

# Quantum Cryptography

by Caboom

## 1) And God said let there be... tutorial

This essay can be little out of usual hacking/cracking topic, but I wanted to present you a new technologies that are now used. Also, this tutorial has a 'growing intension' so it will be updated at time to time. The needing for update is mainly here because of need for better explanation because it's hard topic even to those that are familiar with quantum physics and this tutorial is not written for people that are familiar with quantum physics and will give you only basic idea about quantum cryptography. I would be very thankful for any suggestion how to make this tutorial better and clearer because it's very hard to explain some details of quantum theory to people that are not familiar with it. I will be most satisfied if this tutorial can read even my grandmother and get something from it.

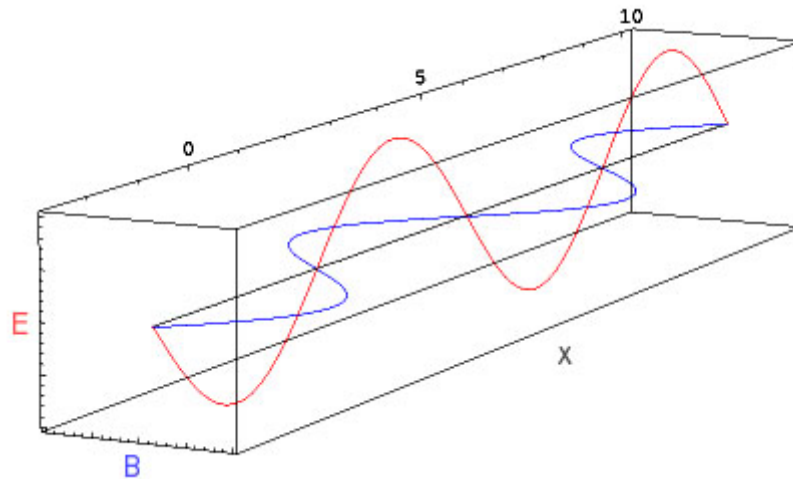
## 2) Classical heaven => Quantum hell

Ok, so let's get to basics of quantum theory. First, let me explain the term '*quantum*'. As a more careful observer can notice the close relative to the word quantum is a word quantity. At the very beginning of this century physicians noticed that there is something wrong with the classical theory, to be more precise, they've noticed that their perspective of the fundamental particles they had are not matching the experimental results they got. The logical conclusion was that there is something wrong with the classical idea they had about atom. *Max Planck* therefore has introduced the new approach to the matter. In the classical physics, electron orbiting (orbiting around is also relative term, I'll explain it little bit later) around the core or the atom could have any possible energy, and related to this, could orbit around the core at any possible distance. The problem with that vision was that because the electron is negative charged and core, because consisted of positive protons and neutral neutrons, was positive charged it was expected that electron would collapse into core for about 0.0000000001 sec (because of different charges, core attracts electron). The answer was that electron can't have any energy while orbiting around core, energy of electron is *quanted*. This means that electron has strongly defined possible energies, and can orbit only on some distances around atom. To be more precise, even that is not definitely true, the electron is not orbiting exactly around orbits, orbits are only defining the place where is best possibility to find electron. Confused? You should be... at least shocked if you've never heard about it. This brings us to the rather confusing and paradoxal world of quantum mechanics (quantum mechanics - one of parts of physics dealing with the phenomena of the small world, basically it research the movement of the particles, parallel to ordinary mechanics in classical world, but much wider). In world of quantum mechanic we are not talking about the exact value, but the possible value. To make it more clear, say you want to find the place where is the particle you're especially interested in, you won't be able to find the exact spot and say here it is, what you'll get will be something like beaver that had car accident... one relatively wide circle darkest in the center... That center is the place where is the greatest probability to find the particle, but not necessary the place where particle really is. That is consequence of our impossibility to make perfect measurement. In our world of 'big' objects, measurements we take are good enough to say 'beaver was 1.5m long' (hmmm... long

