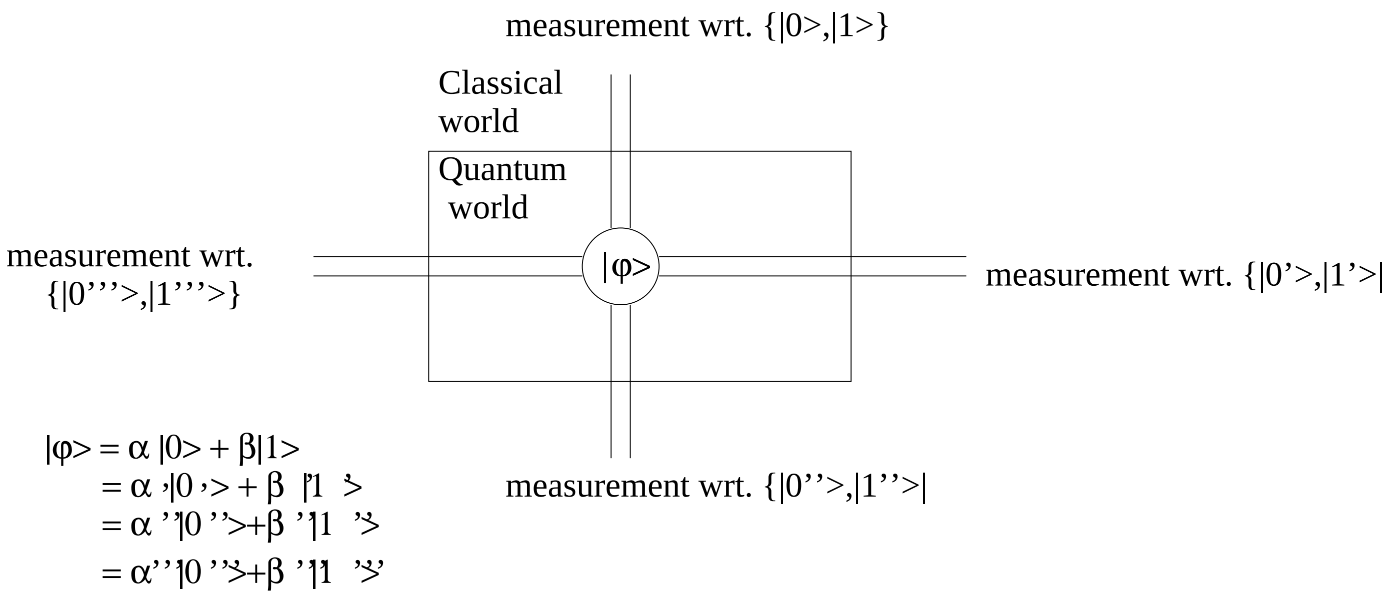
$$\alpha|0\rangle + \beta|1\rangle$$

with respect to the basis

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

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

$$0 \text{ with probability } |\alpha|^2$$
$$1 \text{ with probability } |\beta|^2$$



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:

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

QUANTUM MEASUREMENT

of the states of 2-qubit registers

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

1. Measurement with respect to the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

   RESULTS:

$$\begin{array}{ll} 00 & \text{with probability} \quad |\alpha_{00}|^2 \\ 01 & \text{with probability} \quad |\alpha_{01}|^2 \\ 10 & \text{with probability} \quad |\alpha_{10}|^2 \\ 11 & \text{with probability} \quad |\alpha_{11}|^2 \end{array}$$

2. Measurement of particular qubits:

   By measuring the first qubit we get

$$0 \;\; \text{with probability} \quad |\alpha_{00}|^2 + |\alpha_{01}|^2$$

$$\text{and} \quad |\phi\rangle \quad \text{is reduced to the vector} \quad \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

$$1 \; \text{with probability} \quad |\alpha_{10}|^2| + |\alpha_{11}|^2$$

$$\text{and} \quad |\phi\rangle \quad \text{is reduced to the vector} \quad \frac{\alpha_{10}|10\rangle + \alpha_{11}|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}$$

NO-CLONING THEOREM

INFORMAL VERSION: Unknown quantum state cannot be cloned.

