Quantum key distribution
&
Privacy Amplification

By Hanif Bayat Movahed, #0248243,
University of Guelph, Project for QIP course

Introduction:

Key distribution needs lots of technique and information. In this project I have tried to cover two different ways of Quantum Key distribution and describe the details of the first one and explain the privacy amplification of the second one.

In this project, first I tried to give the brief history about the key distribution techniques and the relation between the classical and quantum key distributions. I used various references such as: [1], [3], [6], [7], [8] for this part. Then in parts 2, 3, 4 I tried to cover completely the key distribution technique that was given by "C. H. Bennet, F. Bessette, G. Brassard, L. Salvail and J. Smolin" in 1991. I paid attention much in part 3 to the process of Eves dropping. My main reference for these parts is [1], but I used some other sources such as [5], [7]. In part 5, I tried to cover the concept of privacy amplification and describe in detail another way of key distribution, which is based on Bell's Theorem (It was given by K.Ekert in 1991), my main references for this part are [2], [3], [4]:

1. History of key distribution:

The classical key distribution is present in our every day life. For example when you buy some thing with your credit card on the internet you are already using some key distribution protocols. On one hand it may be assumed that this process is secure but experts know that it can theoretically be monitored by a third party easily and the secure code can be unlocked (decoded) by using an advanced computer or using some professional techniques. On the other hand, it is proven that quantum computers can factorize integer numbers much faster than today's computer, which is important to mention because the most advanced classical cryptography techniques depend on the difficulty of factorizing large integer numbers. (Refer to R. Rivest, A. Shamir, and L. Adleman, *"On Digital Signatures and Public-Key Cryptosystems"*, MIT Laboratory for Computer Science) In order to find more secure way to transmit information the quantum key distribution has been invented.

1.1: What is classical key distribution?

The purpose of key distribution is to communicate information between two people in a restricted way. In classical cryptography the security of crypto string depends on the security of encrypting and decrypting processes. The string is ciphered by special algorithms. The algorithms of encrypting and decrypting can be revealed to anybody else and can be publicly announced. The security of information text (bits) absolutely depends on the secrecy of the key which is the special parameters in the ciphers that consist of random, long string of bits.

The input of the encrypting algorithm consists of key and plaintext and the input of decrypting algorithm consisted of result of the encrypting algorithm with the cryptogram and the key.

To clarify the above context, I give you some simple, basic classical cryptography methods as an example:

Simplest case: We can map one number to each letter regarding its place in the alphabetical order and exchange every letter or number with a different letter which place number is $\underline{n}$ items more than the initial one. Numbers can be changed in the same way, we can add $\underline{n}$ to that number and use the $number + n \overset{10}{\equiv}$ as result. For example:

If n is 4: Guelph2003 $\rightarrow$ Kxiptl6447
If n is 5: World 89 $\rightarrow$ Btwqi 34

In every key distribution we may have third party who is called Eve. So if we assumed that there is third party in this system, Eve can guess the map by paying attention to the frequency of the alphabet and find n by calculating the frequency. So this problem can be solved if we map each letter and number by different number each time they occur (Two same letters are replaced by different letters.)

To solve the above problem we can change every word by paying attention to the place of it in the string. For example n can be calculated as the place of the letter or number, plus arbitrary number m in the string.

If m is 2, Waterloo $\rightarrow$ Zeykytxy

As we can see we have two Y regarding the two different alphabets and the two O are mapped to two different letters in resulted string.

In order to establish the key, users should use very secure and reliable channel. It should be mentioned that however it is difficult for third party (Eve) to intercept on this channel but in fact any classical key distribution can be passively monitored. The problem is that, if Eve intercepts the channel, the users can not detect the attack!

Mathematicians in 1970s invented a new key distribution, using the fact that some special mathematical operations are easier to do in one direction than the other direction. For

example factorizing a large integer number in comparison with multiplying the factors to each other is much harder.

In public key distribution, which was invented in 1970, two different keys are used, one of them is a public key and the other one is a private key. It means that anyone can crypt the string but just one person, who has the private key, can decrypt the string.

1.1.1: Method of R.L.Rivest, A.Shamir, and L. Adleman for classical key distribution:

This key distribution is based on the difficulty of factorizing large integer numbers. First the message should be represented as an integer between 0 and n-1 and let us call this number M. (We can break messages in to the blocks of size n, and represent each block as a number between 1 and n). n is the product of two large secret prime numbers of p and q

$$(n=p*q).$$

Then rise M to the power of (e) and take the remainder of M^e over n (which is called C).

$$C \overset{n}{\equiv} M^e$$

Decryption is similar to the encryption but the secret, power d is used, which is defined bellow:

$$e.d \overset{(p-1)(q-1)}{\equiv} 1$$

Therefore the security of the system is related to the difficulty of factoring the published divisor, n. If we can factorize n, we can find p and q. By knowing p and q, we can find d. (Which is our secret key)

To understand better why this process transfers the information, the underlying mathematics is given bellow:

$$M^{\Phi(n)} \overset{n}{\equiv} 1$$

$\Phi(n)$ Is the Euler totient function, which is equal to the positive integer numbers less than n which are relatively prime to n. The value of this function for p and q are (p-1) and (q-1) respectively.

By using one of the properties of Euler totient function we can derive that

$$\Phi(n) = \Phi(p).\ \Phi(q) \text{ (It is the character of this kind of function)}$$
$$= (p-1)\ .\ (q-1) = n-(p+q)+1$$
$$e.d \overset{(p-1)(q-1)}{\equiv} 1 \Rightarrow e.d = (p-1)(q-1)*s+1 \text{ (s is coefficient)}$$

Now we can use the $M^{\Phi(n)} \equiv 1 \pmod n$ and $C \overset{n}{\equiv} M^{e}$.

$$(\text{Mod } n)\quad M^{\Phi(n)} \equiv 1 \Rightarrow M^{e.d} \overset{n}{\equiv} M$$

$$(M^{e})^{d} \overset{n}{\equiv} C^{d} \overset{n}{\equiv} M$$

Therefore by using d and n and C we can get M in decoding process.

