QUANTUM COMPUTING 9

Jozef Gruska

Faculty of Informatics
Brno
Czech Republic

December 13, 2018

9.QUANTUM CRYPTOGRAPHY

Quantum cryptography is the area of science and engineering how one can use quantum phenomena for achieving cryptographic tasks with better security that classical cryptography can do.

From practical point of view, quantum cryptography is in advance developmental and demonstration state.

The last big achievements is that of Chinese scientists and engineers who achieved sending quantum particles from a satellite to a ground station separated 1200 km.

The above result is of a key importance for establishing ultrasecure communication networks and, eventually, a space-based quantum internet.

Chinese scientists and engineers also used their satellite-ground station communiction to demonstrate quantum entanglement for the distance 1200 km.

PROLOGUE

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

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

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

Experimentally, secure quantum key distribution has been tested, first time in 1985 for distance 32.5 cm and later, but before 2016, using polarization or phase of photons, for distance up to 150 (200)-500 km using standard optical fibres and for the distance up to 144 km in open air (from Canary island to Tenerife). Earth-to-satellite quantum bit transmissions are considered as feasible. Quantum cryptography is therefore in the advanced experimental and development stage.

FUNDAMENTAL DIFFERENCES

between classical and quantum cryptography

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

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

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

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

CLASSICAL CRYPTOGRAPHY — ELEMENTS

Classical cryptography has four main important components:

- Secret-key cryptosystems:

  CESAR, HILL, VIGENERE, AFFINE, TRANSPOSITION¡...

  DES, AES.

- Public key cryptosystems:

  RSA, ElGamal, knapsack, and elliptic curves,

- Digital signatures

- Cryptographic protocols.

  Coin-tossing, bit commitment, oblivious transfer,...

  Authentication, voting, ...

CLASSICAL CRYPTOGRAPHY — EXAMPLE

$$e(k, w) = c \qquad\qquad d(k, c) = w$$

encoding algorithm, key, plaintext, cryptotext; decoding algorithm

EXAMPLE

ONE-TIME PAD cryptosystem

$$e(k, w) = k \oplus w = c \qquad d(k, c) = k \oplus c = w$$

A secret-key cryptosystem is so much secure how much secure is key distribution, provided each time different random key is used.

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 successes of the experimental quantum information processing research.

It is believed and hoped that it will be

quantum key generation (QKG)

where one can expect the first

transfer from experimental to developmental stage.

POLARIZATION of PHOTONS - I.

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

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 he rope as 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 from side to side is set up. If this way moves a light beam, it is called "horizontally polarized".

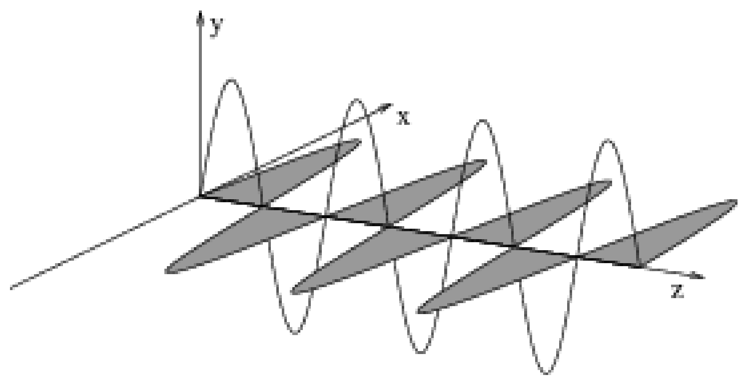


Figure 1: Vertically and horizontally polarized photons

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

CIRCULAR POLARIZATION

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".

PHOTON POLARIZERS

There is no way to determine exactly the 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 $\cos^2(\theta - \theta_1)$.

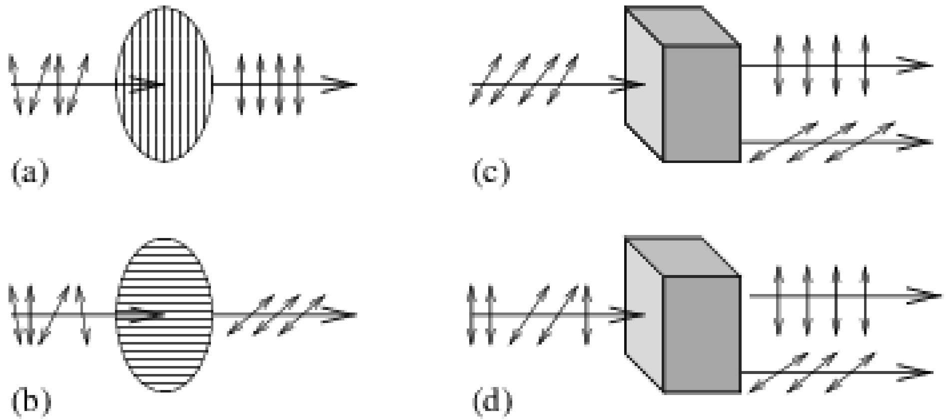


Figure 2: Photon polarizers and measuring devices

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 ??a,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.

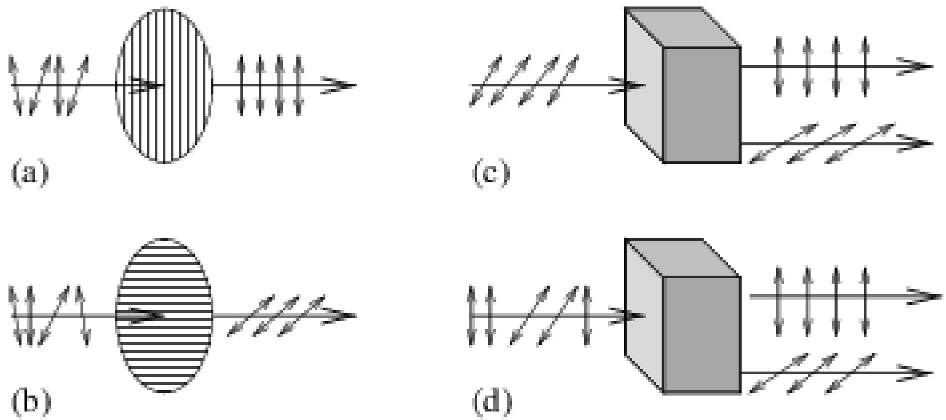


Figure 3: Photon polarizers and measuring devices

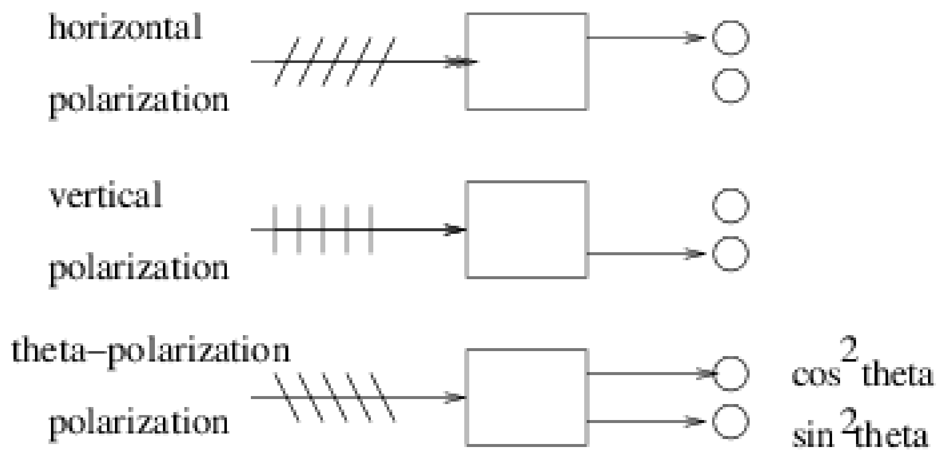


Figure 4: Example concerning polarization of photons

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 does it cost 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 INCREASE due to EAVESDROPER

