Lecture 12: Quantum key distribution.

Secret key. BB84, E91 and B92 protocols. Continuous-variable protocols.

1. Secret key. According to the Vernam theorem, any message (for instance, consisting of binary symbols,
01010101010101),
can be encoded in an absolutely secret way if the one uses a secret key of the same length. A key is also a sequence, for instance,
01110001010001.
The encoding is done by adding the message and the key modulo 2:
00100100000100.
The one who knows the key can decode the encoded message by adding the key to the message modulo 2. The important thing is that the key should be used only once. It is exactly this way that classical cryptography works.

Therefore the only task of quantum cryptography is to distribute the secret key between just two users (conventionally called Alice and Bob). This is Quantum Key Distribution (QKD).

2. BB84 protocol, proposed in 1984 by Bennett and Brassard – that's where the name comes from. The idea is to encode every bit of the secret key into the polarization state of a single photon. Because the polarization state of a single photon cannot be measured without destroying this photon, this information will be 'fragile' and not available to the eavesdropper. Any eavesdropper (called Eve) will have to detect the photon, and then she will either reveal herself or will have to re-send this photon. But then she will inevitably send a photon with a wrong polarization state. This will lead to errors, and again the eavesdropper will reveal herself.

The protocol then runs as follows. Alice sends a sequence of pulses (for instance, femtosecond pulses with 80 MHz rep. rate), each of which, ideally, contains a single photon polarized differently. Alice encodes zeroes into H-polarized photons while unities she encodes into V-polarized photons (red arrows in Fig. 1). But this happens only in half of the cases. The other half of bits, chosen randomly, are encoded using a diagonal polarization basis (blue arrows in Fig. 1). Then, the 'D' polarization corresponds to zero and the 'A' polarization, to unity.

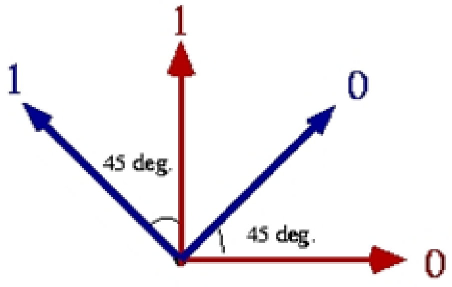

Fig.1

The receiver, Bob, measures the polarization using a standard setup (a PBS or a Glan prism with two single-photon detectors in the output ports, or a calcite crystal also followed by two detectors). This way Bob can distinguish between H and V polarizations if he uses the HV basis (further denoted as '+'). But in half of the cases Bob randomly changes his basis (the orientation of his prism) to AD (denoted as 'X').

After a certain number of bits has been transmitted (and all photons have been detected and destroyed!), Bob publicly announces which basis he used for each bit. Alice then says in which cases they used the same bases. They throw out the bits where they used different bases, and leave only those where they used the same one. After this procedure (key sifting) the length of the key is reduced twice, but what remains is random and coincides for Alice and Bob.

Then, they check if there was eavesdropping. To this end, they take a part of the key for instance, (10%) and compare it. This procedure is also public, but these 10% are then discarded. If the eavesdropping took place, the key would contain errors. Then the whole key is thrown out and the procedure is repeated again.

The table below gives an example of transmitting 8 bits of a secret key. After the key sifting, only 4 bits are left.

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	**X**	+	**+**	+	X	**+**	X	**X**
Photon polarization Alice sends	**D**	V	**V**	H	A	**H**	D	**A**
Bob's random measuring basis	**X**	X	**+**	X	+	**+**	+	**X**
Photon polarization Bob measures	**D**	D	**V**	A	V	**H**	V	**A**
public discussion of basis								
Shared secret key	0		1			0		1

One does not have to use polarization; it is also possible to encode the bits into the phase of single photons. But the advantage of polarization is that it is conserved rather well in the course of light propagation through the atmosphere. Now, the largest transmission distance is from a satellite to a ground station, ~1200 km.