For more information (Refer to R. Rivest, A. Shamir, and L. Adleman, *"On Digital Signatures and Public-Key Cryptosystems"*, MIT Laboratory for Computer Science)

1.2: Quantum key distribution:

We should use various mathematical techniques to restrict the third party from a successful attack in classical key distribution but in quantum cryptography the information is protected by the laws of physics. This secure system of communication uses the Heisenberg uncertainty principle as well as quantum entanglement. Heisenberg uncertainty says that measuring the value of one quantum observable implies an intrinsic uncertainty about the value of some other variables (such as position and momentum of particle). Entanglement means that two spatially separated quantum systems, which interacted with each other in the past, can share information in the form that this information can not be accessible just by measuring either of them alone.

Theoretical quantum cryptography was born in sixties when Stephan Wiesner wrote "Conjugate Coding" but unfortunately this paper was unpublished at that time and was announced several years later, when he met Gilles Brassard in occasion of the 20th IEEE symposium in October 1979.

This idea was published as public key cryptography in a Crypto paper ("Quantum cryptography or unforgeable subway tokens") . Initially quantum cryptography was thought as a science fiction work, because it seemed that the required technology was out of reach. For example the Weisner's method in his paper "Conjugate coding" need the ability to store a single polarized photon for days without important absorption or loss of polarization and it is clear that storing the polarized photon for days without any loss of polarization is nearly impossible.

It took time to realize that photons can be used to transmit the information and not for storing the information. The first experiment regarding the key distribution took place in 1989. (You can refer to "The dawn of a new era for quantum cryptography: the experimental prototype is working!" by Bennet, C. H. and G. Brassard)

Three main types of quantum cryptosystems that have been announced by the Cambridge center for quantum computing are as bellow:

1. Cryptosystems with encoding based on two non-commuting observables proposed by S.Wiesner (1970), and by C.H.Bennett and G.Brassard(1984) (refer to "Experimental quantum cryptography," J. Cryptology 5 , 3 (1992).). In this technique the photons are sent in two different conjugate bases (measuring in one basis will randomize the other one). The key distribution technique that is described in parts 2, 3, 4 of this this paper (my project) is related to this kind of cryptosystems.

2. Cryptosystems with encoding built upon quantum entanglement and the Bell theorem proposed by A.K.Ekert (1990). In this technique the Bells basis, which are entangled, are used for sending the information. (Refer to A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); A.K. Ekert, J.G. Rarity, P.R. Tapster, and G.M. Palma, Phys. Rev. Lett. **69**, 1293 (1992)). The part 5 of this paper (privacy amplification) is mostly related to this kind of cryptosystems. You can find more in the section 5-2 of this paper.

3. Cryptosystems with encoding based on two non-orthogonal state vectors proposed by C.H.Bennett (1992), (refer to P D. Townsend, J.G. Rarity, and P.R. Tapster, Electron. Lett. **29**, 1291 (1993).)

Bennete and his colleagues designed the first quantum key distribution channel but other researchers picked other areas near this subject such as: 1. Crepeau & Kilian general character of a quantum channel. 2. Ekert : Implementation of quantum key distribution. It should be noted that Ekert paper in 1991 is one of the most famous papers on key distribution and quantum cryptography.

2. **Background of Quantum key distribution:**

2.1: First simple model:

Alice and Bob want to distribute one secret key while they do not have any shared information. The third party, who is called"Eve", wants to get access to this secret key. It is assumed that the digital communication (Classical communication) can be passively monitored and Alice and Bob can not know of the existence of a third party (because it doesnot disturb the information). But in quantum key distribution, it is possible to create a channel, in which transition can not be read or copied by third party. (The monitoring results in disturbing the information.)

Heisenberg's uncertainty principle is the key of this kind of distribution. The two operators, which are not exchangeable (Meaning that you can not measure them at the same time in certainty or measuring one of them effects on the value of other one) , are used for this kind of cryptography. These two operators are the photon's linear and circular polarization. As we know from quantum theory if we observe one physical system with operator A while it is in the eigenstate of operator B, while $[A,B]\neq 0$ then we

have probabilistic observation of the other one. If this observation is completely randomize the other one, we will call those bases, conjugate bases.

The two concerned conjugate bases are rectilinear basis (horizontal and vertical polarization) and the circular basis (left circular and right circular). We call these two bases “canonical bases” that consist of 4 bases. We can define other basis consisting of 45 and 135 degree diagonal polarization, which are used in eavesdropping strategies.

One of the priorities of Quantum cryptography is that we can assume that the computer of Eve can solve the NP hard problem as well. (It means that the factorizing of large integer number can be done in polynomial order.)

The very basic method of quantum key distribution (QKD) has 4 main steps. First Alice sends a random sequence of photons, which are in 2 sets of bases and were introduced before. Second, Bob measures them randomly in one of the 2 sets of bases (4 bases). Third, Bob informs Alice (not secretly) what kind of operator he used. Fourth, Alice informs Bob about the correct basis. In this way Bob can discard all of the wrong bits, which he measured in wrong way.

If we declare this algorithm clearly and in more details it will be as bellow:

1. Alice sends a random sequence of photons which are polarized in horizontal or vertical or right-circular or left-circular bases. (In 2 different sets of conjugate bases)
2. Bob measures the received photons in one of the 2 sets of bases. So if he measures the photon in the same basis as Alice sent her information, his result is correct but if he measures in different bases his results will be completely random. (That is the exact definition of conjugate bases!).It should be mentioned that some photons may not be observed at all! (Because of the weak technology that has been used to detect or some other reasons!)
3. Bob tells Alice which kind of operator he used.
4. Alice informs him about the correct operator.