beaver), but if you look more careful 1.5m could be 1.485755432m or 1.49532221m or 1.5000000m, do you get the point, what is behind? You always have error in measurement. In the world of small object, measurements are so sensitive that you can't for instance measure the position and impulse (impulse is product of mass and speed, it determines the movement) of particle, that is for one of fundamentals of quantum mechanic. Of great importance is to understand that physics is based on measurement, not on the theory. So let us make conclusion... Quantum mechanic is dealing with 'small' world of atoms and fundamental particles, while classical physics founded mainly by Isaac Newton is dealing with the 'big' world of beavers... In quantum world all observables (things that we can measure) have discrete values (that means that you can't have any value of observable, for instance, electron can't have any energy while orbiting around atom), and we can speak only about probability for real events... there are many more rules, but these are one of the basic. If you want to know more, you can take some of many good quantum mechanics books, but watch... be sure that you're good with linear algebra and you've been through the higher courses of math, or avoid books with equations.

### 3) ...and God also said let there be light

We've now been through the basics of quantum mechanics, don't give up... I have to explain to you some facts about light also before I get to the point. The phenomena of matter is that it's constructed from smaller parts. The smallest ones that we know that build all other bigger constructions of nature, like atoms and molecules we call *fundamental particles*. What physicians have found was that particles are not particles in a sense of marbles that are wondering around, but they are also waves. Let me break one more illusion for you. Particles are not looking like balls, as the matter of fact you can't say that particle has any shape. If someone shows you a picture of a black blurred ball, and tells you: "it's the picture of electron", he is probably showing you a picture of energy distribution of electron (... huh it doesn't matter, it's just not the picture of exact particle, remember that with probability? It's that story). What I'm pointing at? In this 'quantum cryptography' play main role is played by light, so I have to say something about light and terms like *polarization* and *phase shift*. Let me explain that wave-particle thing. You've probably heard for photons, and you've probably heard for electro-magnetic waves. See the usual picture of electromagnetic wave (E - electrical field, B - magnetic field, x-some direction the light is traveling)



Well that are two views on the same thing we call light. The light has really bad manners, I could say the light is acting little bit schizophrenic. It determines of the measure we take, we can see that light is acting like electro-magnetic wave, or that the light is made of particles we call photons. No, it's not like water, where we have great amount of particles that interact and make waves we can see. This is result of fundamental organization of nature that we call duality. I will stop at this moment with further explanations why is this that way. Yes there is deeper reason, but... let us stop here ok?

Let me now explain terms *polarization* and *phase shift*. Do you see that x axis? It the one represented with the long black line in the middle of graphic. Well, why couldn't you rotate other two axes around it? There is not any reason why you couldn't rotate the whole picture around that axis. Let us suppose we have two waves of same wavelength (oh yes, this is the one more flavors of light, actually that is the value that determines the energy of wave, and this value determines is this a radio wave, normal visible light, x - ray, gamma ray etc.), and let them travel the same path x. But what about that other two axes E and B? One wave must have axes E and B at the constant angle 90 degrees (you'll also see in further text expressions like  $\pi$ ,  $\pi/2$ , that is the other way to mark the angles,  $\pi = 180$  degrees, yes that is the same one  $\pi = 3.14...$  Ok, now you know you can rotate those two axes E and B around axis x and what you can do with it? If you for instance take some arbitrary position of vectors E and B, let it be position of axes you can see in figure 1 on the picture bellow:

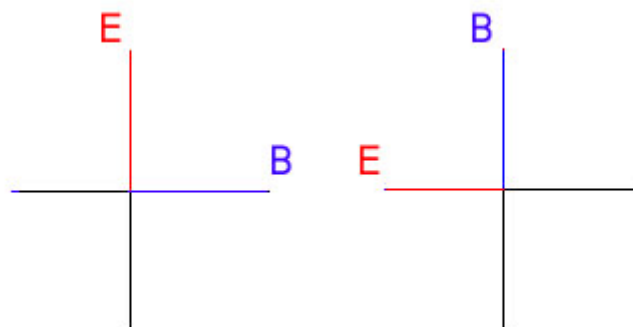
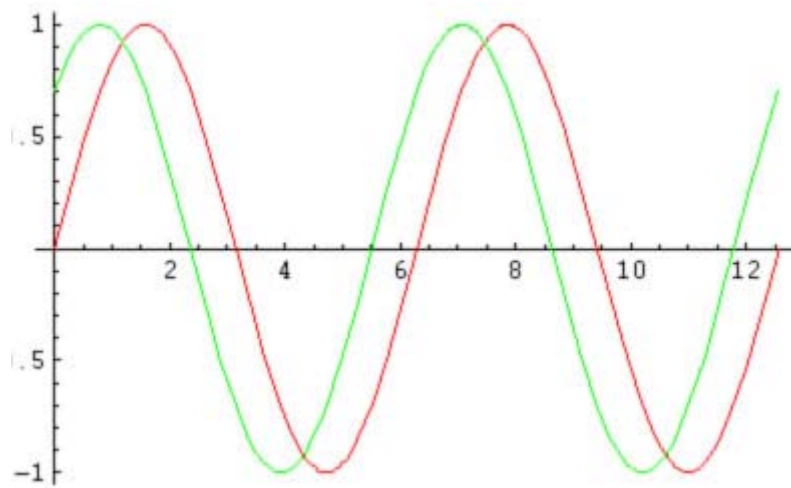


Figure 1

Figure 2

If you take positions of vectors E and B like on figure 1 as the arbitrary (polarization is not definitive term, there is not existing absolute position of vectors E and B but you must first define some arbitrary position of vectors E and B and then consider the term of polarization), you can see if you look a little bit closer on figure 2 that vectors E and B are rotated for 90 degrees anticlockwise (or, you can also say rotated for  $\pi/2$ ). We now can finally define the term of polarization. You can say that the electro-magnetic wave on figure 2 is polarized for 90 degrees (of course, compared to our arbitrary polarization on figure 1). Even one photon, if we consider particle side of light, can be polarized, why? Because, as I've explained before, the light is both particle and wave, and even one photon can be considered also for wave (sorry, not further explanations for now...), and you can also say that photon is polarized at some angle. When you use some light source like bulb you have electro-magnetic waves of all possible angles of polarizations. You can get especially polarized light at some angle with the piece of equipment called *polarizator*.

Now there is only one term left to define, *phase shift*. You could see on the picture above (one 3D picture) that function that describe electro-magnetic wave really looks like wave. That is Sine function, and you can see that is periodical function. Now I will tell you that period of this function is 360 degrees or  $2\pi$ . That 'periodical' means that the function is repeating it's image after some value x. Look now on the picture bellow:



You can see that the green and red functions are the same one function, but shifted on the x axis. To be more precise i will say that equation for red function is  $\sin(x)$  and equation for green function is  $\sin(x+\pi/4)$ . I can now say that green function is *phase shifted for  $\pi/4$  (45 degrees)* considering red function. Same thing is for electromagnetic wave because electromagnetic wave is described with sine function (that is one of possible ways to describe electromagnetic wave, but for purpose of this tutorial this is good enough).

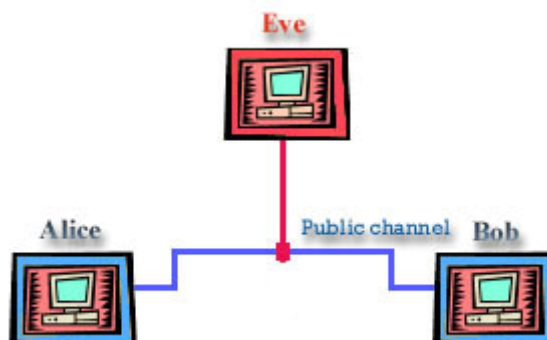
#### 4) To those that are still with us...

Now that are basic terms of physics needed for purpose of further reading explained, we can now pass to the basic topic of this text, and this is (in case you already forgot it by now) quantum cryptography and its advantages compared to normal cryptography. This long beginning was not mainly there in purpose of explanation of quantum cryptography itself, but in purpose of explaining how the information is distributed. The main reason why quantum crypto is so impressive is that there is used one of the fundamentals of physics in very practical way.

