Quantum Cryptography

Submitted by: Yoav Pollack

Introduction:

Classical Cryptography has several inherent flaws. The much acclaimed Public Key method for example, relies on the difficulty of solving certain mathematical problems such as factoring large numbers. Quantum computers should, in theory, be able to solve these problems, rendering these methods obsolete.
In quantum cryptography, quantum channels are used to distribute keys only. The coded messages are sent through public channels.
In classical communication a signal can be split and then amplified, so that the communicating parties cannot know whether eavesdropping has taken place. This puts in jeopardy the sharing of private keys. In contrast, the 'no cloning' theorem of quantum mechanics states that we cannot duplicate the unknown state of a particle in order to have copies of the original.

The proof of the 'no cloning' theorem goes as follows:
$|\psi\rangle$ is the original state of particle A and $|Blank\rangle$ is some general state of a particle B which we shall use to copy particle A. The overall state is therefore $|\psi\rangle \otimes |Blank\rangle$. an operation on a particle should be unitary, and we wish it to copy the original state:

$$U(|\psi\rangle \otimes |Blank\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{1}$$

This should of course work for any state, and we therefore choose without loss of generality another state which is neither the same nor orthogonal to the original one of particle A.

$$U(|\phi\rangle \otimes |Blank\rangle) = |\phi\rangle \otimes |\phi\rangle \tag{2}$$

Taking the inner product of the the two results we arrive at:

$$(\langle Blank| \otimes \langle\phi|)(U^\dagger U)(|\psi\rangle \otimes |Blank\rangle) = (\langle\phi| \otimes \langle\phi|)(|\psi\rangle \otimes |\psi\rangle) = (\langle\phi||\psi\rangle)^2 \tag{3}$$

on the one hand. On the other hand:

$$(\langle Blank| \otimes \langle\phi|)U^\dagger U(|\psi\rangle \otimes |Blank\rangle) = (\langle Blank| \otimes \langle\phi|)(|\psi\rangle \otimes |Blank\rangle) = \langle\phi||\psi\rangle \tag{4}$$

We arrive at a contradiction since we assumed the states are not identical or orthogonal.

This means that if we limit communication to single particles we can avoid the problem of split signals, and worry only about measurements of the signal as detailed shortly.

Quantum Cryptography can be achieved by two conceptually different methods. Using single photons or using entangled particles. The following scenarios of quantum cryptography are naive examples meant to illustrate the main concepts. In practice many more considerations have to be taken into account.

Single Photons (BB84 protocol):

There are several ways in which single photons can be used to encrypt data, all of which apply the same principles. As an instructive example we shall focus on the polarized photons scheme. In this scheme, the party interested in sending encrypted data (commonly called Alice), sends single

polarized photons to the receiving party (Bob). The scheme requires that, on the transmitting side, the polarization of these photons would be randomly selected between one of two orthogonal states (say $|\Leftrightarrow\rangle$ and $|\Updownarrow\rangle$ corresponding to 0 and 1 bits).
Furthermore these photons have to go through a Pockels Cell, a device which can rotate the polarization of the photons (say by 45^o) or leave it unchanged, and does so randomly (the operation of the Pockels Cell shall determine the basis in which the polarized photons are at eigenstates, we refer to the 0^o rotation as the $\oplus$ basis, and the 45^o as the $\otimes$ basis). Note that while both apparatus (photon emitter and Pockels Cell) operate randomly, Alice knows the results.