5. Now Bob and Alice can recognize what are the trustable data so they can keep the correct-measured photons and discard the incorrect-measured photons and the photons which are not observed at all.
6. This data now can be mapped to the sequence of 0 and 1 according to coding contract.

Bellow there is an example of the above 6 steps. I show the horizontally polarized by (-), vertical polarized by (|), right-circular polarized by (/) and left circular polarized by (\ ) and (+) and (X) are operators respectively measure in rectilinear and circular basis. Our mapping (level 6) is (|, \ = 1) and (- , / = 0):

Alice sends with:step1	+	X	+	+	X	X	+	+	X	X	+
Alice sends to Bob:step1	|	/	|	-	/	\	|	-	\	\	-
Bob measures with:step2	+	+	X	+	X	X	+	X	X	+	X
Bob's results: step 2	|	|	/	-	/	\	|	\	\	-	\
Valid data: step 3 and 4	|			-	/	\	|		\		
Translated to key: step 5,6	1			0	0	1	1		1		

2.2: Second algorithm, considering noise:

If they want to make this procedure safe against Eve's attacks, they should add some more steps to the above protocol. After those steps they should compare two sample parts of their final sets and check whether they are different or not. If Eve measures the photons while it transits from Alice to Bob it creates some amount of error depending on what kind of basis she uses. By checking the amount of error, Alice and Bob can recognize the existence of a third party (If the error is just Intercept/resent). I should mention that in this part it is assumed that the third party cannot corrupt the public messages. If he had this kind of ability, she could sit between them and change the messages in the way that she wants and in the end she could have 2 strings, one like Alice and one like Bob. (For more refer to "secure implementation of identification systems", by Bengio, S.,

G. Brassard, Y. Desmedt, C. Goutier and J. Quisquater, Journal of Cryptography, Vol. 4, no. 3, 1991).
This property of public channel can be produced by using an inherently un jammable public channel.

This basic method has some significant problems:

1. It is supposed that there is no noise while noise exists in every channel, so their shared parts are different without the measuring of a third party (By the effect of the noise).

2. It is supposed that each light beam consists of one photon, while it is so difficult to produce this kind of light. It is easier to make coherent light which is the superposition of different quantum states with different number of photons. If we assume that each light beam has (m) photon and this number is much lower than 1 (It means one photon is sent in every few steps) then we can say that the probability of splitting the pulse into two or more beams light by third party is lower than m×m/2. In this way Eve can get lots of information with creating any error.

The next protocol is the other simple protocol which does not have the above defects. In this protocol it is again assumed that Eve cannot make any corruption on the public messages and Eve listens to all of the messages.

First, Alice sends and Bob receives their messages in 4 bases but with very dim light instead of light which has only one photon. After these steps they should reconcile the differences in the way that a third party gets the least amount of information from their conversation. (Recall that, it is supposed that Eve listens to all of the messages and therefore disturb them.)

In order to distill the less information to Eve, we should declare less information in reconciliation process. So we should randomize the place of mistakes and in this way you can distribute errors in all of your string. For this purpose they should agree on random permutations of the bits in the sequence. In the next step they should find blocks with size

K that in average contains one error. For finding the best value for K we should know the expected error rate which is not easy to define theoretically. Most of the time the best way to find the error rate is that to find it experimentally!

After dividing the string into blocks of the size K, Alice and Bob compare the parity of their own blocks with each other. If the parities are not the same, the error should be found by the bisective search that takes time in order of log(K). After comparing the blocks, some errors still remain. If this error rate is high, we should change K into suitable value (We can check one subset of the string and find the proper K by that) but if it is low we can reduce errors by random permutation and comparing parity of blocks which are bigger sizes. After each comparison they discard the last bit of each block because they do not want to leak any information to Eve. But in this way many bits of information are scarified for security. If there are N blocks, and 2 errors remained, N bits will be scarified and the probability of finding the errors is $\frac{1}{N}$. So it is not a very good strategy. Therefore other strategies have been designed to reduce the rate of errors in the string. One of the regarding strategies eliminate N bits while the probability of remaining error decrease to 2^{-N} (in comparison with $\frac{1}{N}$). In this strategy they compare the parity of completely random subset of their string. The probability of two remaining errors in one subset is exactly 0.5.

After the following steps, Alice and Bob may reach the point where there is no error but they are not aware of their success so they should continue the comparisons for some more steps. If they do not find any difference in a few more steps they can stop their work.

As it is said above the rate of Eve's information can be calculated. It can be shown that If Eve's information about the string not worth more than N bits, her information after the reconciliation will be N parity bits about the shared information between Alice and Bob. (If it is said that Eve knows N parity bits it means that she knows the parity of N non empty subset of the shared string.)

In this step, we should use the privacy amplification that is proper for this kind of key distribution. Privacy amplification is a sort of error correction that allows the partners to map the similar shared random keys to shorter shared key, but in a completely confidential way.

Unfortunately I have not found the paper of "C.H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion" , SIAM Journal on Computing 17 (1988), 210--229. 14" to add more details about this kind of privacy amplification but it was claimed by the Paper of "Experimental Quantum Cryptography" (Which is my main reference for this part) that if Eve's knowledge about the shared string is less than L deterministic bits, we can use function H (hash function) that map N bits to N-L-S bits string that, Eve's information about that is less than $2^{-s}/\ln 2$ bit! That s is an arbitrary security parameters. (Parity bits are one kind of deterministic bits so this function works here too) The privacy amplification theorem shows that Eve knows nothing at all about the final string after Alice and Bob used Hash function. The amazing point about Hash function is that if there is a single difference between Alice and Bob's string before using the Hash function we will have a completely uncorrelated strings after using it!

3. Eaves dropping strategies:

We can categorize the main strategies of Eaves dropping as 1. Intercept/Resend, 2. Beam splitting. The aim of this part is to calculate the amount of information which is leaked to Eves by these two different Eaves dropping.

3.1: Intercept/Resend:

If there is m photon in each light beam and $m<<1$ then we can assumed the probability of detecting of the pulse is equal to m.