If Alice sends randomly chosen bit

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

or

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

and Bob measures the encoded bit by choosing randomly the standard 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

$$\frac{1}{2}\cdot\frac{1}{4}+\frac{1}{2}\left(\frac{1}{2}\cdot\frac{1}{4}+\frac{1}{2}\cdot\frac{3}{4}\right)=\frac{3}{8}$$

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

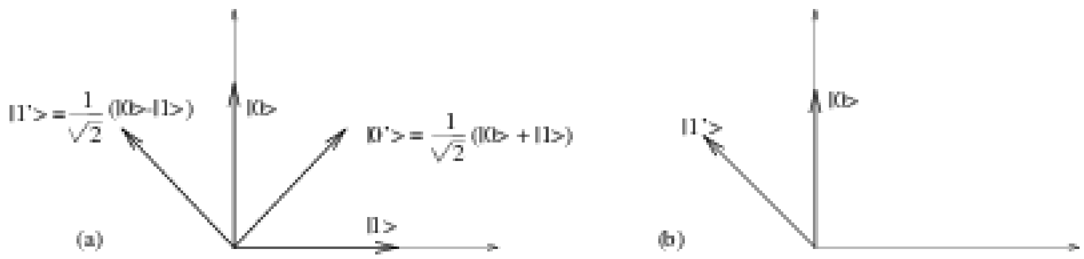


Figure 5: Polarizations of photons for BB84 and B92 protocols

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.

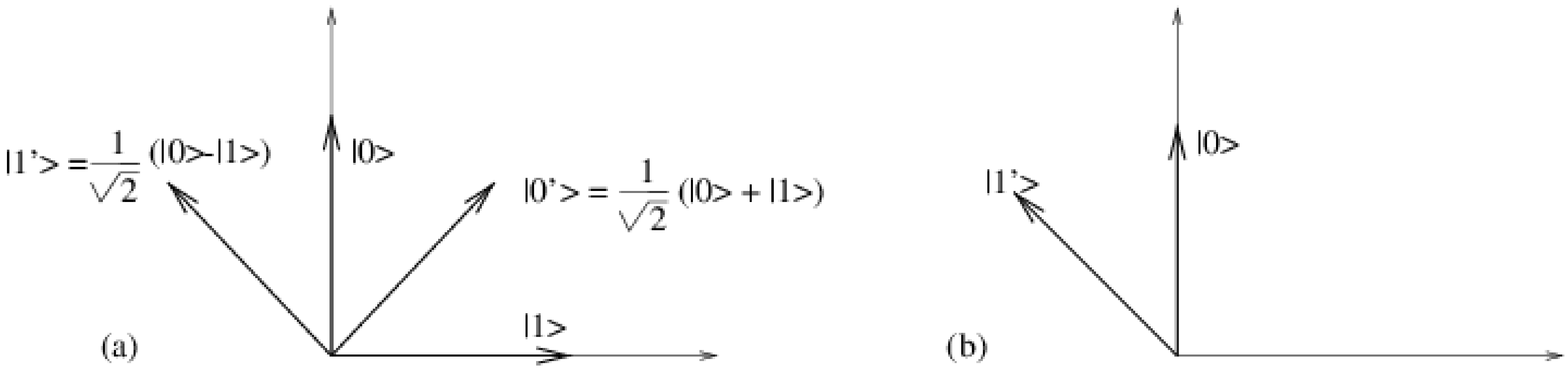


Figure 6: Polarizations of photons for BB84 and B92 protocols

Transmissions

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

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

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

Figure 7: Quantum cryptography with BB84 protocol

Figure 7 shows the possible results of the measurements and their probabilities.

An example of an encoding–decoding process is in the Figure 9.

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

Figure 8: Quantum transmissions in the BB84 protocol—R stands for the case that the result of the measurement is random

Raw key extraction and tests

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

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

Figure 9: 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.

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 chosen 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.

B92 PROTOCOL

A simpler protocol for quantum key generation, called B92, has been developed by Ch. Bennett in 1992.

Protocol: Alice uses for encoding of randomly chosen bit-sequence some two non-orthogonal states and encoding is deterministic. Bob uses for decoding/measurement two noncommutative measurements.

Example of an encoding/decoding procedure

Alice's bit	Alice's encoding	Bob's bit	Bob's test for	Test's result and probability	Correctness
0	$\|0\rangle$	0	$\|0'\rangle$	Yes/No (prob. $\frac{1}{2}$)	random
		1	$\|1\rangle$	No (prob. 1)	correct
1	$\|1'\rangle$	0	$\|0'\rangle$	No (prob. 1)	correct
		1	$\|1\rangle$	Yes/No (prob. $\frac{1}{2}$)	random

Figure 10: Encodings/decodings with B92 protocol

Example

1	0	0	0	1	1	0	0	0	1	1	Alice's random seq.
$\|1'\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1'\rangle$	$\|1'\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1'\rangle$	$\|1'\rangle$	Alice's polarizations
1	0	0	0	1	0	0	1	1	0	1	Bob's random sequence
$\|0'\rangle$	$\|0'\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0'\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0'\rangle$	$\|0'\rangle$	$\|1\rangle$	$\|0'\rangle$	Bob's test for
No	R	No	No	No	R	No	R	R	R	No	outcomes of test
1	R	0	0	1	R	0	R	R	R	1	resulting Bob's bit

Figure 11: Quantum transmissions within B92 protocol

B92 protocol is also called *minimal QKG protocol*.

SECURITY of B92 PROTOCOL

We show that Eve with an undetectable probe cannot obtain any information from B92 protocol.

Let $|\phi\rangle$ and $|\psi\rangle$ be two non-orthogonal states used in B92 protocol. Thus

$$\langle\phi|\psi\rangle \neq 0$$

and let U be the unitary performed by Eve's detection probe, to be initially in state $|\Psi\rangle$.

