IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 3 Issue 11 November, 2015

Quantum Cryptography: A new Approach for Information Security

Debasish Hati[1]; Souradeep Sarkar[2]; Prasun Kr. Mitra[3]

Lecturer, Technique Polytechnic Institute, Hooghly, West Bengal, India[1]
Lecturer, Technique Polytechnic Institute, Hooghly, West Bengal, India[2]
Lecturer, Technique Polytechnic Institute, Hooghly, West Bengal, India[3]
debasishhati2013@gmail.com[1];souradeep_sarkar@rediffmail.com[2];mitra.prasun@gmail.com[3]

ABSTRACT

Quantum cryptography is the art and science of exploiting quantum mechanical properties to perform cryptographic tasks. It is a technology that ensures ultimate security. Compared to current cryptography that could be defeated by the development of an ultra high-speed computer, quantum cryptography ensures secure communication because it is based on the fundamental physical laws. It is an emerging technology in which two parties may simultaneously generate shared, secret cryptographic key material using the transmission of quantum states of light. Quantum cryptography is a new method for secret communications offering the ultimate security assurance of the inviolability of a Law of Nature. The quantum cryptography relies on two important elements of quantum mechanics-the Heisenberg Uncertainty principle and the principle of photon polarization.

Keywords: Quantum cryptography, network security, Quantum key distribution (QKD).

1. INTRODUCTION

In our modern age of telecommunications and the Internet, information has become a precious commodity. Sometimes it must therefore be kept safe from stealing - in this case, loss of private information to an eavesdropper. In the history of cryptography, It is a recent technique that can be used to ensure the confidentiality of information transmitted between two parties, usually called Alice and Bob, by exploiting the counterintuitive behaviour of elementary particles such as photons.

The main aim of cryptography is to protect data transferred in the likely presence of an enemy. A cryptographic transformation of data is a procedure by which plaintext data is encrypted, resulting in a modified text, called cipher text, that does not expose the original input. The cipher text can be reverse-altered by a designated recipient so that the original plaintext can be recaptured. The techniques of cryptography are usually categorized as traditional or modern. Traditional techniques use operations of coding i.e. use of alternative words or phrases, transposition i.e. reordering of plaintext, and substitution i.e. alteration of plaintext characters). Whereas, modern techniques use computers, and depends upon extremely long keys, convoluted algorithms, and intractable problems to achieve assurances of security. There are two main fields of modern cryptographic techniques: Public key encryption and Secret key encryption. A public-key encryption, in which a message is encrypted with a recipient's public key. The message cannot be decrypted by anyone who does not possess the matching private key, who is thus presumed to be the owner of that key and the person associated with the public key. A secret key is an encryption key known only to the party or parties that exchange secret messages. The risk in this system is that if either party loses the key or it is stolen, the system is broken. The development of quantum cryptography was encouraged by the short-comings of classical cryptographic methods, which can be divided as either "public-key" or “secret-key" methods. Quantum cryptography is an approach to a cryptography based on the laws of quantum physics.

Quantum cryptography is an attempt to allow two users to communicate using more secure methods than those guaranteed by traditional cryptography. Traditionally, cryptographic security relied on mathematics and took into account the limited computation powers that we have developed. Breaking a cryptographic code would involve factoring extremely large numbers into two primes, typically of over 100 digits in length, which was assumed to be impossible in a reasonable amount of time (less than a million years) even if all of the available computers today worked exclusively on one

such problem. However, just because there is no algorithm efficient enough to do the factoring quickly, does not mean that such an algorithm could not be found eventually. Quantum cryptography, which uses photons and relies on the laws of quantum physics instead of "extremely large numbers," is the cutting edge discovery which seems to guarantee privacy even when assuming eavesdroppers with unlimited computing powers.