It is assumed that in the intercept and resend process, Eve has access to efficient detectors that she resends the photon in the same polarization as she detected. The intensity of resent photons should be the same as the initial photons. (To eliminate any suspicion)

In classical physics Eve can monitor any information without making any error and she can get all of the information. But in quantum cryptography can be proved that Eve can get the bits with probability $(2+\sqrt{2})/4 \approx 85\%$ and she creates error of at least 25% for each of her interferences.

It should be mentioned that the amount of information that Eve can get from this process depends strongly on what kind of basis Eve used. There are 2 choices for Eve, on one hand she can use canonical bases and find the deterministic information about the data. On the other hand she can use the Breidbart bases (half way between rectilinear and circular) and find every bit with a probability near 85%!

Even thought this basis gives less Shannon information (The type of information developed by Claude Shannon and Warren Weaver in the 1940s. Shannon information is concerned with quantifying information such as number of bits, to keep track of alphanumeric characters) to Eve in compare with canonical basis (40% in compare with 50%), it makes Alice and Bob throw away more information during the privacy amplification process in comparison to the situation where Eve uses canonical bases.

To prove the above claims regarding the percentage of information that Eve can gain and what is her maximum efficiency in that process, Q is defined as an arbitrary polarization state on the Poincare sphere by (X, Y, Z). X, Y, Z represent the rectilinear, diagonal and circular components respectively.

If we assume that this state is measured in P and –P basis, that they are two opposite points on the Poincare sphere, the probability of measuring Q in P direction is $\cos^2(\alpha/2) = (1+\cos\alpha)/2$. α represents the angle between Q and P on the Poincare sphere and the probability of measuring Q in –P has a complementary probability of $(1-\cos\alpha)/2$. It is obvious that if Q=P or Q=-P you can measure qubits completely precisely in those basis.

Two of the concerned three standard bases are canonical basis and the other one is diagonal basis. These bases are represented as followings: ($\pm 1, 0, 0$) represent the horizontal and vertical basis, ($0, \pm 1, 0$) related to 45 and 135 degree (diagonal), ($0, 0, \pm 1$) related to the left and right circular.

It is easy to understand that if we measure each of these states in the other basis the result will be absolutely random. It is the exact meaning of the conjugate basis.

Alice can send a photon in rectilinear basis, horizontal or vertical basis, ($\pm 1, 0, 0$) or circular basis ($0, 0, \pm 1$) and Eve measures it in {P,-P} direction and resend it in {P', -P'} direction. If Alice send them in horizontal basis (If it is in horizontal basis Eve should detect in it +P direction and if it is in vertical base Eve should detect it in –P direction and the other results are counted as an error. It means that +P and –P are mapped to horizontal and vertical direction respectively) it is clear that the error rate for Eve will be (1-X)/2 where X refers to ($\cos \alpha$) . If she sends them in circular basis ($0, 0, \pm 1$) the error will be (1-Z)/2. Therefore in average Eve gets information with the error rate near

$$\frac{1}{4}[(1-X) + (1-Z)].$$

If she wants to minimized her error, she should minimized [2-(X+Z)]. Therefore X+Z should me maximized and by considering the fact that $X^2+Y^2+Z^2=1$ (by omitting Y) we reach $X^2+Z^2=1$ so $X=Z=\sqrt{2}/2$. The error probability of Eve in this situation is $(2-\sqrt{2})/4 \approx 15\%$. This happens when Eve measure in the basis between rectilinear and circular basis, as was told before. This basis is called the Breidbart basis. (For more refer to "Quantum cryptography or unforgeable subway token" by Bennett, Brassard, Breidbart and Wiesner"")

It can be shown that Bob's error probability, when Alice sends her bits in rectilinear basis, is $\frac{1}{4}[(1-X)(1+X') + (1+X)(1-X')]$. And if Alice sends in circular basis, it is $\frac{1}{4}[(1-Z)(1+Z')+(1+Z)(1-Z')$. The average of above value is the average error of Bob.

$$\frac{1}{8}[(1-X)(1+X') + (1+X)(1-X')+(1-Z)(1+Z')+(1+Z)(1-Z')]$$

$$= \frac{1}{8}[(1-X+X'-XX') + (1+X-X'-XX') + (1-Z+Z'-ZZ') + (1+Z-Z'-ZZ')]$$

$$= \frac{1}{8}[2*(1-XX') + 2* (1-ZZ')]$$

$$= \frac{1}{4}[(1-XX') + (1-ZZ')]$$

The error rate of Bob is in minimum when (XX'+ZZ') is in a maximum point and it is clear that it happens when Y =Y'=0. Then we can write (XX'+ZZ') as bellow:

$$(XX'+ZZ')= (XX'+\sqrt{1-(X*X)}\ .\sqrt{1-(X'*X')}\ )$$

If we define X as Sin(α) and define X' as Sin(β) then:

$$= (\text{Sin}(\alpha)*\text{Sin}(\beta))+(\text{Cos}(\alpha)*\text{Cos}(\beta))$$

$$=(\text{Sin}(\alpha)*\text{Cos}(90-\beta))+(\text{Cos}(\alpha)*\text{Sin}(90-\beta))=\text{Sin}(90+\alpha-\beta)$$

So this sequence will be maximum when α=β and it implies that X=X' and Z=Z'.

Therefore Bob's error probability attains its minimum value of $(\frac{1}{4})$ when P=P and the basis is in the XZ plane (Y =0). In particular this can happen while Eve Intercepts/resends in either rectilinear, circular or Breidbart basis. As you can see from the above calculation Bob error will be more than $(\frac{1}{4})$, if $P \neq P'$ or if $Y \neq Y'$. In this way Eve will make more errors.