Since Eve's probe is undetectable, we have

$$|\Psi\rangle|\phi\rangle \rightarrow U|\Psi\rangle|\phi\rangle = |\Psi'\rangle|\phi\rangle$$

and

$$|\Psi\rangle|\psi\rangle \rightarrow U|\Psi\rangle|\psi\rangle = |\Psi''\rangle|\psi\rangle$$

where $|\Psi'\rangle$ and $|\Psi''\rangle$ denote the states of Eve's probe after the detection of $|\phi\rangle$ and $|\psi\rangle$, respectively.

Note that since Eve is undetectable her probe has no effect on the states $|\phi\rangle$ and $|\psi\rangle$.

Therefore $|\phi\rangle$ appears on both sides of the first equation above and $|\psi\rangle$ appears on both sides of the second equation.

Thus

$$\langle\langle\phi|\langle\Psi|U^*|U|\Psi\rangle|\psi\rangle\rangle = \langle\phi|\langle\Psi|\Psi\rangle|\psi\rangle = \langle\phi|\psi\rangle$$

because of the unitarity of U and because $\langle\Psi|\Psi\rangle = 1$

In addition to

$$\langle\langle\phi|\langle\Psi|U^*|U|\Psi\rangle|\psi\rangle\rangle = \langle\phi|\langle\Psi|\Psi\rangle|\psi\rangle = \langle\phi|\psi\rangle$$

we have

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

As the result we have

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

However,

$$\langle\phi|\psi\rangle \neq 0$$

implies that

$$\langle\Psi'|\Psi''\rangle = 1.$$

since $|\Psi'\rangle$ and $|\Psi''\rangle$ are normalized, this implies

$$|\Psi'\rangle = |\Psi''\rangle.$$

This implies that Eve's probe is in the same state no matter which of the states $|\phi\rangle$ and $|\psi\rangle$ is received.

Thus Eve obtains no information whatsoever.

ANOTHER VERSION of B92 PROTOCOL

- Alice keeps sending n times a quantum system in one of two randomly chosen given non-orthogonal states $|\phi\rangle$ or $|\psi\rangle$.
- Bob measures the received system randomly either in $\{|\phi\rangle, |\phi^{\perp}\rangle\}$ basis or in $\{|\psi\rangle, |\psi^{\perp}\rangle\}$ basis.
- Bob let Alice to know in which cases he got 100% clear outcome (if measurement outcomes is $|\phi^{\perp}\rangle$ or $|\psi^{\perp}\rangle$) and they discard all other outcomes.
- The rest of the protocol is as before.

DRAWBACKS of B92 PROTOCOL

B92 protocol has the following serious drawbacks.

The eavesdropper may use so-called POVM measurement to get one of the results

$$|\phi\rangle, |\psi\rangle, \textit{don't know}$$

This means that an eavesdropper can be sure that when the result of measurement is $|\phi\rangle, |\psi\rangle$ then it corresponds to the state that was sent and therefore eavesdropping introduces no noise.

If the result of measurement is *don't know* then eavesdropping would introduce a noise. However, in this case the eavesdropper can discard the quantum system sent by Alice so that Bob receives nothing.

It is therefore of large importance to follow the number of missing quantum systems.

QUANTUM ATTACKS

Individual or intercept-resent attacks. Each quantum signal is first measured by Eve and then resent.

Coherent or **joint attacks**. Instead of measuring the particles while they are in transit from Alice to Bob, one–by–one, Eve regards all the transmitted particles as a single entity. She then couples this entity with a simple auxiliary system (ancilla), prepared in a special state, and creates the compound system. Afterwards, she sends the particles to Bob and keeps the ancilla.

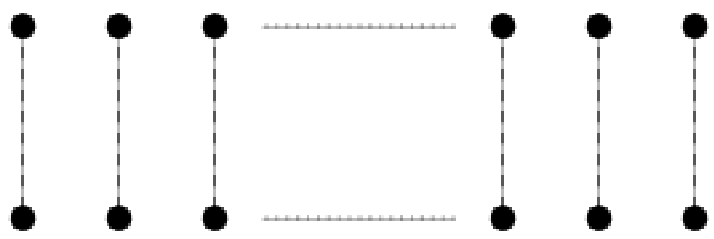
After the end of the public interactions between Alice and Bob (for error detection, error correction and privacy amplification), Eve extracts from her ancilla some information about the key. Such attack are directed against the final key. They represent the most general type of attacks that is possible. (However, no particular attack of this type has been suggested so far.)

Trojan horse attack. This refers to the possibility that an entanglement with environment can "open the door" and let a "Trojan horse to get in to gather information about quantum communications in the protocol"..

EPR METHOD for QUANTUM KEY GENERATION

Let Alice and Bob share n pairs of particles in the entangled state

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



n pairs of particles in EPR state

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

SHANNON THEOREMS

Shannon theorem says that n bits are necessary and sufficient to encrypt securely n bits.

Quantum version of Shannon theorem says that $2n$ classical bits are necessary and sufficient to encrypt securely n qubits.

EKERT's QKG PROTOCOL

Ekert developed a 3-state protocol that uses the so-called Bell's inequalities to detect the presence, or absence, of an eavesdropper (as a so-called hidden variable).

Example — in terms of photon polarizations.

A randomly chosen sequence of pairs of photons, in one of the following states

$$|\phi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\frac{3\pi}{6}\rangle - |\frac{3\pi}{6}\rangle|0\rangle)$$
$$|\phi_1\rangle = \frac{1}{\sqrt{2}}(|\frac{\pi}{6}\rangle|\frac{4\pi}{6}\rangle - |\frac{4\pi}{6}\rangle|\frac{\pi}{6}\rangle)$$
$$|\phi_2\rangle = \frac{1}{\sqrt{2}}(|\frac{2\pi}{6}\rangle|\frac{5\pi}{6}\rangle - |\frac{5\pi}{6}\rangle|\frac{2\pi}{6}\rangle)$$

is sent, by a moderator, to Alice and Bob, with one photon of each pair to Alice and second to Bob.

Both Alice and Bob measure their particles by randomly choosing one of the observable

$$\mathcal{O}_1 = \{|0\rangle, |\frac{3\pi}{6}\rangle\} \quad \mathcal{O}_2 = \{|\frac{\pi}{6}\rangle, |\frac{4\pi}{6}\rangle\} \quad \mathcal{O}_3 = \{|\frac{2\pi}{6}\rangle, |\frac{5\pi}{6}\rangle\}$$

and record bit-outcomes of the measurements.

Using a communication via a public channel they determine the cases they used the same measurement. The corresponding bits form the **raw key**.

The two remaining subsequences of bits , one at Alice another at Bob, form the so-called **rejected key** which is then used to detect eavesdropping, using the method discussed next.

BELL INEQUALITIES I.

A special type of Bell inequalities is a tool to detect the presence of an eavesdropper for the Ekert-type QKG protocols.