Let's turn our eyes now on standard crypto systems, because they are roots of quantum cryptography. We could define cryptography as the art of hiding information in a string of bits that are meaningless to any unauthorized party. To succeed in our task to hide information we usually use an algorithm to combine *message* with some additional information that we usually call *key* to produce *cryptogram*. This technique is called *encryption*. Yeah, I know that most of you heard this story before, but I must make things clear here, so have patience and you will be rewarded, maybe. The thing you probably don't know if you are newbie into cryptography and information theory is that person that encrypts is traditionally called *Alice* and person that receives a message is traditionally called *Bob* (that mainly stands for A and B). Just look at the picture.



My sympathy in this story goes to character that is traditionally called *Eve*. That is the evil one, Eve stands for eavesdropper. As the word says that is the one that intercepts the information that Alice sends to Bob. Eve is that unauthorized, malevolent person we usually call cracker. As I've said before, just look at the picture.



Yes, now we have complete picture of problem that we are dealing with. Public channel is usual channel we use to distribute information like phone lines, optical cable, internet, maybe power lines in the recent future, etc.

For any crypto-system to be secure, it should be impossible to unlock cryptogram without Bob's key. This in practice is softened to that the system is just extremely difficult to crack. The main idea is that the message should remain protected as long as the information message contain is valuable (that explain why is DES for instance, crackable at all). Crypto-systems are divided in two main classes. This depends on wether key is shared in secret or public. I will give you two examples, one for every group; "one-time" pad and RSA, exposing their qualities, and disabilities.

## 5) "One-time" pad vs. RSA in normal cryptography

### *"One time" pad*

This system was proposed by Gilbert Vernam at AT&T in 1935 (quite old system, I must say), involve sharing a secret key and is the only crypto-system that provides proven, perfect secrecy. In this case Alice encrypts a message using a randomly generated key and then simply adds each bit of the message to the corresponding bit of the key. The scrambled message is then sent to Bob, who decrypts the message by subtracting the same key. It can be seen below

<b>Alice</b>			
Message			<b>11001010</b>
Add key	+		<b>01110010</b>
Scrambled Key	=		<b>00111100</b>
<b>Transmit</b>			
<b>Bob</b>			
Scrambled text			<b>00111100</b>
Subtract key	-		<b>01110010</b>
Message	=		<b>11001010</b>

Normally, encrypted text doesn't contain any information until you use key. Although perfectly secure, the problem with this system is that is essential that Alice and Bob share common secret key, which must be at least as long as the message itself. They can also use the key for single encryption (that explains name 'one-time' pad), because if they used key more than once Eve could record all of the scrambled messages and start to build picture of the key. The real trouble starts here. If they want to share same key, then key must be transmitted by some

trusted means, such as courier or through personal meeting between Alice and Bob. Yeah, now begins a story of espionage... etc. I can think a couple of thousand problems here, ranging from authentication problems, expensive meeting, eavesdropping, etc... I believe you can think even more of them due it's 3am now that I'm writing this. It's same with net, let me just mention IP-spoofing. Got it? I believe you do. The good thing is that if Eve would like to crack message, not knowing the key, she would have to try all combinations, and yet not knowing which was right.

### *RSA (Rivest, Shamir, Adleman)*

RSA belongs to other class of crypto-systems, so called "*public-key crypto-systems*". First public-key crypto-systems were proposed in 1976 by Whitfield Diffie and Martin Hellman who were at Stanford University then. They used so called *one-way* functions in which is easy to compute the function, for instance,  $f(x)$  (that means that we have some function depending on some variable  $x$ ) but they are hard to compute in other way. In way to define what is meant by 'hard to compute in other way' we can for instance take time as a factor, the good one crypto-system could be one that a time to do a task grows exponentially with the number of bits used to encrypt. For example we can take breaking number on prime factors. Let me show it this way, you can work out that  $109 \cdot 59$  is 6431, but it would take much longer time to us to find out that the prime factors of 6431 are 59 and 109.

