QUANTUM COMPUTING 9

Jozef Gruska

Faculty of Informatics
Brno
Czech Republic

November 10, 2002

9. QUANTUM CRYPTOGRAPHY

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

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

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

Experimentally, secure quantum key distribution has been tested, using polarization or phase of photons, for distance of 47 km using standard optical fibres and for the distance of 1.6 km in open air. Earth-to-satelite quantum bit transmissions are considered as feasible. Quantum cryptography is therefore in the advanced experimental and development stage.

FUNDAMENTAL DIFFERENCES

between classical and quantum cryptography

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

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

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

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

CLASSICAL CRYPTOGRAPHY — ELEMENTS

Classical cryptography has four main important components:

- Secret-key cryptosystems:

  CESAR, HILL, VIGENER, 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, ...

$\boxed{\text{CLASSICAL CRYPTOGRAPHY — EXAMPLE}}$

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

encoding key plaintext cryptotext $\qquad$ decoding
algorithm $\qquad\qquad\qquad\qquad$ 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 achievments 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

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.

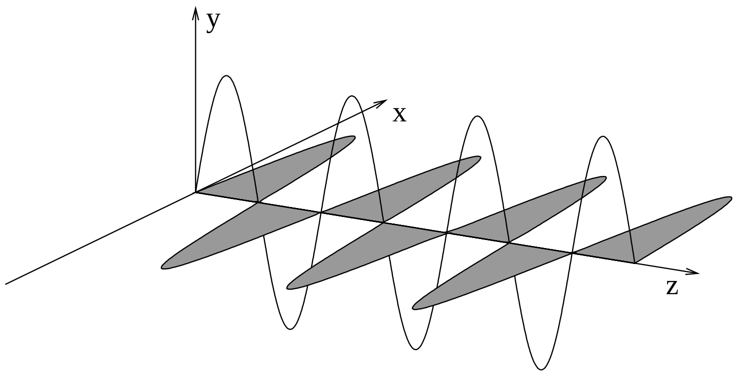

Figure 1: Electric and magnetic fields of a linearly polarized photon

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 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 $\cos^2(\theta - \theta_1)$.

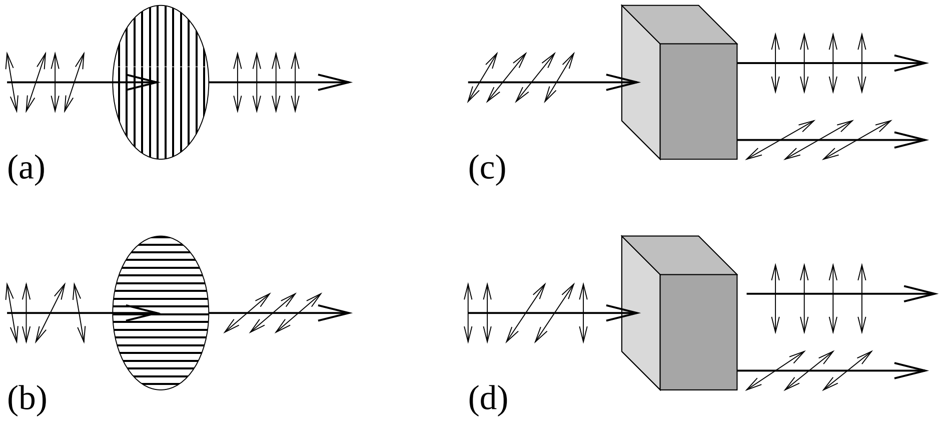

Figure 2: Photon polarizers and measuring devices-80%

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 2a,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 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