If Eve intercepts in the diagonal basis (0, ± 1, 0) regardless of her resending basis the error will become maximum as the bellow calculation show:

$$Y=\pm 1 \Rightarrow X=Z=0$$

$$\text{Bob's Error}= \frac{1}{4}[(1-XX') + (1-ZZ')] =\frac{1}{4}[2-XX'-ZZ']= \frac{1}{4}[2]= \frac{1}{2}$$

As we said above Eve creates error of at least $\frac{1}{4}$, but this is only true if Eve's measures every photon and her apparatus effects each of the photon which passes. If Eve measures P percent of photons, she will make at least (P/100)* $\frac{1}{4}$ of error in Bob's information bits.

If there are T errors in the string Alice and Bob can conservatively estimate the amount of the bits that have been intercepted/resent by calculating the upper limit for that. This upper limit is $4t+5\sqrt{12t}$, $5\sqrt{12t}$ is related to a five standard-deviation allowance. In order to understand exactly how this number came from you can refer to Appendix 2 of "Experimental Quantum Cryptography" the main reference of this project.[1] The information is gathered by Eve through this process will not worth more than $(4/\sqrt{2})\,t+5\sqrt{(4+2\sqrt{2})t}$. But it is clear that the noise or other problems has not been calculated here, for example the error can be made by optical misalignment or disturbance in the quantum channel. For calculating the precise amount of intercept/resend we should calculate the amount of errors which originate from other sources.

For this purpose the Alice and Bob measure the amount of errors in the absence of Eve. But this approach has some problems if Eve is clever enough to reduce those errors by using certain techniques.

3.2: Beam splitting:

As was said before, the transmitted light has *m* photon in each beam as most of the time it is hard to produce pure single photon states. Eve can use a partly silvered mirror to divert a fraction of the light beam for herself and allows the rest to be received by Bob, this fraction is called *f*. In this way Eve has an opportunity to measure them immediately but in this way she may loose some information by using wrong bases so she may wait until the moment that current basis will exposed by Alice. In this way, she can detect the

photon by probability of fm. The main feature of this kind of attack is that it does not produce any error but reduce the intensity by the factor of 1-m.

More realistically it is not very hard for Eve to store the light for a long time. If there is a chance for Eve to store the information for a long time, Alice and bob can wait for longer time before publicly inform each other about what the correct basis. In this way Eve can learn Alice's string in best point ($m/\sqrt{2}$.) The other problem that exists in current method is that most of the transportation system that can be used for photon transition has natural attenuation. In this way we can not be sure easily whether the light density has been reduced by third party or Noise.

Eve can use some more transparent channel and by this way she has an opportunity to allowing Bob to receive only pulses that she has splitted them. Anyway, here we assume that the high transparent optical channel is accessible. If their communication has N successful pulses, they can conservatively estimate the upper limit for Eve's information as Nm+5$\sqrt{Nm(1-m)}$. The second term is a 5 standard deviation allowance for lucky Eve!

4. Experimental quantum Key distribution:

Here I just talk briefly about the one of the first quantum experiment that has been done by Bennet, Bessette and Brassard, Salvail and Smolin in 1991.

In this experiment, they exchanged faint flashes of polarized light and distilled smaller part of this shared information after they had discussed about weather Eve interfered in the information or not. The third party's information (Eve) would be an exponentially (dramatically) small fraction of one bit!

This experiment was done by one IBM PC computer that had some separate software for Alice and Bob and optionally Eve. Alice and Bob's software communicate with each other just by a public channel.

Alice light source was on the left side of optical bench consisted of a green light emitting diode (LED Stanley type), a 25 micron pinhole and 25 mm focal length to form the collimated beam, a 550 ± 20 nm interference filter to reduce the intensity and spectral width of the light and Polarized filter to polarized beam horizontally. After the filtration and polarization intensity became 0.1 photon per pulse. This low intensity helps to minimize the chance of Eve to split the light.

Bob's receiving apparatus was on the right end of the optical bench, consisted of one Pockle cell and calcite Wollason prism, oriented so as to split the beam into beams which were vertically and horizontally splitted. Bob's pocket cell was operated at quarter wave voltage too. In this way he could use the same Wollaston prism to make a measurement of both rectilinear and circular basis depends on the voltage was on or off.

I do not want to talk much about this experiment but it is important to know that they used a 32 cm quantum channel that was far from an ideal quantum channel because we need secure key distribution for long distances. (We can transfer information directly to each other in close distance very easily!) To understand more you can refer to part three of reference number one.

Quantum cryptography based on polarization-based cryptography is now a mature technology. Many different prototypes and commercial devices are built. For example the apparatus bellow is made by the Geneva based company ID Quantique.

This photo was taken from Cambridge CQC, http://cam.qubit.org/articles/crypto/quantum.php

5. Privacy Amplification:

5.1. Introduction:

The bellow text reviews the privacy amplification papers that are about the general quantum key distribution. The privacy amplification technique, that is described bellow, is focused on the kind of quantum cryptography, which based on Bell's Theorem and not the one that we have described above.

The existing quantum cryptography techniques face problems in noisy channels, but they can be useable when they use classical privacy amplification techniques. In this part the quantum privacy amplification will be introduced and it will be proved that it is secure over a noisy channel.

Privacy amplification is a sort of cryptographic version of error correction. First, Alice and Bob have similar shared strings (bits of information) that Eve has some information about. But in end, they have a shorter shared identical key which is absolutely confidential.

This scheme is called 'entanglement purification' procedure and it just needs a single qubit operation as well as a few Controlled-Not. The technology of concerning gates has been provided already. This technique will put a small bound on the information that Eve can extract from the string.

As was said in part 2, Alice and Bob have access to a quantum communication channel as well as classical exchange channel. The classical channel can be potentially monitored but not disturbed by Eve. The security of this process depends strongly on other techniques (Privacy amplification) in the noisy channel. This problem comes from the fact that it not easy to recognize errors which were created by Eve and the errors which were made by noise.