However, some of these one way functions have a so called "trapdoor", which means there is easy way to compute function in difficult direction with some additional information, in this case key or password. So if you for instance know that one prime factor of 6431 is 59, it's not hard to calculate other prime factor. RSA is based on that function I've explained above. It is believed today, but there is not any strong theory, that the time needed to find prime factors of an integer, and to obtain private key, grows exponentially with the number of input bits. There could be major security hole here if someone finds out that there is faster way to calculate prime factors, the problems are enlarging with the fact that the most money transactions security systems are based on RSA. Hey... brakes here, lamer alarm (only for those of you that need it) ... Don't think that you'll find out the way to factorize prime numbers, and break into Wall-Street server in about 10 minutes, all with loud music causing brainstorm in you head (that looks like that idiotic description of hackers, seen so often on media)... Generations of mathematicians (and yes there are some much more intelligent than me and you together) dedicated their careers to that task, and all this story draws it's roots from Fermat I think, all back to 19-th century so... just don't blame yourself, ok. If you wish to dedicate your lives to science, just forget that picture of Albert Einstein developing his special theory of relativity for one long weekend when his wife had PMS and the couldn't do anything else, OK? Hacking is science and art, like mathematics or physics (and programming, off course), and it takes long, long time, and great dedication. I'll pull water now, and continue this topic...

Ok, what means public crypto-system at all. Well that means that you with one key you make (pass that you type), you get two keys, public and private. Looks like good bargain to me. You can share public key with the all world, and they can encrypt message with it, but once the message is encrypted only, and only the owner of private key can read it. Also, when you send message that you've encrypted with private key (you keep it for yourself, that's what that private means), that message will be decrypted with public key, but the public key won't decrypt any message that are is not encrypted with private key. That explains the term digital signature. No, you can't compute private key having public key, at least not for some reasonable time, considering, off course, that the other side choose hard password to break.

We are getting close to topic here. There is one more reason (that is mostly the reason for having quantum cryptography as a solution) why RSA could became unreliable in the future.

There are devices, that are only theory now (but good one, believe me, experiments say so), that are called quantum computers (I'll write an essay on them too, very soon), that could factorize numbers not exponentially, but linearly with number of bits. The explanation is in, let us say, parallel processing that is even more parallel than any other that exists now. Yeah, it sounds stupid, and maybe I'm stupid, but I can't put the idea of quantum computing in one sentence.

## 6) The last (exit).... but not least

Well, as we could see, the public crypto-systems like RSA could become useless in the future (don't worry, you'll be grandpas by that time), with the appearances of the first useable quantum computers (boxes in further text). You have one possible way, and yet the simplest one, to secretly send a message. You can always turn to secret-key systems, such as Vernam's system described above, if you have the way to perfectly hide the secret key from Eve. This is the exactly the moment where quantum physics enters the scene.. Bob and Alice must share a secret key (in opposite of public-key systems), and quantum cryptography allows two physically separated parties to create random secret key without resorting to the services of courier. What's even better it also allows them to verify that the key has not been intercepted. Quantum cryptography is not therefore a totally new crypto-system, but the procedure to distribute the key in perfect secrecy from other parties like Eve (hehehehe). So, let me put this I've just said in few words; quantum crypto is not crypto algorithm, but it allow a key to be securely distributed and is consequently a natural complement to Vernam's cipher.



To understand how quantum cryptography works we can consider the "BB84" communication protocol, which was introduced in 1984 by Charles Bennett of IBM and Gilles Brassard from the University of Montreal. Alice and Bob are connected by a quantum channel and a classical public channel (see the picture above). If single photons are used to carry information the quantum channel is usually optical fibre. The public channel, however, can be any communication link, such as phone line or internet. Let us stop now a little and say something about information. The information in computer world is represented by series of 0's and 1's that assembled together in defined order present information. That information can be anything numbers, words, pictures, we only need to know how to interpret that binary information (binary stands for there is information represented by series of 0 and 1, but this is really out of topic so.... sorry I wasted eyes to those that well know that, but I felt like saying it). Well, that 0 and 1 while traveling your phone lines is represented like some voltage. Usually in the world of digital electronics logical 0 and 1 are represented like 0V and 5V considering the ground (sometimes -5V and 5V, and 0V can represent some other state). In the case of quantum channel carriers are

photons and as we could see we can use polarization and phase shift.... can you dig it? Yes, we can define some arbitrary angles of polarization or phase shift (well do you see now why was that story so long). In practice, the public link is also optical fibre, with both channels differing only in the intensity of light pulses. How this thing work?