2. LITERATURE REVIEW

The first application of quantum information theory was found by Wiesner in the early 1970s. He proposed using the spin of particles to make unforgivable bank notes. Roughly speaking, the spin of a particle obeys the uncertainty principle: an observer cannot get all the information about the spin of a single particle; he would irreversibly destroy some part of the information when acquiring another part. By encoding identification information on bank notes in a clever way using elementary particles, a bank can verify their authenticity by later checking the consistency of this identification information. At the atomic scale, the forger cannot perfectly copy quantum information stored in the elementary particles; instead, he will unavoidably make mistakes. Simply stated, copying the bank note identification information is subject to the uncertainty principle, and thus a forgery will be distinguishable from a legitimate bank note.

The plan was issued in 1983 in Sigact News, and at the same time two scientists Bennet and Brassard, familiar with the idea of Weisner, were ready to issue their own ideas. Then in 1984, they delivered the first quantum cryptography protocol called the "BB84." The protocol is provably secure, depending on the quantum property that information gain is only possible at the expense of disturbing the signal if the two states we are trying to distinguish are not orthogonal. The first experimental prototype based on this was made in 1991. It functioned over a distance of 32 centimetres. Over time, the technology has been improved and the distance extended to kilometres. Later on in June 2004, The first computer network in which communication is secured with quantum cryptography is up and running in Cambridge, Massachusetts. The leader of the quantum engineering team at BBN Technologies in Cambridge, Chip Elliott, transmitted the first packets of data across the Quantum Net. After that, a team at the University of Vienna transferred entangled photons across the river Danube, through free space in June 2003. In April 2004, the first money transfer encrypted by quantum keys occurred between two Austrian banks. The two buildings were 500 meters away from each other, yet fibre optics was fed through 1.5 kilometres of sewage system to link them together.

3. QUANTUM KEY DISTRIBUTION

As already mentioned, quantum key distribution (QKD) is a technique that allows two parties, conventionally called Alice and Bob, to share a common secret key for cryptographic purposes. In this section, I wish to give a general idea of what QKD is and the techniques it involves. The concepts will be covered in more details in the subsequent chapters.

To ensure the confidentiality of communications, Alice and Bob agree on a common, yet secret, piece of information called a key. Encryption is performed by combining the message with the key in such a way that the result is incomprehensible by an observer who does not know the key. The recipient of the message uses his copy of the key to decrypt the message.

Let us insist that it is not the purpose of QKD to encrypt data. Instead, the goal of QKD is to guarantee the secrecy of a distributed key. In turn, the legitimate parties may use this key for encryption. The confidentiality of the transmitted data is then ensured by a chain with two links: the quantum-distributed key and the encryption algorithm. If one of these two links is broken, the whole chain is compromised; hence we have to look at the strengths of both links.

First, how is the confidentiality of the key ensured? The laws of quantum mechanics have strange properties, with the nice consequence of making the eavesdropping detectable. If an eavesdropper, conventionally called Eve, tries to determine the key, she will be detected. The legitimate parties will then discard the key, while no confidential information has been transmitted yet. If, on the other hand, no tapping is detected, the secrecy of the distributed key is guaranteed.

As the second link of the chain, the encryption algorithm must also have strong properties. As explained above, the confidentiality of data is absolutely guaranteed if the encryption key is as long as the message to transmit and is not reused for subsequent messages. This is where quantum key distribution is particularly useful, as it can distribute long keys as often as needed by Alice and Bob.

Let us detail further how QKD works. Quantum key distribution requires a transmission channel on which quantum carriers are transmitted from Alice to Bob. In theory, any particle obeying the laws of quantum mechanics can be used. In practice, however, the quantum carriers are usually photons, the elementary particle of light, while the channel may be an optical

fiber (e.g., for telecommunication networks) or the open air (e.g., for satellite communications).

In the quantum carriers, Alice encodes random pieces of information that will make up the key. These pieces of information may be, for instance, random bits or Gaussian-distributed random numbers, but for simplicity of the current discussion, let us restrict ourselves to the case of Alice encoding only zeroes and ones. Note that what Alice sends to Bob does not have to – and may not – be meaningful. The whole point is that an eavesdropper cannot predict any of the transmitted bits. In particular, she may not use fixed patterns or pseudo-randomly generated bits, but instead is required to use "truly random" bits.