Einstein believed that quantum mechanics is incomplete and that using some *hidden variables* one could develop a complete quantum theory without nonlocal influences, where one could believe in the existence of an objective reality for quantum phenomena.

A Gedanken experiment suggested by Bell (1964) and the corresponding physical experiments by Aspen (1982), and many others, demonstrated that the above Einstein's idea does not work.

BELL INEQUALITIES II.

Let a pair of electrons in the EPR state is created and sent off in two directions. Let us have on each path (of the same length) a switch and two Stern-Gerlach magnets, set at different angles.

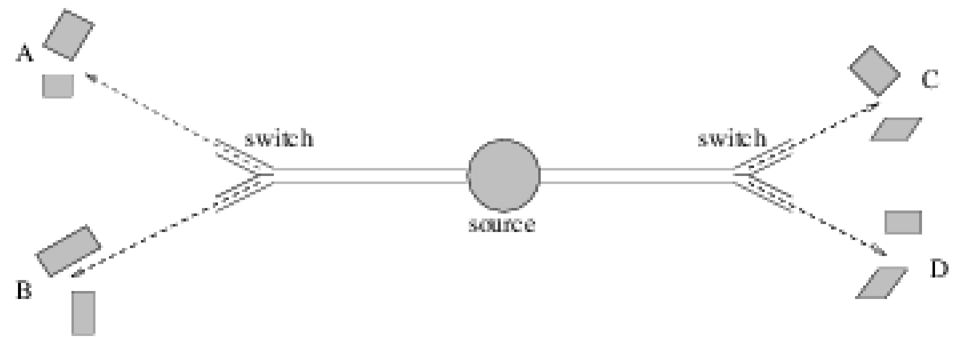


Figure 12: Aspect's experiment

For $Y \in \{A, B, C, D\}$ let $Y = 1$ or $Y = -1$ denote in which of two possible ways an electron gets out. At each particular experiment let one of the two variables A and B and one of C and D gets one of the values $1, -1$ and

$$X = C(A + B) + D(A - B)$$

can take on one of the values $2, -2$. Therefore, in case of many experiments

$$-2 \leq EX \leq 2.$$

Bell calculated that quantum mechanics theory implies that EX can be up to $2\sqrt{2}$ and Aspect's experiment, and many other experiments, confirmed Bell's expectations.

WHAT CAN a BAD EVE DO DURING EKERT's PROTOCOL?

Eve has no chance to get some information about the key from the particles while they are in transit because there is no information there.

Eve has two possibilities for destruction:

- To measure one, or both, of the particles on their way to Alice/Bob and this way to prevent Alice/Bob to share a common key.
- To substitute her own carefully prepared particles for those generated by the moderator from the source.

Bell's inequalities for the Ekert protocol

Denote by

$$Pr(\neq, i, j)$$

the probability that corresponding bits of Alice's and Bob's rejected sequences are different if Alice measures with observable $\mathcal{O}_i$ and Bob with observable $\mathcal{O}_j$. Moreover,

$$Pr(=, i, j) = 1 - Pr(\neq, i, j)$$

$$\Delta(i, j) = Pr(\neq, i, j) - Pr(=, i, j)$$

and

$$\beta = 1 + \Delta(2, 3) - |\Delta(1, 2) - \Delta(1, 3)|.$$

The Bell inequality for this protocol is $\beta \geq 0$ but quantum mechanics theory implies

$$\beta = -\frac{1}{2}$$

By measuring β one can therefore determine the presence or absence of an eavesdropping.

QUANTUM CRYPTOGRAPHIC PROTOCOLS

A variety of quantum cryptographic protocols have already been developed for basic cryptographic tasks. Some of them will now be presented.

The key issue is whether for basic cryptographic tasks there exist unconditionally secure quantum cryptographic protocols.

BASIC CLASSICAL CRYPTOGRAPIC PROTOCOLS

Cryptographic protocols are specifications how two parties, Alice and Bob, should prepare themselves for a communication and how they should behave during a communication in order to achieve their goal and be protected against an adversary.

In **coin-flipping protocols** Alice and Bob can flip a coin over a distance in such a way that neither of them can determine the outcome of the flip, but both can agree on the outcome in spite of the fact that they do not trust each other.

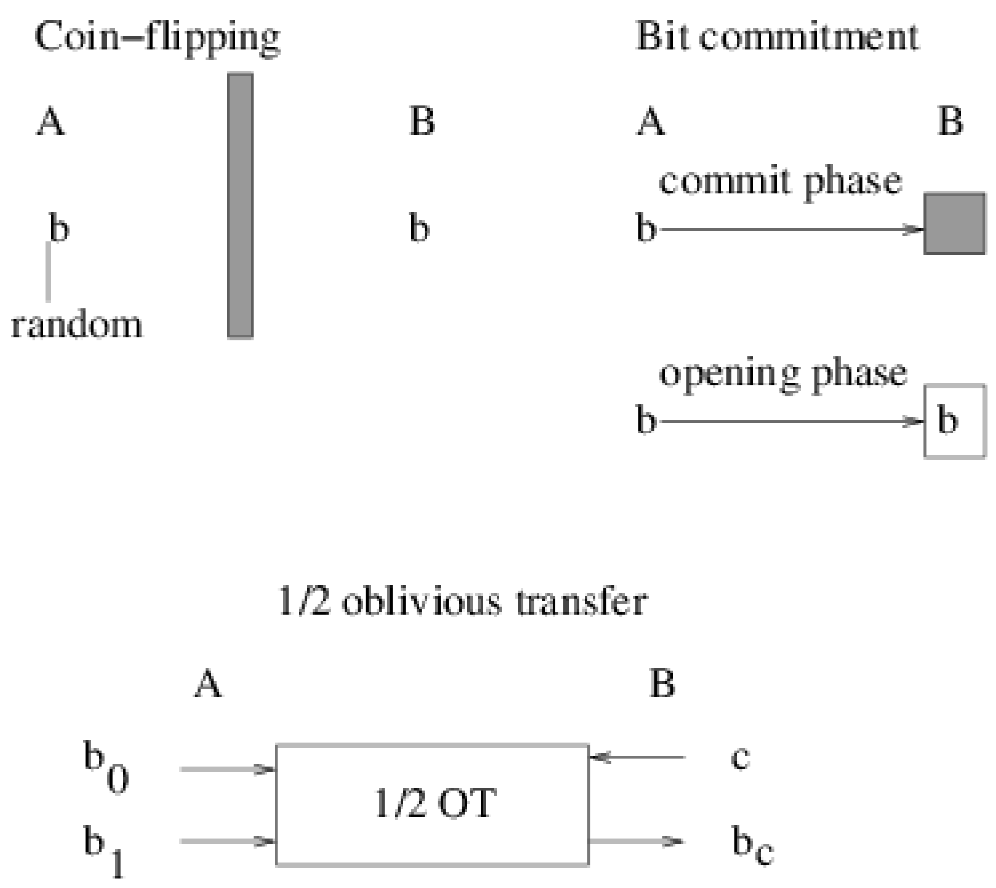
In **bit commitment protocols** Alice can choose a bit and get committed to it in the following sense: Bob has no way of learning Alice's commitment and Alice has no way of changing her commitment.