In part 2 a technique was described, that does not need to recognize the source of errors (because we assume that the Eve listens to all messages) but in that technique we used some kinds of privacy amplification in the end. And some special function by the name of Hash 'H' was used, that maps the string to the smaller secret string. (It was not described in detail)

The classical privacy amplification can be used when we are completely confident about the security of the keys. (For more information regarding the classical privacy amplification you can refer to "Generalized privacy amplification" by Bennett, Brassard and Crepeau, Maurer.[9])

But the security of classical privacy amplification has been proved for a classical communication channel and a classical Eve. (I am not sure if these proofs complete or not?!). For example they do not cover the beam splitting case (Part 3.2) in which Eve has the ability to store photons and later measure them

In the technique which will be described bellow, Alice and Bob can produce the pairs of qubits near pure states and maximally entangled. They can produce this from any supply of pairs of qubits with non zero entanglement.

5.2: Quantum Cryptography based on Bell's Theorem:

The Ekert scheme uses entangled pairs of photons that can be produced by Alice or Bob or by some other sources. In any case they can have one of the qubits at the end of distribution. Bellow I describe this kind of key distribution very briefly and for more information refer you to [4].

Alice and Bob use three helpful properties of entanglement.

1. It is possible to make entangled states which are perfectly anti correlated. In this case if Alice and Bob both measure their particles in + (measure in rectilinear basis), if Alice result is (|) then bob result should be (-) and the reverse is true

too. This fact is true for any pair of complementary (orthogonal) polarized photons.

2. These kinds of states have a property that is usually called quantum non-locality. If Alice and Bob use different polarization their result are not completely anti-correlated but they will in general be statistically correlated. This implies that Alice's result is better than random guesses.

3. Eaves dropping will weaken these correlations. Therefore Eves dropping can be detected. (Whether, I am not sure this detection is valid for some other techniques, except intercept and resend, such as beam splitting)

Bells' bases are some pairs of entangled photons that can be used in this kind of key distribution:

$$|\phi^{\pm}>= \frac{1}{\sqrt{2}}(|00>\pm|11>)$$

$$|\Psi^{\pm}>= \frac{1}{\sqrt{2}}(|01>\pm|10>)$$

Alice and Bob gain one qubit from each pair. If there is noise in the system each pair may be entangled with other pairs and with the environment. These pairs are described by density operators.

There is a channel that consists of a source that emits these pair of particles in z axis toward Alice and Bob. They measure their particles after the particles have separated in Ai and Bi axis respectively. It is supposed that Ai and Bi are in X-Y plane, perpendicular to the trajectory of the particle.

We can describe the Ai and Bi by azimuthal angels that are measured from the vertical x axis.

θ_1^a=0, θ_2^a=45, θ_3^a=90 and θ_1^b=45, θ_2^b=90, θ_3^b=135

(a) refers to Alice and (b) refers to Bob.

Then Alice and Bob choose the orientation of their detector randomly. Each measurement in $\frac{\hbar}{2}$ units can yield +1, -1 regarding the up and down spin.

The correlation coefficient of the measurement is calculated by

$$E(Ai,Bi)=P{+}{+}(Ai,Bi) + P{-}{-}(Ai,Bi) - P{+}{-}(Ai,Bi) - P{-}{+}(Ai,Bi),$$

Here $P\pm\pm(Ai,Bi)$ represents the probability that results ± 1 has been detected along Ai and ± 1 has been obtained along Bi.

After transition they will announce their orientation of their measurer through public channel. They discard all the qubits, which one of the qubit was not successful enough to be measured. If they use the same orientation, it is okay to announce their measurement by public channel. This ability will allow them to be assure that their basis are anti correlated and therefore can be used as information.

The Eve cannot elicit any information from particles, which are in transitted because there is no encoded information there. Only after Alice and Bob measure them and announce it in public the information will come out. If Eve sends the qubits by herself she will not be successful enough because she does not know which orientation will be used for measuring.

You can refer to "Quantum Cryptography Based on Bell's Theorem" by Artur K. Ekert, Physical Review Letters, Volume 67, Num. 6, August 1991. [4]

5.3: Privacy amplification for Ekert's model:

This scheme is based on the iterative quantum algorithm which is started with a collection of qubit pairs in mixed states. Select some of them and start to converge them to $|\Phi^+><^+\Phi|$. (I should mention again that here we use a density matrix, therefore the density matrix will converge to the above amount). If the algorithm is not used perfectly it will fluctuate in the neighborhood of the above amount.

As we told in part 2 for considering noise we should assume that Eve interacts with all of the qubits that are sent or received by Alice and Bob.

We consider the case in which Eve has the ability to make qubits pairs as well. In this case Eve can make two qubits pairs by her own desire and send one qubit from each pair to each of Alice and Bob. (This kind of error was not talked about in the original Ekert paper regarding using Bell's theorem for key distributing [4].)

We define ρ and ρ' as density matrixes of Alice and Bob respectively

Now we want to find specific procedure that map the density matrix of ρ to new density matrix, which has bellow character:

$$\begin{bmatrix} A,0,0,0 \\ 0,B,0,0 \\ 0,0,C,0 \\ 0,0,0,D \end{bmatrix} \Rightarrow \begin{bmatrix} (A^2+B^{2)}/N,0,0,0 \\ 0,2(CD)/N,0,0 \\ 0,0,(C^2+D^2)/N,0 \\ 0,0,0,2AB/N \end{bmatrix}$$

Where $N=(A+B)^2+(C+D)^2$

It should be mentioned that above matrix was written in bell states therefore

$$A=<\phi^+|\rho|\phi^+>,\ B=<\psi^-|\rho|\psi^->,\ C=<\psi^+|\rho|\psi^+>,\ D=<\phi^-|\rho|\phi^->$$

This procedure consists of two rotations and a controlled not. As you may know the qubits are spin $\frac{1}{2}$ particles and the computation bases are the eigenvalue of the z components of the spins. The two rotations are +90 and -90 degree rotation about the x axis the first one is for Alice and the other one is for Bob. These rotations can be calculated as:

$$\text{Exp}(-I.(\pm(90/2))X)=\text{Cos}(\pm(90/2)).I - i.\text{Sin}(\pm(90/2)).X \quad (X \text{ is Pauli matrix})$$
$$= \text{Cos}(\pm 45).(|1><1|+|0><0|)-i.\text{Sin}(\pm 45).(|0><1|+|1><0|)$$