During the transmission between Alice and Bob, Eve might listen to the quantum channel and therefore spy on potential secret key bits. This does not pose a fundamental problem to the legitimate parties, as the eavesdropping is detectable by way of transmission errors. Furthermore, the secret-key distillation techniques allow Alice and Bob to recover from such errors and create a secret key out of the bits that are unknown to Eve.

After the transmission, Alice and Bob can compare a fraction of the exchanged key to see if there are any transmission errors caused by eavesdropping. For this process, QKD requires the use of a public classical authenticated channel, as depicted in Fig. 1.1. This classical channel has two important characteristics, namely, publicans and authentication. It is not required to be public, but if Alice and Bob had access to a private channel, they would not need to encrypt messages; hence the channel is assumed to be public. As an important consequence, any message exchanged by Alice and Bob on this channel may be known to Eve. The authentication feature is necessary so that Alice and Bob can make sure that they are talking to each other.

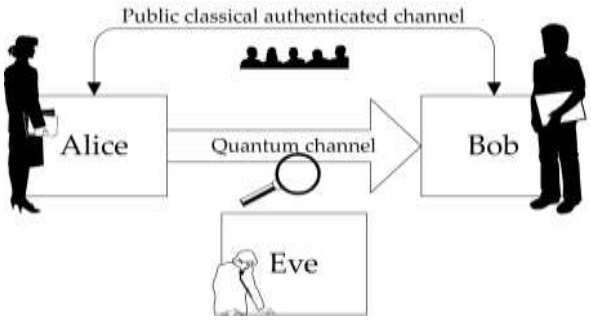

Figure 1.1: Quantum key distribution comprises a quantum channel and a public classical authenticated channel. As a universal convention in quantum cryptography, Alice sends quantum states to Bob through a quantum channel. Eve is suspected of eavesdropping on the line.

3.1 Encoding random bits using qubits

Any message can, at some point, be converted into zeroes and ones. In classical information theory, the unit of information is therefore the bit, that is, the set {0,1}. The quantum carriers of BB84, however, cannot be described in classical terms, so we have to adapt our language to this new setting.

There is a correspondence between the quantum state of some physical system and the information it carries. Quantum states are usually written using Dirac's notation, that is, with a symbol enclosed between a vertical bar and an angle bracket, as in $|\psi\rangle$, $|1\rangle$ or $|x\rangle$; quantum pieces of information follow the same notation.

In quantum information theory, the unit of information is the qubit, the quantum equivalent of a bit. Examples of physical systems corresponding to a qubit are the spin of an electron or the polarization of a photon. More precisely, a qubit is described by two complex numbers and belongs to the set

$$\{\alpha|0\rangle +\beta|1\rangle : |\alpha|2+|\beta|2=1,\alpha,\beta\in C\}, \quad (1.1)$$

with $|0\rangle$ and $|1\rangle$ two reference qubits, corresponding to two orthogonal states in a quantum system. The qubits $|0\rangle$ ($\alpha=1,\beta=0$) and $|1\rangle$ ($\alpha=0,\beta=1$) may be thought of as the quantum equivalent of the bits 0 and 1, respectively. For other values of α and β, we say that the qubit contains a superposition of $|0\rangle$ and $|1\rangle$. For instance, the qubits $2\text{-}1/2|0\rangle +2\text{-}1/2|1\rangle$ and $\sin\pi/6|0\rangle +i\cos\pi/6|1\rangle$ are both superposition's of $|0\rangle$ and $|1\rangle$, albeit different ones.

In BB84, Alice encodes random (classical) bits, called *key elements*, using a set of four different qubits. The bit 0 can be encoded with either $|0\rangle$ or $|+\rangle =2\text{-}1/2|0\rangle +2\text{-}1/2|1\rangle$. The bit 1 can be encoded with either $|1\rangle$ or $|-\rangle =2\text{-}1/2|0\rangle -2\text{-}1/2|1\rangle$ – note the difference in sign. In both cases, Alice chooses either encoding rule at random equally likely. Then, she sends a photon carrying the chosen qubit to Bob.