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

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

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

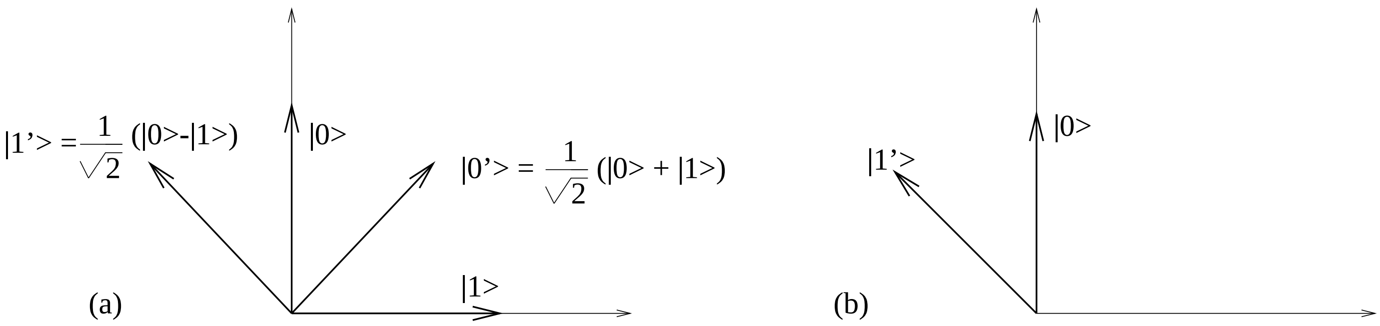

Figure 3: Polarizations of photons for BB84 and B92 protocols

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

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

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

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

Transmissions

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

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

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

Figure 4: Quantum cryptography with BB84 protocol

Figure 4 shows the possible results of the measurements and their probabilities.

An example of an encoding–decoding process is in the Figure 6.

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

Raw key extraction

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

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

Figure 6: 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 $2^{-(n-k-1)}/\ln 2$.

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 7: 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 8: 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 transformation performed by Eve's detection probe, which is assumed to be initially in the 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.

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.)

Collective attacks. Their power is between that of individual attacks and coherent attacks. Eve brings each transmitted particle into an interaction within an auxiliary system and, at the end, after listening to all public discussions, she measures all auxiliary systems together

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

Successes

1. Transmissions using optical fiber to the distance of 47 km.
2. Open air transmissions to the distance of 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 fiber. (Current error rates: $0,5 - 4\%.$)
3. To move from the experimental to the developmental stage.

CLASSICAL and QUANTUM ONE-TIME PAD

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 the so-called Pauli matrices.

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 choosen 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 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 observables

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

and record bit-outcomes of the measurement.

Using a communication via a public channel they determine the cases they used the same mesurement. 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.

The so called Bell inequalities are a tool to detect the presence of an eavesdropper for 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.

Gedanken experiment by Bell and physical experiment by Aspen demonstrated that this Einstein idea does not work.

BELL INEQUALITIES II.

Let a pair of electrons whose spins add up to zero is created and sent off in two directions. Let us have on each path a switch and two Stern-Gerlach magnets, set at different angles.

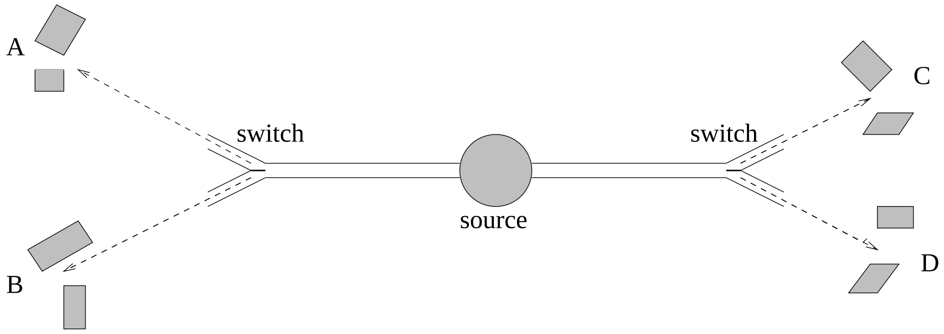

Figure 9: Aspect's experiment

For $Y \in \{A, B, C, D\}$ let $Y = 1$ or $Y = -1$ denote in which of two posible ways an electron gets out.

At each particular experiment one of 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 showed that quantum mechanics implies that EX can be up to $2\sqrt{2}$ and Aspect's experiment confirmed Bell's expectations.

DETECTION of EAVESDROPPING

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 distruction:

- To measure one or both 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 source.

Bell's inequalities for the Ekert protocol

Denote

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

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

$$\beta = 1 + \Delta(1, 2) - |\Delta(0, 1) - \Delta(0, 2)|.$$

Bell inequality for this protocol is $\beta \geq 0$ but quantum mechanics (without hidden variables) implies

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

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