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

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

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

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

Let

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

Then

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

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

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

BELL STATES

States

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

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

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

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

QUANTUM n-qubit REGISTER

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

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

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

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

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

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

is used then

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

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

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

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

QUANTUM PARALLELISM

If

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

then the mapping

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

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

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

Let

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

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

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

IN A SINGLE COMPUTATIONAL STEP 2^n VALUES OF f ARE COMPUTED!

IN WHAT LIES POWER OF QUANTUM COMPUTING?

In quantum interference or in quantum parallelism?

OR

in QUANTUM ENTANGLEMENT?

Let

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

be a (global) state of two
nterlinevery distant particles,
for example
on two planets

CLASSICAL versus QUANTUM CRYPTOGRAPHY

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

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

- Since classical cryptography is volnurable 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 agains 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 achievments 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 development stage.

POLARIZATION of PHOTONS

Mainly polarized photons are currently used for experimental quantum key generation. This is why polarization of photons will now be dealt with in more details.

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.

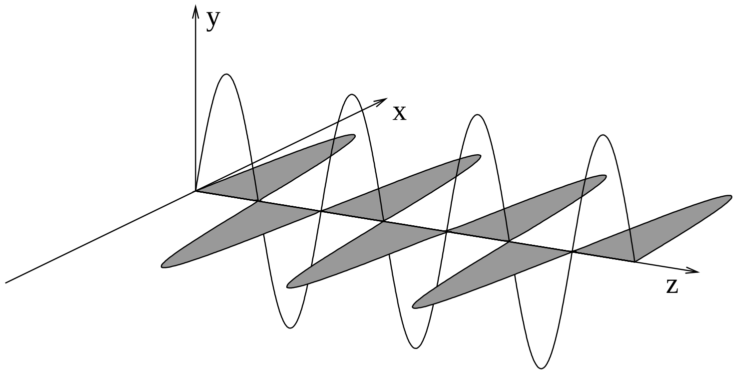


Figure 6: Electric and magnetic fields of a linearly polarized photon

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

If the electric field vector rotates about the direction of propagation forming a (right-) left-handed screw, we have (right) left **eliptic polarization** .

If the rotating electric field vector inscribes a circle, we have (right) left **circular polarization**.

PHOTON POLARIZERS

There is no way to determine exactly polarization of a single photon.

However, for any angle θ there are θ-**polarizers**—"filters"—that produce θ-polarized photons from an incoming stream of photons and they let θ_1-polarized photons to get through with probability $\cos^2(\theta - \theta_1)$.

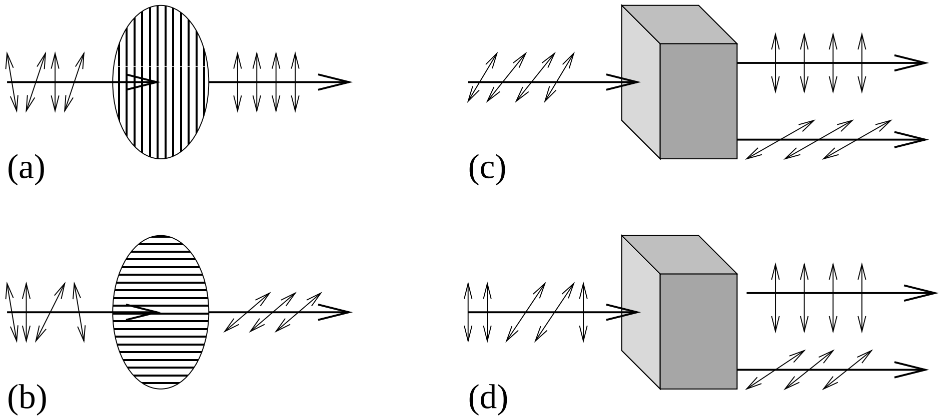


Figure 7: Photon polarizers and measuring devices-80%

Photons whose electronic fields oscillate in a plane at either $0°$ or $90°$ to some reference line are called usually **rectilinearly polarized** and those whose electric field oscillates in a plane at $45°$ or $135°$ as **diagonally polarized**. Polarizers that produce only vertically or horizontally polarized photons are depicted in Figure 7a,b.