When the photon arrives at Bob's station, he would like to decode what Alice sent. For this, he needs to perform a *measurement*. However, the laws of quantum mechanics prohibit Bob from determining the qubit completely. In particular, it is impossible to determine accurately the coefficients α and β of the received qubit $\alpha|0\rangle +\beta|1\rangle$. Instead, Bob must choose a pair of *orthogonal* qubits and perform a measurement that distinguishes only among them. We say that two qubits, $|\varphi\rangle =\alpha|0\rangle +\beta|1\rangle$ and $|\psi\rangle =\alpha'|0\rangle +\beta'|1\rangle$, are

orthogonal iff $\alpha\alpha'^*+\beta\beta'^*=0$.

Let us take for instance the qubits $|0\rangle$ and $|1\rangle$, which are orthogonal. So, Bob can make a measurement that distinguishes whether Alice sends $|0\rangle$ or $|1\rangle$. But what happens if she sends $|+\rangle$ or $|-\rangle$? Actually, Bob will obtain a result at random! More generally, if Bob receives $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ he will measure $|0\rangle$ with probability $|\alpha|2$ and $|1\rangle$ with probability $|\beta|2$ – remember that $|\alpha|2+|\beta|2=1$. In the particular case of $|+\rangle$ and $|-\rangle$, Bob will get either $|0\rangle$ or $|1\rangle$, each with probability 1/2. Consequently, Bob is not able to distinguish between $|+\rangle$ and $|-\rangle$ in this case and gets a bit value uncorrelated from what Alice sent.

So, what is so special about the qubits $|0\rangle$ and $|1\rangle$? Nothing! Bob can as well try to distinguish any pair of orthogonal states, for instance $|+\rangle$ and $|-\rangle$. Note that $|0\rangle$ and $|1\rangle$ can be equivalently written as $|0\rangle = 2\text{-}1/2|+\rangle + 2\text{-}1/2|-\rangle$ and $|1\rangle = 2\text{-}1/2|+\rangle - 2\text{-}1/2|-\rangle$. Hence, in this case, Bob will perfectly decode Alice's key element when she sends $|+\rangle$ and $|-\rangle$, but he will not be able to distinguish $|0\rangle$ and $|1\rangle$. An example of transmission is depicted in Fig. 1.2.

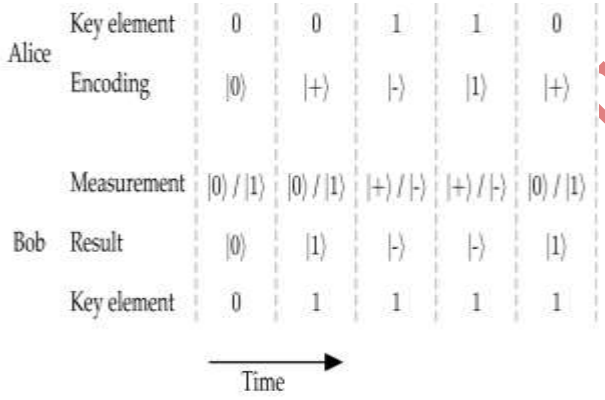

Figure 1.2: Example of transmission using BB84. The first two rows show what Alice sends. The bottom rows show the measurement chosen by Bob and a possible result of this measurement.

In the BB84 protocol, Bob randomly chooses to do either measurement. About half of the time, he chooses to distinguish $|0\rangle$ and $|1\rangle$; the rest of the time, he distinguishes $|+\rangle$ and $|-\rangle$. At this point, Alice does not reveal which encoding rule she used. Therefore, Bob measures correctly only half of the bits Alice sent him, not knowing which ones are wrong. After sending a long stream of key elements, however, Alice tells Bob which encoding rule she chose for each key element, and Bob is then able to discard all the wrong measurements; this part of the protocol is called the sifting, which is illustrated in Fig. 1.3.