Alice commits herself to a bit x using a *commit*(x) procedure, and reveals her commitment, if needed, using *open*(x) procedure.

In **1-out-2 oblivious transfer protocols** Alice transmits two messages m_1 and m_2 to Bob who can chose whether to receive m_1 or m_2, but cannot learn both, and Alice has no idea which of them Bob has received.

In **standard oblivious transfer protocols** Alice can send a message to Bob in such a way that Bob receives the message with probability $\frac{1}{2}$ and a garbage with probability $\frac{1}{2}$. Moreover, at the end Bob knows whether he got a message or a garbage, but Alice has no idea which of them Bob has received.

PRIMITIVES of CRYPTOGRAPHIC PROTOCOLS



CLASSICAL COIN-FLIPPING (BY PHONE) PROTOCOL

The history of cryptographic protocols started with the following Blum's coin-flipping protocol (1981):

Protocol 0.1 (Coin-flipping by telephone)

1. *Alice chooses two large primes p, q, sends Bob $n = pq$, and keeps p, q secret.*
2. *Bob chooses a random number $y \in \{1, \ldots, \lfloor \frac{n}{2} \rfloor\}$ and sends Alice $x = y^2 \bmod n$.*
3. *Alice computes four square roots $(x_1, n - x_1)$ and $(x_2, n - x_2)$ of x. (Alice can compute them because she knows p and q.)*

   Let $x_1' = \min\{x_1, n - x_1\}$, $x_2' = \min\{x_2, n - x_2\}$. Since $y \in \{1, \ldots, \lfloor \frac{n}{2} \rfloor)\}$, either $y = x_1'$ or $y = x_2'$.

   Alice then guesses whether $y = x_1'$ or $y = x_2'$ and tells Bob her choice (for example, by reporting the position and the value of the leftmost bit in which x_1' and x_2' differ).
4. *Bob tells Alice whether her guess was correct (head) or not correct (tail).*

Later, if necessary, Alice can reveal p and q, and Bob can reveal y.

QUANTUM COIN-FLIPPING PROTOCOL

Alice's random bits	1	0	1	1	0	1	1	0	0	1	1
Alice polarization choice						rectilinear					
photons sent	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
Bob's observable	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$
Bob's table for $\mathcal{B}$	1			1			1		0	1	
Bob's table for $\mathcal{D}$		1	1					0			0
Bob's guess of Alice's pol.						rectilinear					
Alice's message						you WON					
Alice's original bits	1	0	1	1	0	1	1	0	0	1	1
comparison with $\mathcal{B}$	Y			Y			Y		Y	Y	
comparison with $\mathcal{D}$		N	Y					Y			N

Figure 13: Illustration of a quantum coin-flipping protocol

1. Alice randomly chooses a sequence of bits (for example 10110110011) and a polarization (rectilinear or diagonal—standard or dual). Finally, Alice sends the resulting sequence of the polarized photons to Bob.
2. Bob chooses, for each received photon, randomly, an observable, $\mathcal{B}$ or $\mathcal{D}$, and measures the incoming photon. He records the result into two tables—one for observable $\mathcal{B}$ and the second for observable $\mathcal{D}$. Since some photons can get lost during the transmissions, there can be holes in both tables. At the end of all transmissions, Bob makes a guess whether Alice choose rectilinear or diagonal polarization and announces his guess to Alice. He is to win if the guess is correct; to lose otherwise.
3. Alice tells Bob whether he won or lost by telling him the polarization she choose. She can certify her claim by sending Bob the random sequence of bits she choose at Step 1.
4. Bob verifies Alice's claim by comparing his records in the table for the basis she claims to choose. There should be a perfect agreement with the entries in that table and no perfect correlation with the other table.

Alice's random bits	1	0	1	1	0	1	1	0	0	1	1
Alice polarization choice					rectilinear						
photons sent	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
Bob's observable	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$
Bob's table for $\mathcal{B}$	1			1			1		0	1	
Bob's table for $\mathcal{D}$		1	1					0			0
Bob's guess of Alice's pol.					rectilinear						
Alice's message					you WON						
Alice's original bits	1	0	1	1	0	1	1	0	0	1	1
comparison with $\mathcal{B}$	Y			Y			Y		Y	Y	
comparison with $\mathcal{D}$		N	Y					Y			N

Figure 14: Illustration of a quantum coin-flipping protocol

CAN BOB OR ALICE CHEAT?

1. Bob is not able to cheat.

   Bob would be able to "cheat" only would he be able to guess with probability $> \frac{1}{2}$, on the base of photons he received, which basis (polarization) Alice has chosen (what contradicts physical laws).

2. Alice could potentially cheat only in Step 1 or in Step 3.

   - **Alice cannot cheat in Step 3**

     In order to cheat she would need to send sequence of bits matching the entries of Bob's table for two possible bases (polarization). The probability she keeps making correct guess about Bob's measurement goes fast to 0.

- **Alice CAN CHEAT at Step 1 by making a clever use of entanglement!**

In Step 1, instead of sending a sequence of isolated photons, polarized in one of two ways, she produces pairs of photons, each in the state

$$\frac{1}{2}(|01\rangle + |10\rangle),$$

she sends to Bob one photon of each pair and stores the other one.

After Bob's guess, in Step 2, she measures her photon in the opposite basis as was Bob's guess. By that she receives a sequence of bits perfectly correlated with Bob's table corresponding to the basis he did not choose as his guess in Step 2. Alice then announces her sequence in Step 3.

CLASSICAL BIT COMMITMENT with ONE-WAY FUNCTION

Commitment phase: • Alice and Bob choose a one-way function f;

- Bob sends a randomly chosen r_1 to Alice;
- Alice chooses a random r_2 and her committed bit b and sends to Bob $f(r_1, r_2, b)$.

Opening phase: • Alice sends to Bob r_2 and b;

- Bob computes $f(r_1, r_2, b)$ and compares with the value he has already received.

CLASSICAL BIT COMMITMENT with SYMMETRIC CIPHER

Commitment phase:
- Alice and Bob choose a symmetric cryptosystem with an encryption algorithm e_k;
- Bob sends Alice a randomly chosen string r;
- ALice chooses a random key k, a commitment b and sends to Bob $e_k(rb)$

Opening phase:
- Alice sends to Bob the key k;
- Bob performs decryption and verifies b and r.

Comment: The role of r chosen by Bob is to make unfeasible for Alice to find two keys k_1 and k_2 such that $e_{k_1}(r0) = e_{k_2}(r1)$.