Generation of orthogonally polarized photons.

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

Fig. c — a calcite crystal that makes θ-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 KEY GENERATION – PROLOGUE

Quantum cryptography is, similarly as classical cryptography, a continuous fight between good and bad.

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: Alice prepares a quantum system in a specific way, unknown to the eavesdropper, Eve, and sends it to Bob.

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 $|\phi_1\rangle, \ldots, |\phi_n\rangle$ that **are not** mutually orthonormal and that p_i is the probability that $|\psi\rangle = |\phi_i\rangle$.

TRANSMISSION ERRORS

If Alice sends randomly chosen bit

$$0 \text{ encoded randomly as } |0\rangle \text{ or } |0'\rangle$$

or

$$1 \text{ encoded as randomly as } |1\rangle \text{ or } |1'\rangle$$

and Bob measures the encoded bit by choosing randomly the stadard or the dual basis, then the probability of error is $\frac{1}{4}$

If Eve measures the encoded bit, sent by Alice, according to the randomly chosen basis, standard or dual, then she can learn the bit sent with the probability 75%.

If she then sends the state obtained after the measurement to Bob and he measures it with respect to the standard or dual basis, randomly chosen, then the probability of error for his measurement is $\frac{3}{8}$ – a 50% increase with respect to the case there was no eavesdropping.

Indeed the error is

$$\frac{1}{2} \cdot \frac{1}{4} + \frac{1}{2}\left(\frac{1}{2} \cdot \frac{1}{4} + \frac{1}{2} \cdot \frac{3}{4}\right)$$

BB84 QUANTUM KEY GENERATION PROTOCOL

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

Preparation phase

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

Quantum transmission

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

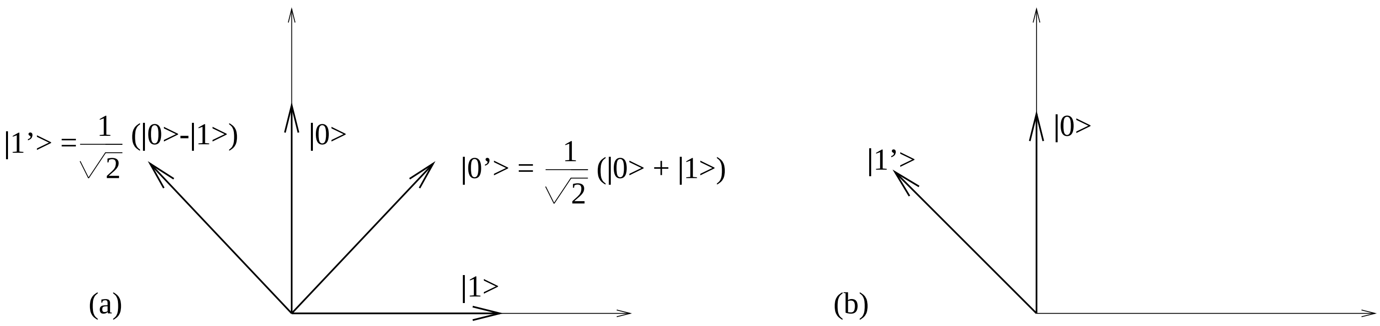


Figure 8: Polarizations of photons for BB84 and B92 protocols

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

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

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

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

Transmissions

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

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

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

Figure 9: Quantum cryptography with BB84 protocol

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

An example of an encoding–decoding process is in the Figure 11.