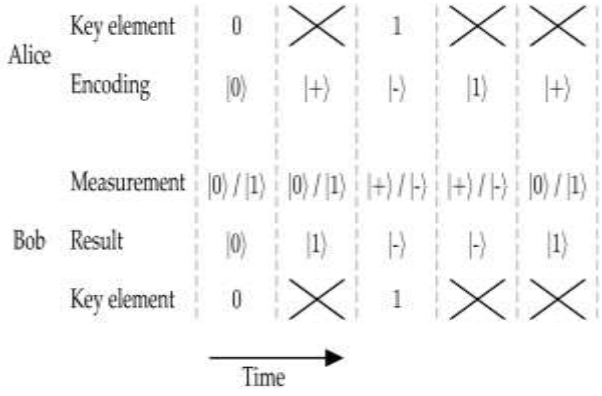

Figure 1.3: Sifting of the transmission of Fig. 1.2. The key elements for which Bob's measurement does not match Alice's encoding rule are discarded.

To summarize so far, I have described a way for Alice to send random bits to Bob. Alice chooses among four different qubits for the encoding (two possible qubits per bit value), while Bob chooses between two possible measurement procedures for the decoding. Bob is not always able to determine what Alice sent, but after sifting, Alice and Bob keep a subset of bits for which the transmission was successful. This transmission scheme allows Alice and Bob to detect eavesdropping, and this aspect is described next.

3.2 Detecting eavesdropping

The key feature for detecting eavesdropping is that the information is encoded in non-orthogonal qubits. Eve can, of course, intercept the quantum carriers and try to measure them. However, like Bob, she does not know in advance which set of carriers Alice chose for each key element. Like Bob, she may unsuccessfully distinguish between $|0\rangle$ and $|1\rangle$ when Alice encodes a bit as $|+\rangle$ or $|-\rangle$, or vice versa.

In quantum mechanics, measurement is destructive. Once measured, the particle takes the result of the measurement as a state. More precisely, assume that an observer measures a qubit $|\varphi\rangle$ so as to distinguish between $|0\rangle$ and $|1\rangle$. After the measurement, the qubit will become either $|\varphi\rangle \rightarrow |\varphi'\rangle = |0\rangle$ or $|\varphi\rangle \rightarrow |\varphi'\rangle = |1\rangle$, depending on the measurement result, *no matter what* $|\varphi\rangle$ *was*! In general, the qubit after measurement $|\varphi'\rangle$ is not equal to the qubit before measurement $|\varphi\rangle$, except if the qubit is one of those that the observer wants to distinguish (i.e., $|0\rangle$ or $|1\rangle$ in this example).

Every time Eve intercepts a photon, measures it and sends it to Bob, she has a probability 1/4 of introducing an error between Alice's and Bob's bits. Let us break this down. Eve has a probability 1/2 of measuring in

the right set. When she does, she does not disturb the state and goes unnoticed. But she is not always lucky. When she measures in the wrong set, however, she sends the wrong state to Bob (e.g., $|+\rangle$ or $|-\rangle$ instead of $|0\rangle$ or $|1\rangle$). This situation is depicted in Fig. 1.4. With the wrong state, Bob will basically measure a random bit, which has a probability 1/2 of matching Alice's bit and a probability 1/2 of being wrong.

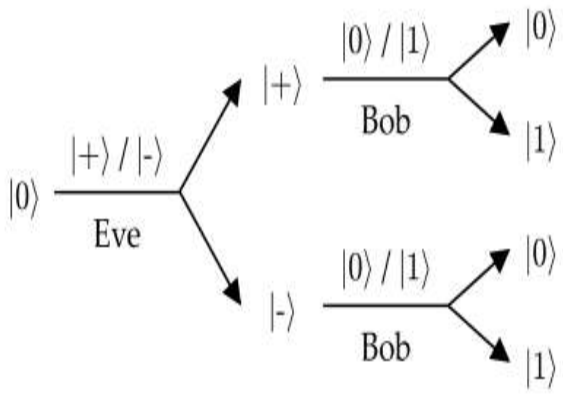

Figure 1.4: Possible events when Eve uses the wrong measurement for eavesdropping.