BENNETT-BRASSARD QUANTUM BIT COMMITMENT

Commitment phase: Input to the bit b

- Alice chooses a random binary vector $\mathbf{r} = (r_1, \ldots, r_n)$.
- Bob chooses a random binary vector $\mathbf{s} = (s_1, \ldots, s_n)$
- **for** $i = 1$ **to** n Alice sends to Bob a quantum system in the state $H^b|r_i\rangle$.
- Bob measures the system he obtained in the basis $\{H^{s_i}|0\rangle, H^{s_i}|1\rangle\}$ and sets z_i to 0 (to 1) if the result of the measurement is $|0\rangle$ or $|0'\rangle$ (is $|1\rangle$ or $|1'\rangle$).

Opening phase

- Alice sends the commitment b and the vector $\mathbf{r}$ to Bob
- If there is an i such that $b = s_i$ and $r_i \neq z_i$, then Bob rejects; otherwise it accepts b as correct commitment.

Correctness of the Bennett-Brassard bit commitment protocol

Both, Bennett and Brassard, knew that their protocol is not unconditionally secure.

QUANTUM BIT COMMITMENT PROTOCOLS

In 1993, Brassard, Crépeau, Jozsa and Langlois develop a quantum bit commitment protocol, the so-called BCJL-protocol and provided a proof that it is unconditionally secure.

In 1995 a flaw in the proof of unconditional security of the BCJL-protocol was discovered.

In 1996 two proofs were given that there is no unconditionally secure quantum bit commitment protocol.

The point is that a variant of cheating strategy demonstrated for our quantum coin tossing protocol, a clever misuse of entanglement by Alice, can be always used, in a modified form.

The fact that there is no unconditionally secure quantum bit protocol can be seen as a bad news because bit commitment is a primitive on which many cryptographic protocols can be built.

BCJL — PROTOCOL

Let $\varepsilon > 0$ (be an upper bound on the error rate of the quantum channel being used).

Protocol 0.2 (commit (x))

1. Bob chooses a generator matrix G of a binary linear (n, k, d)-code C such that $\frac{d}{n} > 10\varepsilon$ and $\frac{k}{n} = 0.52$ and announces G to Alice.
2. Alice chooses:
   - 2.1. a random string r of length n and announces it to Bob;
   - 2.2. a random k-bit vector s, such that $r \cdot c = x$, where $c = sG$;
   - 2.3. a random sequence b of length n of the polarizations, $\mathcal{B}$ or $\mathcal{D}$, and sends to Bob the sequence c of bits through a sequence of n photons with the polarization of the ith photon $P_{b_i}(c_i)$, where $P_0(0) = 0^\circ$, $P_0(1) = 90^\circ$ and $P_1(0) = 45^\circ$, $P_1(1) = 135^\circ$.
3. Bob chooses a random string b' of n bits and measures the ith photon, containing encoding of c_i, according to the basis $M(b'_i)$, where $M(0) = \mathcal{B}$ and $M(1) = \mathcal{D}$. Let c' be the n-bit vector where c'_i is the result of the measurement of the ith photon.

Alice keeps the bit x and vectors c and b secret, until the opening takes place, and Bob keeps vectors b' and c' secret.

Protocol 0.3 (open (c, b, x, c', b'))

1. Alice sends vectors c, b and bit x to Bob.
2. Bob verifies that c is a codeword of C and computes $B = \Sigma_{\{i \mid b'_i = b_i\}} \frac{c_i \oplus c'_i}{n/2}$, in order to verify that the error rate is under the limit of those pairs of outgoing and measured bits that were polarized/measured by the same basis.
3. if $B < 1.4\varepsilon$ and $x = r \cdot c$, then Bob accepts, otherwise Bob rejects.

QUANTUM OBLIVIOUS TRANSFER PROTOCOLS I

It is easy to design a simple and perfectly secure QOTP provided transmissions and detectors are perfect and no party cheats.

Protocol 0.4 (Ideal one-photon standard QOTP)

1. Alice chooses a bit b and sends it to Bob through one photon encoded using a randomly chosen basis—standard or dual.
2. Bob measures the photon with respect to a randomly chosen basis—standard or dual.
3. Alice lets Bob know the basis she choose.

At the end Bob has a 50% chance to know b for sure and he knows whether he knows b for sure. Alice has no information whether Bob knows the bit for sure.

Problems with this protocol.

1. Imperfect devices (Alice's source, a noisy channel, or Bob's detector) could much affect the probability of success of Bob's measurement.

2. Bob could "cheat" by making his measurement in the so called Breidbart basis

$$\mathcal{B}_0 = \{\theta_0, \theta_1\},$$

where

$$\theta_0 = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle; \quad \theta_1 = -\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle$$

This way he could learn b with a larger probability - with probability $\cos^2\frac{\pi}{8} \approx 0.85$.

1-out-of-2 QOTP

Parameter agreeing phase

Alice and Bob find out, or agree during their communication, on the following parameters:

ε — the expected error rate of the communication channel;

α — the fraction of photons Bob is able to detect successfully;

n — the security parameter; number of photons to be transmitted;

C — a binary linear error-correcting code capable of correcting, well, n-bit words transmitted with the expected error rate ε.

Transmission phase

Alice chooses a random binary string of length $\frac{2n}{\alpha}$ and sends each of the bits through a polarized photon using randomly either the standard or dual polarization basis.

Measurement phase

Bob measures each incoming photon by a randomly chosen basis ($\mathcal{B}$ or $\mathcal{D}$) and records the basis chosen and the results of the measurements into tables.

Bob expects to receive $2n$ photons. If he gets more, he ignores additional bits. if less, he adds randomly chosen bits.

At the end of transmissions, Bob reports to Alice arrival times of all $2n$ photons, but neither the bases nor the results of his measurements.

Bases-revealing phase.

Alice tells Bob, through a public channel, the bases she used to encode her random sequence of bits during the transmission phase.

Design of good and bad sequences phase.

Bob partitions his $2n$ bits into two sequences, each of length n.

Into the “good” sequence he puts as much as possible of bits he obtained when he used the correct basis for measurements.

The “bad” sequence contains as much as possible of other bits.

Bob then tells Alice indices of bits of both sequences, but not which one is “good” and not which one ‘is “ bad”.

At this point Bob shares with Alice a binary word of his good sequence (with respect to an expected error rate not greater than ε). Concerning the bad sequence, Bob shares almost nothing with Alice.

Of course, the above process is not ideal. There can be errors introduced because that Bob did not use exactly n times correct basis for measurement . However, the number of errors introduced this way should be negligible.

Error-correction phase.

Using the code C, Alice computes syndromes of her words corresponding to the good and bad sequence of Bob, and sends syndromes to Bob, who uses them to perform error correction on his good and bad sequences.

Privacy amplification phase.

Alice chooses randomly two subsets of bits, one from her "good" and one from her "bad" sequence and computes their parities. She let Bob know the "addresses" of bits she chose, but not their values.

This way Bob can compute the parity of the corresponding subset of his good sequence, but he will have no idea about the parity Alice obtained for the subset of bits corresponding to his bad sequence. Alice knows that she has no idea which one Bob knows.