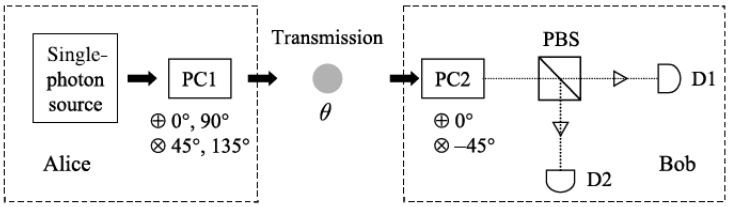
On the receiving side, the photons go through another Pockels Cell this time with an opposite rotation (-45^o or 0^o). The photons then go through a Polarization Beam Splitter (PBS) which sends the photons to one of two detectors according to their polarizations, vertical to the first and horizontal to the second. A general polarization of a photon is given by:

$$\psi_\theta\rangle = sin\theta|\Leftrightarrow\rangle + cos|\Updownarrow\rangle \tag{5}$$

so that the probabilty of sending any polarized photon to the either detector is:

$$P_1 = |\langle\Updownarrow|\psi_\theta\rangle|^2 = cos^2(\theta) \qquad P_2 = |\langle\Leftrightarrow|\psi_\theta\rangle|^2 = sin^2(\theta) \tag{6}$$

Note that Bob knows not only the readings of the detectors, but also the randomly selected basis of the Pockels Cell ($\oplus$ for 0^o rotation, and $\otimes$ for the -45^o rotation).



The way in which Alice and Bob can extract a shared key using this process is as follows:
After Alice had sent a sufficient amount of photons (bits) to Bob (the raw key), they compare their choice of bases using a public channel. The use of the public channel for communication does not impair the secrecy of the process, as only the choice of bases is revealed and not actual bits. We shall see later why this is of no help to a potential eavesdropper. Moreover the use of a public channel is essential as it guarantees no one can alter the messages exchanged.
Bob then discards every bit measured in the wrong basis (arriving at a sifted key), and sends a subset of the remaining bits to Alice for analysis. Alice can tell by this subset whether eavesdropping has taken place, or whether the key is secure.

The following table lists all the possible combinations and tells in which instances Alice and Bob get a shared bit:

Alice's Base	⊕	⊕	⊕	⊕	⊕	⊕	⊗	⊗	⊗	⊗	⊗	⊗
Alice's Bit	1	1	1	0	0	0	1	1	1	0	0	0
Bob's Base	⊕	⊗	⊗	⊕	⊗	⊗	⊗	⊕	⊕	⊗	⊕	⊕
Bob's Bit	1	1	0	0	0	1	1	1	0	0	0	1
Same Base	Y	N	N	Y	N	N	Y	N	N	Y	N	N
Kept Bits	1			0			1			0		

Now a third illegitimate party (Eve) wants to acquire the key as well. She cannot, as mentioned before, duplicate the photons. This is why this scheme uses single photons. If more than a single photon is emitted, Eve can read one photon and let its duplicate copies pass through unaffected thereby avoiding detection. With a single photon scheme, Eve has to measure the polarization of the original photons sent, and send new photons of her own to Bob. Such measurements would give the exact polarization of the photons if measured in the right basis, but of course eve has no way of knowing which base Alice chose (randomly). If measured in the wrong basis, the readings of the photons' polarizations would be probabilistic. The amount of data Eve tries to acquire determines the ease with which she is detected. For simplicity we shall assume Eve tries to acquire the whole key. Eve can use a setup like Bob's (only without the Pockels Cell which is redundant for her). Lets say Eve measure in the $\oplus$ basis, meaning she does not rotate the polarization of the photons. Any photons Alice sends in the $\oplus$ basis (50% of photons), would be correctly measured by Eve and sent onwards to Bob as if a measurement has not taken place. However the rest of the photons sent in the $\otimes$ basis have an equal chance of being measured in each detector. The photons sent onwards to Bob therefore are completely uncorrelated to the original ones, and have a 50% chance of registering a wrong result even if Alice and Bob chose the same Basis. This kind of eavesdropping attempt would register as an overall 25 % error in the sifted key, this is what Alice looks for in her analysis of the subset of the sifted key.

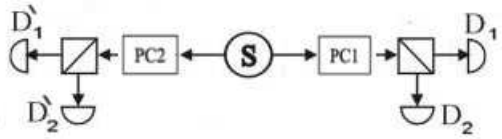
This is of course a primitive and simplified version, but it illustrates how the 'no cloning' and the principles of quantum measurements, can be used to ensure detection of unwanted measurements.