An important question is how to produce single photons. One way is to use light emitted by single atoms, molecules, colour centers in diamond, or quantum dots. However, this requires a lot of effort and does not provide ‘on demand’ photons; with an account for emission and collection efficiency, these emitters are still probabilistic. In practice, one still uses weak coherent states (with the mean photon number per pulse ~0.2-0.3).

3. E91 protocol, proposed by Artur Ekert in 1991, uses Bell states emitted by a common source (SPDC) and distributed between Alice and Bob. Alice and Bob use then randomly chosen polarization bases. Then, Alice interprets H, D states as 0 and V, A states as 1. Bob should do the opposite to get the same key if the state $\left|\Psi^{(-)}\right\rangle$ is used. In this case they will have the identical key, because

$$\left|\Psi^{(-)}\right\rangle = \frac{1}{\sqrt{2}}\{\left|H\right\rangle_A \left|V\right\rangle_B - \left|V\right\rangle_A \left|H\right\rangle_B\}, \qquad (1)$$

but if we pass to the diagonal basis, we get

$$\left|H\right\rangle_A = a_H^{+}\left|0\right\rangle = \frac{1}{\sqrt{2}}(a_D^{+} + a_A^{+})\left|0\right\rangle = \frac{1}{\sqrt{2}}(\left|D\right\rangle_A + \left|A\right\rangle_A),$$

$$\left|V\right\rangle_A = a_H^{+}\left|0\right\rangle = \frac{1}{\sqrt{2}}(a_D^{+} - a_A^{+})\left|0\right\rangle = \frac{1}{\sqrt{2}}(\left|D\right\rangle_A - \left|A\right\rangle_A),$$

The same with the B photon; therefore, $\left|\Psi^{(-)}\right\rangle$ can be also written as

$$\left|\Psi^{(-)}\right\rangle = \frac{1}{2\sqrt{2}}\{(\left|D\right\rangle_A + \left|A\right\rangle_A)(\left|D\right\rangle_B - \left|A\right\rangle_B) - (\left|D\right\rangle_A - \left|A\right\rangle_A)(\left|D\right\rangle_B + \left|A\right\rangle_B)\} =$$

$$= \frac{1}{2\sqrt{2}}\{\left|A\right\rangle_A\left|D\right\rangle_B - \left|D\right\rangle_A\left|A\right\rangle_B\}.$$

(Generally, the singlet state $\left|\Psi^{(-)}\right\rangle$ is invariant to any basis transformation.) Therefore, for the 'X' basis, Alice and Bob will detect orthogonally polarized states.

To check the existence of an eavesdropper, Alice and Bob test Bell's inequalities.

4. B92 protocol, proposed by Bennett in 1992, uses two non-orthogonal states, for instance $\left|H\right\rangle$ for 0 and $\left|D\right\rangle$ for 1 (Fig. 2).

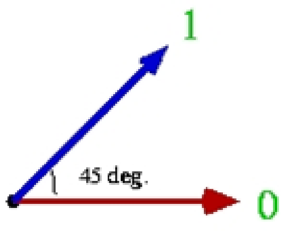

Fig.2

Alice sends 0 or 1 bits, but 0 she sends in the '+' basis, and 1, in the 'X' basis, and again she randomly chooses the basis. Bob also chooses the basis randomly. If he obtains V polarization in the '+' basis, it could not be H, so he writes down '1'. But if he obtains, in this basis, H, it could be actually D, so he says that the result is inconclusive (see Fig. 3) and throws this bit out.

The same happens if Bob uses the 'X' basis and obtains D: it could be D, but it also could be H; therefore the result is inconclusive (Fig. 3) and the bit is discarded. And only if Bob obtains A in the 'X' basis, he writes down '0' because it could not be D.

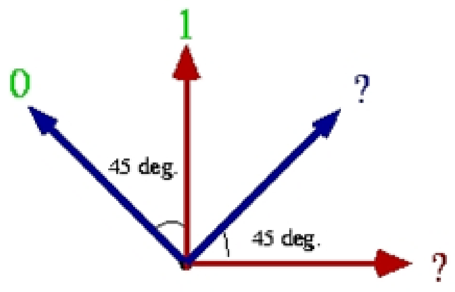

Fig. 3

The B92 protocol is easier to realize than BB84 and, as we will see later, it can be applied to continuous-variable states. It is believed however to be less secure than BB84.