For Alice is: $\frac{1}{\sqrt{2}}(|1><1|-i.|1><0|-i.|0><1|+|1><1|)$

And for Bob is: $\frac{1}{\sqrt{2}}(|1><1|+i.|1><0|+i.|0><1|+|1><1|)$

After above steps, each of Alice and Bob should use the quantum Controlled-Not operation:

$$|0><0| \otimes I+|1><1| \otimes X \Rightarrow$$
$$\text{Controlled-Not } |a>|b>=|a>|a \oplus b> \quad \{a, b\} \in \{0,1\}$$

We call the first bit control and the second bit target bit but if we want the operation that the first bit works as target and the second bit acts as control bit we should use this kind of controlled not gate: $I \otimes |0><0|+X \otimes |1><1|$ (To find more about various interesting functions of Controlled-Not you can refer to "Conditional Quantum Dynamics and Logic Gates", Phys. Rev. Lett. Vol. 74, No. 20, pp 4083-4086 (1995)

As I understand from the paper of "Quantum privacy amplification and the security of quantum cryptography over noisy channels"[2] after using the two above rotations Alice and Bob should perform two instance quantum controlled-Not operation. One ρ comprise two control qubits and the ρ' comprise the two target qubits. Then they measure the target qubits in the X, Y, Z basis. If the results coincide they will continue with the controlled pair and omit the target bits otherwise they discard both pairs.

It should be mentioned that, if you want to calculate the above matrixes (to use them in calculating the final density matrix) you should bring them to Bells' bases. You can change the matrix from rectilinear bases to Bell's basis just by using a Hadamard gate.

Now ρ will change to:

$$\begin{bmatrix} (A^2 + B^{2)} / N,0,0,0 \\ 0,2(CD)/N,0,0 \\ 0,0,(C^2 + D^2)/N,0 \\ 0,0,0,2AB/N \end{bmatrix} = \begin{bmatrix} A',0,0,0 \\ 0,B',0,0 \\ 0,0,C',0 \\ 0,0,0,D' \end{bmatrix}$$

Where N= $(A+B)^2$ +$(C+D)^2$ is the probability that whether, Alice and Bob's results on the target bits are the same or not.

It is completely clear that the density matrix should have trace equal to one so we have 3 independent parameters in the density matrixes.

In the following, it will be proved that QPA (Quantum privacy amplification) will map a ρ which has A>0.5 to the pure state:

$$\begin{pmatrix} 1,0,0,0 \\ 0,0,0,0 \\ 0,0,0,0 \\ 0,0,0,0 \end{pmatrix}$$

This matrix can be shown as {1, 0, 0, 0} also.

It means that the result is in the completely pure state. That claim will be proved by proving these two following assertion

1. Find the function that increases in the region R = {A ∈ {0.5,1], B, C, D ∈ [0,0.5}, A+B+C+D=1}
2. The extreme value of this function (defined in the above statement) in the above region corresponds to the {1, 0, 0, 0}

The above statements mean that the point {1, 0, 0, 0} is an attracter in the region of interest.

The first function that can be imagined for this purpose is A, because it will be maximized in {1, 0, 0, 0}. But in this case it faces problems in the first condition. It means that A' (The second value of density matrix) is not always bigger than A and it will not increase by each iteration. There are some cases that the following function works well. For example you can see "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels" by Bennett, Brassard, Popescu, B. Schumacher, Smolin and Wootters.

The function that is assumed in this text has quadric form.

$$F(A,B)=(2A-1)(1-2B)$$

It is obvious that above function depends on just 2 variables of 3. (We have 3 independent variables)

First it will be showed that in each step this function will be increased (If A>0.5 then therefore B, C and D are < 0.5). It means that: $F(A',B') > F(A,B)$

And then it will be shown that if the initial values of the density matrix belongs to the concerned region it will stay there by the QPA steps, because if it is possible for it to jump out from this region, we can not prove that it will converge to {1, 0, 0, 0}.

For first aim we will calculate $F(A',B')-F(A,B)$

$$F(A',B')-F(A,B)=(2A'-1)(1-2B')-(2A-1)(1-2B)$$
$$=(2((A+B)^2/N)-1)(1-(2CD/N))-(2A+2B-4AB-1)$$
$$=(((A+B)^2-(C+D)^2)/N)-(2CD((A+B)^2-(C+D)^2)/N^2)>0$$
$$(A+B+C+D)=1$$

If we continue this algebra we will reach this equation:

$$Y=2(C+D)^4-4(C+D)^3+4(C+D)^2-(C+D)-(C^2+D^2)<0$$

To prove the above equation we will show first that Y is negative on the boundaries of the region and then we will show that its derivative is zero just in one point of this area and this point is a Minimum. It should be shown that by each iteration, the function still remains in the previous area (Does not jump out):

$$(C+D)=P \text{ and } (C-D) =Q$$

$$\text{then, } 2Y=4P^4-8P^3+8P^2-2P-(P^2+Q^2)$$

$$=4P^4-8P^3+7P^2-2P-Q^2$$

On the boundaries (C+D) = 0.5 or (C+D) =0. The value of the above function is not positive as it is shown bellow $\Rightarrow$

$$P=0.5 \Rightarrow 2Y=0.25-1+1.75-1-Q^2=-Q^2<0$$

$$P=0 \Rightarrow 2Y=0$$

For finding the extreme point we should calculate two partial derivatives and equal them to zero:

$$\frac{\partial y}{\partial P}=+8P^3-12P^2+7P-1=0$$

The second derivation of Y is always positive. Therefore the above equation just has one answer. That answer is P=0.205122. The other derivative of Y with respect to Q should be zero therefore Q=0 and so C=D.