Entangled Particles (E91 protocol):

The scheme for entangled particles cryptography employs a source emitting two entangled particles in the singlet state, one of which goes to Alice and the second one to Bob (we shall call their direction of progression the z axis). The source does not have to be secure in order to accomplish secrecy and can even be in the possession of Eve (although then a third party can simply disable communication of course). Let's assume for simplicity a source of electrons [Actual apllications use photons. The information corresponding to photons will be given in brackets] emitting particles in the state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) \tag{7}$$

where Both Alice and Bob have the same Pockels Cell, Polarization Beam Splitter and detectors setup that Bob had in the previous section.



Alice measures the polarization of the particles in one of three bases obtained by rotation of the $\oplus$ basis around the z axis by the angles $\phi_1^a = 0^o$ $[0^o]$, $\phi_2^a = 90^o$ $[45^o]$ and $\phi_3^a = 45^o$ $[22.5^o]$. Bob measures in the bases rotated by $\phi_1^b = 0^o$ $[0^o]$, $\phi_2^b = -45^o$ $[-22.5^o]$ and $\phi_3^b = 45^o$ $[22.5^o]$. These angles are conspicuously the same ones as in the EPR experiment [The angles for photons are half those for electrons. This is because of the difference between rotations of spin half and spin one particles]. After a sufficient amount of particles have been measured, Alice and Bob exchange information

about the bases chosen using a public channel. Their next step is to proceed and compare the orientations [polarizations] measured when the bases were not identical i.e. when the angles of rotation were not the same. This is also done on a public channel. As in the EPR experiment, we have a correlation function of the measurements:

$$\langle a(\phi_i^a)b(\phi_j^b)\rangle \tag{8}$$

where $a(\phi_i^a)$ is a variable which gives +1 for measurements of up orientation [horizontal polarization] by Alice and -1 for down orientation [vertical polarization] measurements taking into account only measurements in the appropriate angle (ϕ_i^a). $b(\phi_j^b)$ receives similar values according to Bob's measurements
A quantum calculation gives:

$$\langle a(\phi_i^a)b(\phi_j^b)\rangle = -cos(\phi_i^a - \phi_j^b) \tag{9}$$

$$[\langle a(\phi_i^a)b(\phi_j^b)\rangle = -cos(2(\phi_i^a - \phi_j^b))] \tag{10}$$

In a similar manner to the violation of Bell's inequality proof, we define a quantity S composed of the correlation coefficients of measurements in different bases:

$$S = |\langle a(\phi_1^a)b(\phi_3^b)\rangle + \langle a(\phi_1^a)b(\phi_2^b)\rangle + \langle a(\phi_2^a)b(\phi_3^b)\rangle - \langle a(\phi_2^a)b(\phi_2^b)\rangle| \tag{11}$$

Applying the result for $\langle a(\phi_i^a)b(\phi_j^b)\rangle$ and the appropriate angles we get:

$$S = 2\sqrt{2} \tag{12}$$

If Eve tries to obtain knowledge of the particles' orientation, she will reduce the amount of entanglement of the particles and thereby lower the value of S, thus letting Alice and Bob know they are being eavesdropped. If on the other hand the communications is secure, Alice and Bob can now use the remaining measurements (in identical bases) to form a secret key (noting of course that their measurements will be perfectly anti-correlated, $\langle a(\phi_1^a)b(\phi_1^b)\rangle = \langle a(\phi_3^a)b(\phi_3^b)\rangle = -1$).

In this method only 2 out of every 9 measurements are used to create a key, as opposed to around half of the measurements in the BB84 protocol (half of the measurements are discarded due to different bases, and a small subset of the remaining results is compared for eavesdropping analysis thereby compromized). This makes the E91 protocol less efficient. However, in the BB84 protocol, a single photon source is required for every pair of communicators, whereas in the E91 protocol a single source can be used as a switchboard for creating private keys between any pair of would be communicators.

Bibliography:
The Physics Of Quantum Information - Bouwmeester, Ekert, Zeilinger, 2001.
Quantum optics. an introduction - Fox M. 2006