5. Continuous-variable B92 protocols

Any two non-orthogonal states can be used for the B92 protocol. It is important though to have states orthogonal to them, or at least approximately orthogonal. An example is two coherent states. Two coherent states are always non-orthogonal: the scalar product of two coherent states is $\left\langle\alpha\middle|\beta\right\rangle = e^{-|\alpha-\beta|^2}$. For two weak coherent states, this scalar product is always essentially nonzero; therefore two weak coherent states are always non-orthogonal.

Usually the two states just differ by phase; the zero is encoded by the state $\left|\alpha\right\rangle$ and the unity, by the state $\left|-\alpha\right\rangle$ (Fig. 4). This encoding is very simple in practice, using a phase modulator. So Alica sends these two states to Bob, encoding the bit into the phase of a coherent state with a small amplitude, $|\alpha|<1$.

To measure these states, Bob uses homodyne detection. If the value of the q quadrature exceeds the dashed line in Fig. 4, the conclusion is that the state was $|\alpha\rangle$ and Bob writes down ‘1’; if the value is lower than the left dashed line, then the state must have been $|-\alpha\rangle$ and Bob writes down ‘0’. In all other cases the result is inconclusive.

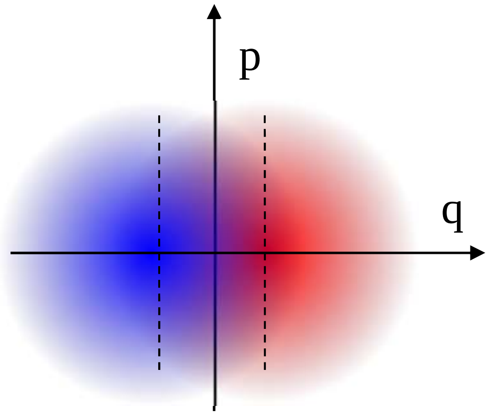

Fig. 4

The same protocol can be realized with polarized bright states of light (this is the protocol running in Erlangen). Indeed, consider now two strong coherent beams polarized approximately circularly, but with small deviations towards H and V directions. Such states can be shown on the Poincare sphere, but not a unity one: the radius now will be given by the mean photon number. They will be close to the North pole (Fig. 5), and provided the radius of the sphere is large, the landscape around the states will be practically flat. Then, the picture will be as in Fig. 4: the two states will be displaced in the H-V direction and partially overlap. A Stokes measurement will distinguish them partially, like the two weak coherent states. And in contrast to homodyne detection, here one does not need a local oscillator, since the role of a local oscillator is played by the circularly polarized polarization component.

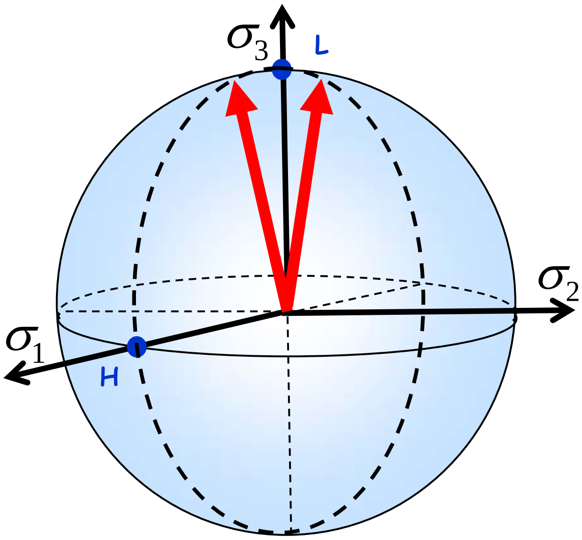

Fig. 5

Literature:

1. D. Bouwmeester, A. Ekert, A. Zeilinger (Eds.), The Physics of Quantum Information.