Let x_0, x_1 be the parity bits Alice knows and $\bar{c}$ be the parity bit Bob knows. At that point Bob knows whether $\bar{c} = x_0$ or $\bar{c} = x_1$.

Oblivious transfer phase for sending bits b_0 and b_1

1. Bob tells Alice whether or not $c = \bar{c}$ for c he chooses.
2. If $c = \bar{c}$, then Alice sends Bob bits $x_0 \oplus b_0$ and $x_1 \oplus b_1$, in this order. If $c \neq \bar{c}$, Alice sends Bob bits $x_0 \oplus b_1$ and $x_1 \oplus b_0$, again in the given order.
3. Bob computes b_c out of two bits he got from Alice.

QUANTUM NON-LOCALITY

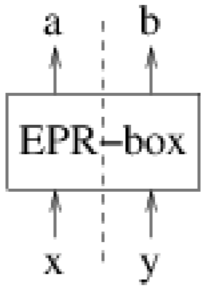
- Physics was non-local since Newton's time, with exception of the period 1915-1925.
- Newton has fully realized counterintuitive consequences of the non-locality his theory implied.
- Einstein has realized the non-locality quantum mechanics imply, but it does not seem that he realized that entanglement based non-locality does not violate no-signaling assumption.
- Recently, attempts started to study stronger non-signaling non-locality than the one quantum mechanics allows.

BEGINNINGS of MODERN STORY of NONLOCALITY

- In 1935 Einstein, Podolsky a Rosen (EPR) used entanglement to attack the validity of quantum physics as a complete theory of Nature.
- They defined an entangled state of two particles such that if a position (momentum) measurement was made on one of the particles, then position (momentum) of second particle was known.
- EPR concluded that position and momentum have to be *elements of reality*, i.e. they have to have predetermined values before measurements.
- If translated into mathematical formalism this means that Local Hidden Variable (LHV) model of Nature has to hold.
- In 1964 Bell showed that if the LHV model holds, then not all predictions of QM can be correct and he also showed a way how to test which model - LHV or QM -holds

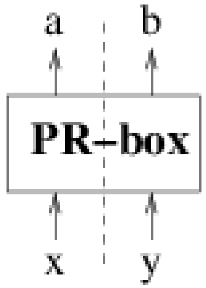
EPR-box versus RP-box

Non-locality exhibited by the measurement of the EPR state can be seen as the implementation of the following *EPR-box*



x = y implies a = b

Also non-locality exhibited by the following *PR-box* does not allow superluminal communication and therefore does not contradict special relativity.



x . y = (a + b) mod 2

However, it is unlikely that there is physical implementation of PR-boxes, as argued later.

MOTIVATION for PR-BOXES

The idea of PR-boxes arises in the following setting:

Let us have two parties, A and B, and let each of the parties $Z \in \{A, B\}$ performs two fully independent measurements on the same quantum state with two outcomes m_0^z and m_1^z (with 0 and 1 as potential values of each).

Let us denote a bound on correlations between two such measurements as

$$B = \sum_{x,y \in \{0,1\}} Prob(m_x^A \oplus m_y^B = x \cdot y).$$

So called Bell/CHCS inequality says that $B \leq 3$ in any classical (or hidden variable) theory.

So-called Cirel'son's bound (Cirel'son, 1980), says that the maximum for B in quantum mechanics is $2 + \sqrt{2}$.

Popescu and Rohrlich developed a model in which the maximal possible bound of B, that is 4, is achievable.

1/2-OT versus PR-boxes

The following important relations hold between 1/2-oblivious transfer and PR-boxes:

- From the security point of view PR-boxes and 1/2-oblivious transfer are equivalent.
- From the communication point of view, the following relations hold

$$\text{PR-box}+1 \text{ classical bit} \rightarrow 1/2\text{-OT} \rightarrow \text{PR-box}$$

- PR-box can be seen as a classical analogue of the EPR sate (and its measurement)
- 1/2-oblivious transfer can be seen as classical analogue of quantum channel (and projective measurement of the transmitted state)

LI/BARNUM's AUTHENTICATION PROTOCOL

Let Alice and Bob share n EPR states

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

and let Alice has another n EPR pairs

$$|\Phi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{12}$$

Protocol: For $1 \leq i \leq n$, the ith step of the protocol will be performed on ith copies of the states $|\Phi^+\rangle_{AB}$ and $|\Phi^+\rangle_{12}$.

- Alice performs CNOT with the qubit of $|\Phi^+\rangle_{12}$ as the control qubit and the qubit of $|\Phi^+\rangle_{AB}$ as the target qubit.
- Alice sends the state $|\Phi^+\rangle_{12}$ to Bob.
- Bob performs CNOT with second qubit of $|\Phi^+\rangle_{12}$ as control qubit and the qubit of $|\Phi^+\rangle_{AB}$ as the target qubit.
- Bob measures particles of $|\Phi^+\rangle_{AB}$ at the Bell basis. If the outcome is $|\Phi^+\rangle$, then the current authentication round succeeds.

Indeed, afer steps 1, 3 and 4 ,the overall states are:

$$|\Phi^+\rangle_{AB}|\Phi^+\rangle_{12} = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)_{AB12}$$

$$\frac{1}{2}(|0000\rangle + |1011\rangle + |1100\rangle + |0111\rangle)_{AB12};$$

$$\frac{1}{2}(|0000\rangle + |1111\rangle + |1100\rangle + |0011\rangle)_{AB12} = +|\Phi^+\rangle_{AB}|\Phi^+\rangle_{12}.$$

QUANTUM SECRET SHARING

There is a simple method how Alice can teleport a qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ (a secret), to Bob and Charles in such a way that they have to cooperate in order to have $|\phi\rangle$.

The basic idea is that Alice couples a given particle P in the state $|\phi\rangle$ with the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ of three particles P_a, P_b and P_c she shares with Bob and Charles and then performs a measurement on the state of particles P and P_a, with respect to the Bell basis $\{\Phi^{\pm}, \Psi^{\pm}\}$. Since

$$\begin{aligned}|\phi\rangle|\psi\rangle &= \frac{1}{2}(|\Phi^+\rangle(\alpha|00\rangle + \beta|11\rangle) + |\Phi^-\rangle(\alpha|00\rangle - \beta|11\rangle)\\ &+|\Psi^+\rangle(\beta|00\rangle + \alpha|11\rangle) + |\Psi^-\rangle(-\beta|00\rangle + \alpha|11\rangle)),\end{aligned}$$

the outcome of the measurement is that particles P_b and P_c get into one of the states

$$\frac{1}{\sqrt{2}}(\alpha|00\rangle + \beta|11\rangle), \frac{1}{\sqrt{2}}(\alpha|00\rangle - \beta|11\rangle), \frac{1}{\sqrt{2}}(\beta|00\rangle + \alpha|11\rangle), \frac{1}{\sqrt{2}}(-\beta|00\rangle + \alpha|11\rangle)$$

and Alice gets two bits to tell her about which of these four cases happened. However, neither Bob nor Charles has information about which of these four states their particles are in.