So, when Eve tries to eavesdrop, she will get irrelevant results about half of the time and disturb the state. She might decide not to send Bob the states for which she gets irrelevant results, but it is impossible for her to make such a distinction, as she does not know in advance which encoding is used. Discarding a key element is useless for Eve since this sample will not be used by Alice and Bob to make the key. However, if she does retransmit the state (even though it is wrong half of the time), Alice and Bob will detect her presence by an unusually high number of errors between their key elements.

Both Bob and Eve have the same difficulties in determining what Alice sent, since they do not know which encoding is used. But the situation is not symmetric in Bob and Eve: all the communications required to do the sifting are made over the classical authenticated channel. This allows Alice to make sure she is talking to Bob and not to Eve. So, the legitimate parties can guarantee that the sifting process is not influenced by Eve. Owing to this, Alice and Bob can select only the key elements which are correctly measured.

To detect the presence of an eavesdropper, Alice and Bob must be able to detect transmission errors. For this, an option is to disclose a part of the sifted key. A given protocol might specify that after a transmission of l+n key elements (e.g., l+n=100 000), numbered from 0 to l+n-1, Alice randomly chooses n indexes (e.g., n=1000) and communicates them to Bob. Alice and Bob then reveal the corresponding n key elements to one another so as to count the number of errors. Any error means there was some eavesdropping. The absence of error gives some statistical confidence on the fact that there was no eavesdropping – Eve might just have been lucky, guessing right the encoding sets or making errors only on the other l key elements. Of course, only the remaining l key elements will then be used to produce a secret key.

3.3 Distilling a secret key

In the case where errors are detected, Alice and Bob may decide to abort the protocol, as errors may be caused by eavesdropping. At least, this prevents the creation of a key that can be known to the adversary. This kind of decision, however, may be a little stringent. In practice, the physical implementation is not perfect and errors may occur for many reasons other than eavesdropping, such as noise or losses in the quantum channel, imperfect generation of quantum states or imperfect detectors. Also, Eve may just eavesdrop a small fraction of the sifted key, making the remaining key elements available for creating a secret key. There should thus be a way to make a QKD protocol more robust against noise.

Alice and Bob count the number of errors in the disclosed key elements and divide this number by n to obtain an estimate of the expected fraction e of transmission errors in the whole set of key elements; e is called the *bit error rate*. They can then deduce the amount of information Eve knows about the key elements. For instance, they can statistically estimate that Eve knows no more than, say, IE bits on the l key elements. This is the *estimation* part of the protocol. The formula giving the quantity IE is not described here; it results from an analysis of what an eavesdropper may do given the laws of quantum mechanics. Also, the quantity IE does not precisely tell Alice and Bob what Eve knows about the key elements. She may know the exact value of IE key elements or merely the result of some arbitrary function of the l key elements, which gives her IE bits of information in the Shannon sense.

At this point, Alice and Bob know that the l undisclosed key elements have some error rate e and that a potential eavesdropper acquired up to IE bits of information on them. Using the public classical authenticated channel, Alice and Bob can still try to make a fully secret key; this part is called *secret-key distillation*.

Secret-key distillation usually comprises a step called *reconciliation*, whose purpose is to correct the

transmission errors, and a step called *privacy amplification*, which wipes out Eve's information at the cost of a reduced key length. I shall briefly describe these two processes.

In the case of BB84, the reconciliation usually takes the form of an interactive error correction protocol. Alice and Bob alternatively disclose parities of subsets of their key elements. When they encounter a diverging parity, it means that there is an odd number of errors in the corresponding subset, hence at least one. Using a dichotomy, they can narrow down the error location and correct it. They repeat this process a sufficient number of times and the result is that Alice and Bob now share equal bits.