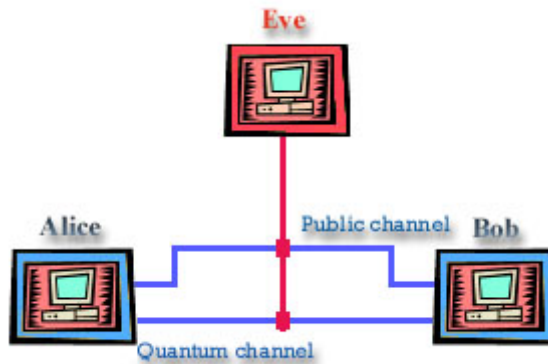
Alice's bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0
Bob's sequence of analyzers	+	x	+	+	x	x	+	+	x	+	x	x	+	+
Bob's measurements	1	0	0	1	0	0	1	1	0	0	0	1	0	0
retained bit sequence	1	-	-	1	0	0	-	1	0	0	-	1	-	0

1) First, Alice has four polarizers, which can transmit, which can transmit single photons polarized either vertically, horizontally, at +45 degrees, or at -45 degrees (look at the picture above). She sends a series of photons down the quantum channel, having chosen at random one of the polarization states for each photon (which in this case represents key, also note on pictures which polarization angles represent 0's and 1's, IT'S NOT MISTAKE, and IT'S VERY IMPORTANT to note so you could understand process).

2) Second, Bob has four analyzers, not two (that are devices that can analyze polarization angle, or several angles at one time, but note, when you put analyzer and there is single photon, if you set analyzer at some angle(s) you will be able only to see if the photon is polarized at that angle(s) or not, also when you perform measure once you can't measure polarization of the same photon again with other analyzer set to measure some other angle(s), because once you measure, the information is destroyed by measuring because of interaction of the measuring system and system you measure, this is represented in physics by so called projection theorem, because you project the measured system onto system that measures, huh sounds confusing.. yeah I've told you that about quantum mechanics, in other words this all means you can't measure ALL angles at once). One analyzer allows Bob to distinguish between photons polarized at +45 degrees and -45 degrees (see the picture above), and other allows him to distinguish between horizontally and vertically polarized photons. Note that Alice has four polarizers and Bob has only two analyzers! Also note how are 0's and 1's set by Alice. That is crucial! What Bob does then? Well, he randomly chose one analyzer and uses it to record each photon. He now writes down which analyzer he used and what it recorded (if he chose wrong analyzer, he won't get any information about the state of photon, in case you forgot, polarization is one of states of photon). For example, if Alice sent a vertically polarized photon and Bob chose to detect photons at +/-45 degrees. Basically if Bob chose +/-45 degrees analyzer there is 50% chance that he will record something, elementary my dear Watson. Even if Bob finds out later that he chose the wrong analyzer, he will have no way of finding out which polarization state Alice sent.

3) Third, after exchanging enough photons, Bob announces on the public channel the sequence of analyzers he used, **but not the results he obtained**.

4) Fourth, Alice compares this sequence with the list of bits she originally sent, and tells Bob on the public channel on which occasions his analyzer was compatible with the photon's polarization. She **does not tell him which polarization states she sent**. If Bob used an analyzer that was not compatible with Alice's photon, bit is simply discarded. For the bits that remain (look at the retained bit sequence at picture), Alice and Bob know that they have the same values - provided that the eavesdropper didn't perturb the transmission. The **bits that are left** Alice and Bob can use to **generate key** that they will use to encrypt the message they will send then by public channel.