Bob now performs a measurement of his particle with respect to the dual basis. He gets out of it one bit of information and Charles's particle P_c gets into one of 8 possible states , which is uniquely determined by bits both Alice and Bob got as the results of their measurements , and which can be transformed into the state $|\phi\rangle$ using one or two applications of Pauli matrices.

EXTRA

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 $|p\rangle = |p_1\rangle \ldots |p_n\rangle$

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

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

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

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

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

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

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

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

FROM QUANTUM ONE-TIME PAD TO QUANTUM PRIVATE CHANNELS

A natural way to generalize one-time pad cryptosystem is that of **quantum private channel** – a synonym for a perfectly secure encryption by perfect randomization for sending messages through noiseless one-way quantum channel.

Basic scenario for a **quantum private channel (QPC)** is that:

- There are m possible keys - unitary matrices U_i, $i = 1, \ldots, m$, over n-qubits, and unitary U_i is chosen with probability p_i;
- Sending, by Alice, of a state $|\phi\rangle$, from a set $\mathcal{S}$ of states, amounts to multiplying at first $|\phi\rangle$ with a randomly chosen U_i and then sending the resulting state;
- Decoding is done by selecting, using shared randomness, and then applying the inverse unitary $U_i^\dagger$;
- Such a protocol is perfectly secure if for all states $|\phi\rangle$ it holds

$$\sum_{i=1}^{m} p_i U_i |\phi\rangle\langle\phi| U_i^\dagger = \frac{1}{2^n}\mathbf{I}_{2^n}. \quad (1)$$

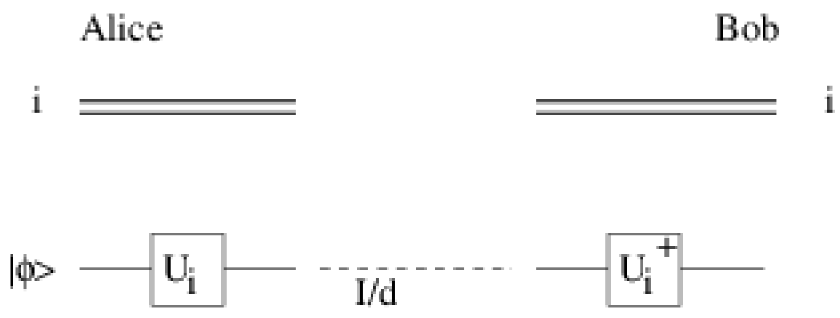


Figure 15: A quantum private channel based on randomization

- If this is the case, we say that the probability distribution $\{(p_i, U_i)\}_i$ specifies a private quantum channel.

Indeed, if (1) is satisfied, then an eavesdropper cannot learn anything about the state being sent.

GENERAL CASE

General case is that the sender/Alice first attaches an ancilla ρ_a to the state $|\phi\rangle\langle\phi|$ to be sent and then randomizes the composed state.

In addition, one should consider also the cases that only states from a special set of states are being transmitted. This leads to the following definition (Mosca et al. 2000):

Definition 0.5 *Let $\mathcal{S}$ be a set of n-qubit states, $\mathcal{E} = \{\sqrt{p_i}U_i \,|\, 1 \leq i \leq k\}$ be a superoperator with U_i being unitaries on an $m \geq n$ qubit register, $\Sigma_{i=1}^{k} p_i = 1$, and ρ_a be an $(m-n)$-qubit density matrix. $[\mathcal{S}, \mathcal{E}, \rho_a, \rho_0]$ specifies a* private quantum channel *if and only if for all $|\phi\rangle \in \mathcal{S}$ it holds*

$$\mathcal{E}(|\phi\rangle\langle\phi| \otimes \rho_a) = \sum_{i=1}^{k} p_i U_i(|\phi\rangle\langle\phi_i| \otimes \rho_a)U_i^{\dagger} = \rho_0.$$

FROM QUANTUM PRIVATE CHANNEL to (APPROXIMATE) RANDOMIZATION

The concept of QPC is closely related to that of randomization (or forgetting) of quantum information/ states and the achievable.

The lower bound for the number of bits needed for QPC is actually the amount of entropy, or the thermodynamical cost, of randomization/forgetting.

Basic definition and result concerning approximate randomization have the following form.

Definition 0.6 *A superoperator $\mathcal{R}$ on $\mathcal{H}_d$ is an ε-randomizing map if, for all pure states $|\phi\rangle$,*

$$||\mathcal{R}(\phi) - \frac{\mathbf{I}_d}{d}||_\infty \leq \frac{\varepsilon}{d}.$$

CAN QUANTUM CRYPTOGRAPHY HELP TO ANSWER QUESTION

WHY QUANTUM MECHANICS?

Can we have for QM axioms whose physical, or better yet information-theoretic or information-processing g, meaning is clear - so we will have a particularly nice answer to the question "Why quantum mechanic s".

It is hoped/believed that QIPCC science will be a useful new source of axioms, with natural interpretations involving the possibility or impossibility of various information processing processes.

Quantum computational complexity has already been used to show why various modifications (or *fant asy versions*) of quantum mechanics are much too powerful and this way we can gain an insight why quan tum mechanics is as it is.

CAN QUANTUM MECHANICS BE DERIVED FROM

SECURITY AXIOMS?

Open problem. Can we built quantum physics from the following two axioms

- Unconditionally secure quantum key distribution is possible.
- Unconditionally secure bit commitment is not possible.

and, perhaps, of few other axioms?

ARE THERE NEEDS FOR BETTER AXIOMS OF QM?

- Basic question: Since special relativity can be deduced from two axioms: the equivalence of inertia reference frames, and the constancy of the speed of light, could not be possible to deduce also quantum mechanics from some simple axioms that have clear physical meaning?
- Could we do that using some information processing based axioms?
- Fuchs and Brassard suggested to consider as axioms (a) the existence of unconditionally secure cryptographic key generation and (b) together with impossibility of secure bit commitment.
- One such attempt was done by Clifton, Bub and Halvorson with three axioms: No signaling, no broadcasting and no bit commitment.
- Could derivation of such axioms be a common task for (quantum) physics and (quantum) informatics?

CBH THEOREM

Clifton, Bub and Halverson (2002) have shown that observable and state space of a physical theory must be quantum mechanical if the following conditions hold:

- no superluminal information transmission between two systems by measurement on one of them;
- no broadcasting of information contained in an unknown physical state;
- No unconditionally secure bit-commitment

Actually they showed that the above constrains force any theory formulated in C^*-algebraic terms to incorporate a non-commuting algebra of observables for individual systems, kinematic independence for the algebras of space-like separated systems and the possibility of entanglement between space-like separated systems.