For secret-key distillation, all the communications are made over the public authenticated classical channel. Remember that Eve cannot intervene in the process but she may listen to exchanged messages, which in this case contain the exchanged parity bits. Therefore, the knowledge of Eve is now composed of IE+|M| bits, with |M| the number of parity bits disclosed during the reconciliation.

To make the key secret, the idea behind privacy amplification is to exploit what Eve does not know about the key. Alice and Bob can calculate a function f of their key elements so as to spread Eve's partial ignorance over the entire result. Such a function (e.g., like a hashing function in classical cryptography) is chosen so that each of its output bits depends on most of, if not all, the input bits. An example of such a function consists of calculating the parity of random subsets of bits. Assume, for instance, that Eve perfectly knows the bit x1 but does not know anything about the value of the bit x2. If the function f outputs x1+x2mod2, Eve has no clue on this output value since the two possibilities x1+x2=0(mod2) and x1+x2=1(mod2) are equally likely no matter what the value of x1 is.

The price to pay for privacy amplification to work is that the output (secret) key must be smaller than the input (partially secret) key. The reduction in size is roughly equal to the number of bits known to Eve, and the resulting key size is thus l-IE-|M| bits. To maximize the key length and perhaps to avoid Eve knowing everything about the key (e.g., l-IE-|M|=0), it is important that the reconciliation discloses as little information as possible, just enough to make Alice and Bob able to correct all their errors.

Notice that errors on the quantum transmission are paid twice, roughly speaking, on the amount of produced secret key bits. First, errors should be attributed to eavesdropping and are counted towards IE. Second, errors must be corrected, for which parity bits must be publicly disclosed and are counted towards |M|.

Finally, the secret key obtained after privacy amplification can be used by Alice and Bob for cryptographic purposes. In particular, they can use it to encrypt messages and thus create a secret channel.

3.4 Example

Sending

1. Alice determines the polarization (horizontal, vertical, left-circular or right-circular) of each burst of photons which she's going to send to Bob. Since a lot of this information will later be discarded, this can probably be done randomly. The goal is not to transfer a specific key, but to agree on a key that is common to both parties.

2. A light source from a light-emitting diode (LED) or from a laser is filtered to produce the desired polarized photons. Ideally, each pulse consists of a single photon. However, in real life it actually has to be a beam of light with very low intensity. If the intensity is too low, a pulse may be undetectable for the receiver, yet if it's too high, then the polarization of the photons can be detected discreetly (i.e. a photon from the beam can be measured by the eavesdropper with respect to both bases without any noticeable difference to the beam). Both cases are undesirable to say the least, so the intensity has to be regulated very carefully. (6)

Receiving and converting

3. Bob randomly generates a sequence of bases (rectilinear or circular), and measures the polarization of each photon with respect to one of them.

4. Bob tells Alice which sequence of bases he used, without worrying about other people hearing this information.

5. Alice publicly responds with which bases were chosen correctly.

6. Alice and Bob discard all observations except for those with the correctly-chosen bases.

7. The remaining observations are converted on to binary code (left-circular or horizontal is 0, and right-circular or vertical is 1).

Correcting errors – step 1

8. Alice and Bob agree on random permutations of bits in the resulting string, to randomize the positions of errors. Two errors next to each other are very hard to detect, yet it is likely that an error with the instruments or because of random noise would alter a sequence of bits one after the other. Randomization helps account for that.

9. The strings are partitioned into blocks of size k, with k ideally chosen to make the probability of multiple errors per block very small. Note that if Alice's string

contains 101100 and Bob's contains 101111, the parity is the same, 1, even though there are two mistakes in the block. Making k small is one of the steps taken to minimize the chance of this happening, since the chances of having two errors in a block of size 50 is much less than in a block of 500, especially after the errors are randomized.

10. Alice and Bob compute and exchange parities for each block. This information can be made public, but, to ensure security, the last bit of each block is then discarded, making the information useless for Eve.