The value of Y in its extreme is -0.17, which is negative. It illustrates that, this value is the minimum of that function. Therefore the value of Y in the interior part of the region is lower than its value on the boundaries so Y is negative in the entire region. It is proved that F is increased by every QPA step.

On the other hand:

$$1-2A'=1-2(A^2+B^2)/N=(N-2(A^2+B^2))/N=((A+B)^2+(C+D)^2-2(A^2+B^2))/N$$

$$=((A+B)^2+(1-(A+B))^2-2(A^2+B^2)/N=(1+2(A+B)^2-2(A+B)-2(A^2+B^2))/N$$

$$=(1+4AB-2(A+B))/N=((2A-1)(2B-1))/N$$

$$\text{So } 1-2A'=((2A-1)(2B-1))/N$$

So if A>0.5 $\Rightarrow$ B<0.5, this shows that the right side of the equation is negative, therefore A' will be higher than 0.5. This means that after each iteration, A' will be more than 0.5 again.

It should be proved that the extreme value of F in the concerned region corresponds to the {1, 0, 0, 0}, by showing that:
F(A,B)=-1-4AB+2(A+B), it is clear that A and B are positive and $(A+B) \leq 1$ therefore $F(A,B) \leq -1-4(0)+2=1$ that the equality is valid for {1,0,0,0}

Therefore by iterating the QPA map the pair approach to its pure state ϕ^+.

It is obvious that the bellow parameters exchanges do not effect on the above result (The QPA iteration is symmetric under the following exchange)

$$A \Leftrightarrow C$$

$$\&$$

$$B \Leftrightarrow D$$

This implies that the result is valid for C>0.5. So if C> (0.5), after the sufficient number of QPA steps it will converge to {0, 0, 1, 0}

The QPA iteration seems to be also symmetric under changing $A \Leftrightarrow B$ or $C \Leftrightarrow D$ but the equation: 1-2A'= ((2A-1)(2B-1))/N is not symmetric under the changing A and B. It is clear from above equation that, if B>0.5, A' will be more than 0.5 (remain in the region) after iteration and it will converge to {1, 0, 0, 0}. This result is valid for D too. It means that if D>0.5, F will converge to {0, 0, 1, 0}.

Now I want to show that what will happen, if A, B, C and D are smaller than 0.5. It can be obtained from 1-2A'= ((2A-1)(2B-1))/N that if A and B are smaller than 0.5, then A' will be less than 0.5. (Paying attention that N is positive) On the other hand:

$$1-2B'=1-4CD/N=1-4CD/N= (N-4CD)/N$$

$$= ((A+B)^2+(C+D)^2-4CD)/N=((1-C-D)^2+(C+D)^2-4CD)/N$$

$$(C-D)^2 \geq 0 \Rightarrow C^2+D^2 \geq 2CD \Rightarrow (C+D)^2 \geq 4CD$$

Therefore the previous expression is always positive except for C=D=0.5

So if C and D are smaller than 0.5, B' will be smaller than 0.5 too. From the above calculation we conclude that if A, B, C, D are smaller than 0.5 then A' and B' will be smaller than 0.5, too. On the other hand

$$A \Leftrightarrow C \;\&\; B \Leftrightarrow D$$

So if A, B, C, D are smaller than 0.5 then A', B', C' and D' will be smaller than 0.5, too. And they will not converge to pure states.

If the input pairs have different density matrixes, the ρ and ρ' will be different. ρ corresponds to {A, B, C, D} and ρ' corresponds to $\{A_s, B_s, C_s, D_s\}$. Then the retained control pairs will be on average in this kind of matrix:

$$\{(AA_s+BB_s)/N, (C_sD+CD_s)/N, (CC_s+DD_s)/N, (AB_s+A_sB)/N\}.$$

Assume Eve has L pairs of qubits with different density matrices. Alice and Bob do not have any idea about the states preparation, which are prepared by Eve.

In this step, Alice and Bob select randomly from the prepared pairs and then use QPA procedures.

As was shown by lots of calculation, QPA is able to purify a collection of pairs in any state ρ which has at least one maximally entangled state. As was shown in previous part it should be one x exists that $\langle x|\rho|x\rangle > 0.5$

In end it should be noted that the above QPA procedure is wasteful in terms of eliminating particles (Therefore information). In each of the iteration at least one half of the particles is lost.

References:

[1] Charles H. Bennet, Francois Bessette, Gilles Brassard, Louis Salvail, John Smolin, "Experimental Quantum Cryptography", *J. of Cryptology* **5**, 3 (1992

[2] David Deutsch, Artur Ekert, Richard Jozsa, Chiara Macchiavello, Sandu Popescu, Anna Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channel", quant-ph/9604039, 30 April 1996

[3] Chiara Macchiavello, "On the analytical convergence of the QPA procedure", quant-ph/9807074 v1, 27 July 1998

[4] Artur K. Ekert, "Quantum cryptography based on Bell's theorem", Physical Review Letters, Volume 67, 1991

[5] Internet text by Carolina Moura Alves, Adrian Kent, "The key distribution problem", Cambridge Center for Quantum Computation, http://cam.qubit.org/articles/crypto/quantum.php

[6] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Comm. of the ACM, 21, no. 2:120-126, 1978

[7] Internet text by Artur K. Ekert, "What is quantum cryptography", last updated March 20, 1995, Cambridge Center for Quantum Computation, http://cam.qubit.org/articles/intros/crypt.php

[8] Michael A. Nielsen, Isaac L. Chuang, "Quantum computation and quantum information", ISBN 0-521-63503-9, Cambridge press, 2000

[9] Charles H. Bennet, Gilles Brassard, Claude Crepeau, Ueli M. Maurer, "Generalized Privacy Amplification", May 31, 1995

[10] Daniel Gottesman, Seminar on "Introduction to Quantum Cryptography" on Oct. 28 in Guelph university.