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

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

Raw key extraction

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

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

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

Test for evesdropping

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

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

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

Error correction phase

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

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

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

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

Privacy amplification phase

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

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

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

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

EXPERIMENTAL CRYPTOGRAPHY

Successes

1. Transmissions using optical fibre to the distance of 47 km.
2. Open air transmissions to the distance 1.6 km at day time (2-7 km experiments are going on)
3. Next goal: earth to satelite transmissions

EXPERIMENTAL CRYPTOGRAPHY

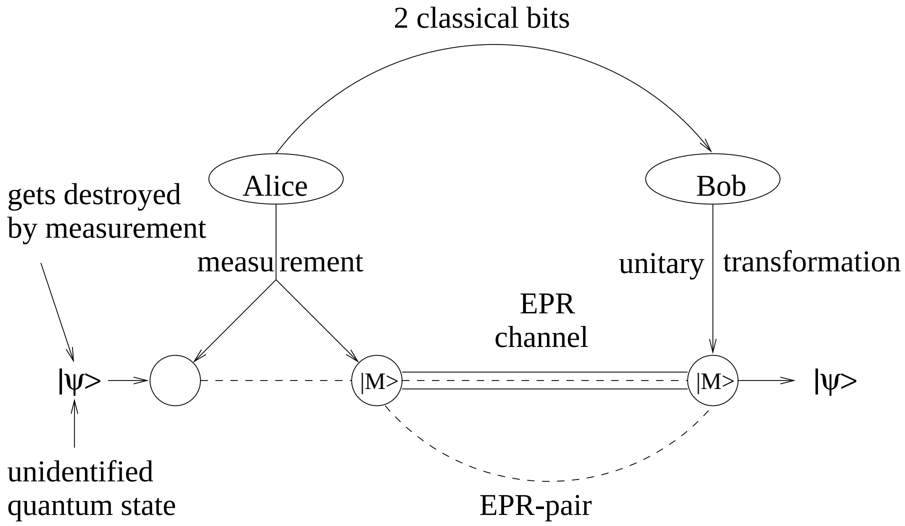
All current systems use optical means for quantum state transmissions

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 fibre. (Current error rates: $0,5 - 4\%$)
3. To move from the experimental to the developmental stage.

QUANTUM TELEPORTATION

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



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |EPR-pair\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Total state

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

Measurement of the first two qubits is done with respect to the "Bell basis":

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

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

QUANTUM TELEPORTATION I

Total state of three particles:

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

can be expressed as follows:

$$\begin{aligned}|\psi\rangle|EPR - state\rangle \;=\; & |\Phi^{+}\rangle\frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle) + |\Psi^{+}\rangle\frac{1}{\sqrt{2}}(\beta|0\rangle + \alpha|1\rangle) \\ & +|\Phi^{-}\rangle\frac{1}{\sqrt{2}}(\alpha|0\rangle - \beta|1\rangle) + |\Psi^{-}\rangle\frac{1}{\sqrt{2}}(-\beta|0\rangle + \alpha|1\rangle))\end{aligned}$$

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

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 measuremnt provides two bits specifying which of the above four operations should be applied.

These four bits Alce needs to send to Bob using a classical channel (by email, for example).

QUANTUM TELEPORTATION II

If the first two particles of the state

$$\begin{aligned}|\psi\rangle|EPR-state\rangle &= |\Phi^+\rangle\frac{1}{\sqrt{2}}(\alpha|0\rangle+\beta|1\rangle)+|\Psi^+\rangle\frac{1}{\sqrt{2}}(\beta|0\rangle+\alpha|1\rangle)\\ &\quad +|\Phi^-\rangle\frac{1}{\sqrt{2}}(\alpha|0\rangle-\beta|1\rangle)+|\Psi^-\rangle\frac{1}{\sqrt{2}}(-\beta|0\rangle+\alpha|1\rangle))\end{aligned}$$

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

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

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

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

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
  classical information - transmitted through a classical cahnnel
- In a quantum teleportation an unknown quantum state $|\phi\rangle$ can be disambled into, and later reconstructed from, two classical bit-states and an maximally entangled pure quantum state.
- Using quantum teleporattion an unknown quantum state can be *teleported* from one place to another by a sender who does not need to know — for teleporattion itslelf — neither the state to be teleported nor the location of the intended receiver.
- The teleportation procedure cannnot be used to transmit information faster than light

  but

  it can be argued that quantum information presented in unknown state is transmitted instanteneously (except two random bits to be transmitted at the speed of light at most).
- EPR channel is irreversibly destroyed during the teleporation process.