Let us now see the case when there is Eve. Suppose the Eve has intercepted both quantum and Public channel (suppose Eve cut the fibre and she set her equipment), and of course, she sends information to Bob so her eavesdropping couldn't be noticed. What's wrong with that picture in this case? Obviously, the disclosed bits cannot be used for encryption anymore. If Eve intercepted their key, the correlation between the values of their bits will have been reduced. For example if Eve had the same equipment like Bob and cuts fibre and measures signal, she will always get random bit whenever she chooses wrong analyzers (that is statistically 50% of all cases). But having intercepted the signal Eve still has to send a photon to Bob to cover her tracks. Therefore, in 50% of cases Alice's and Bob's analyzers match, but what's in case that Eve didn't used a right analyzer and that is in 50% of cases? However in half of these cases photon will accidentally pass through the right analyzer at Bob's side. We can see now that correlation between Alice's and Bob's measures will drop to only 25% in presence of Eve. In that case Alice and Bob will know that information has been intercepted, when they compare keys over public link they will see a greater disagreement (to be more precise, twice greater) and they will drop transmission. Simple isn't it?

## 7) Quantum cryptography in real life

So how you can achieve quantum cryptography in practice? Photons are good candidates to carry information, they are easy to produce and to measure. Story I've presented for polarization can be used same for phase shift. In fact, it's more used than polarization. What's even better they can be transmitted through the optical fibre and over last 25 years attenuation of light (measure of how much photons are lost during transmission) at wavelength of 1300nm has been reduced from several decibels per metre to just 0.35 decibels per kilometre. This means that photons can

travel up to 10km before 50% of them are lost which is sufficient to perform quantum cryptography in local networks. Some of you with more technical education could note that you could use an amplifier to transmit photons, but amplifiers cannot be used because quantum states cannot be copied (in some cases yes, in case of quantum teleportation, but this is not that case). There are also some projects aiming to establish quantum communication from a satellite down to earth or other satellite, but as far as I know this is not yet practice.

Of course, this is not only problem. There is always trouble with quality of link. Uncorrelated bits may originate from several experimental imperfections. First, Alice has to ensure that she creates photons that are exactly the states she choose. If, for instance, a vertical photon is incorrectly polarized at an angle 84 degrees, there is only 1% possibility that Bob will find in channel for horizontally polarized photons. Similar problem is from Bob's side; does he measure exactly 90 degrees. Another difficulty is ensuring that the encoded bits are maintained during transmission. There is also one more problem, due to the birefringence of the fibre, the polarization states received by Bob will, in general, be different from those sent by Alice, and that also asks for calibration of their apparatus, etc. etc.

To overcome these problems, Alice and Bob have to apply a classical error-correction algorithm to their data so that they can reduce the errors below an error rate of  $10^{-9}$  (0.000000001 or one in billion) - the industry standard for digital telecommunications. And since they cannot be sure if the presence of uncorrelated bits was due to the poor performance of their set-up or to an eavesdropper, they have to assume the worst-case scenario - that all the errors were caused by Eve. There is one procedure Alice and Bob may use known as "privacy amplification" in which several bits are combined into one. This procedure ensures that the combined bits correlate only if Alice and Bob's initial bits are the same. The problem with privacy amplification is that it shortens the key length a lot and it's only possible up to certain error. That means that Alice and Bob have to be careful to introduce as few errors as possible when they initially send their quantum bits.

## **8) Last words**

In tradition of a dying tutorial I must now say something to close this text. Well you've now been introduced to one of new technologies that are now used. Don get caught in web... Port 80 is not only thing in communications today, like the phone lines also aren't all. Optical communication has been used for some 20 years, and today not only for T1 backbones. There are some other technologies that go parallel with quantum cryptography, like quantum computing and quantum teleportation that I will also present to you soon. I hope that you've liked this tutorial and I hope I've make it readable. Don't be lazy read it few times if you don't catch me (no, not because it's my tutorial) because it's confusing and hard topic. I'll appreciate any comments and suggestions, and feel free to ask me any question if you have it about quantum technology. You have my mail. Thank you for your time...