11. Any block with different reported is broken down further and a binary search is used to locate and correct the error. Alternatively, if the length of the key is already sufficiently large, those blocks could even be discarded.

12. Steps 9-12 are then repeated with increasing block size, k, in an attempt to discover multiple errors that could've gone undetected within original blocks.

Correcting errors - step 2

13. Finally, to determine if additional errors remain, Alice and Bob do another randomized check. They publicly agree on a random assortment of half the bit positions in their string, and compare parities, followed discarding the last digit, as always.

14. If the strings are different, then there is probability of a disagreement of parities. Then a binary search is used to find and eliminate error, as described above.

15. After r repetitions of step 13 without disagreements, Alice and Bob can conclude that their strings disagree with probability (1/2)r, which can obviously be made arbitrarily small by increasing r.

4. APPLICATION OF QUANTUM CRYPTOGRAPHY

The most infamous and developed application of quantum cryptography is quantum key distribution (QKD). Quantum key distribution [6] is a method used in the framework of quantum cryptography in order to produce a perfectly random key which is shared by a sender and a receiver while making sure that nobody else has a chance to learn about the key, e.g. by capturing the communication channel used during the process. The best known and popular scheme of quantum key distribution is based on the Bennet-Brassard protocol (i.e. BB84), which was invented in 1984 [7]. It depends on the no-cloning theorem for non-orthogonal quantum states. Briefly, the Bennet-Brassard protocol works as follows:

• The sender (usually called Alice) sends out a series of single photons. For each photon, it arbitrarily selects one of two possible base states, with one of them having the possible polarization directions up/down and left/right, and the other one polarization directions which are angled by 45°. In each case, the actual polarization direction is also arbitrarily selects.

• The receiver (called Bob) detects the polarizations of the incoming photons, also randomly selecting the base states.

This means that on average half of the photons will be determined with the "wrong" base states, i.e. with states not corresponding to those of the sender.

• Later, Alice and Bob use a public communication channel to talk about the states used for each photon (but not on the chosen polarization directions). In this way, they can find out which of the photons were by chance preserved with the same base states on both sides.

• Then they reject all photons with a "wrong" basis, and the others signify a sequence of bits which should be identical for Alice and Bob and should be known only to them, provided that the transmission has not been influenced by anybody. Whether or not this happened they can test by comparing some number of the obtained bits via the public information channel. If these bits agree, they know that the other ones are also correct and can finally be used for the actual data transmission.

5. PROSPECTS

Clearly, quantum cryptography is still a long way from being common in information transfer, because the real world is still a long way from theoretical perfection. However, it's important to keep in mind that the basic foundation for this great technique has been laid, and so now it only needs to be refined.

5.1 Future direction

For now, non-quantum cryptography is still very safe, because it relies on algorithms that can't be cracked in less than the lifetime of the universe by all the currently existing computers. So in theory, there is not much need for quantum cryptography yet; however, we never know when technology will take a leap forward and quantum techniques will become necessary to protect our information. When quantum computers will come into play, the computational speeds will increase dramatically, so the mathematical complexity of algorithms will become less of a challenge. It is still debatable whether or not it will be possible to simply increase the numbers use in the algorithms and thus increase the complexity enough to outrun even quantum computer.

Yet there is no debate about the fact that quantum

cryptography is a true breakthrough in the field. It is still being refined and developed further. However, already it is clear that even with its current imperfections, it is many steps above everything that was developed before it. All we need is some years, or maybe decades or even centuries, to refine the technique and make it practical in the real world.

5.2 Current limitations

For now, computers capable to transmitting information using quantum cryptography are very large, custom-made and, thus, expensive. A couple of banks have already taken advantage of this security method, but few other organizations would be able to afford it in the foreseeable future.

With regards to entangled photons, which seem to be absolutely safe, there is also a serious practical problem not only with the cost, but also with keeping them entangled long enough to meet the needs of the real world. While the system is perfect in theory, it is going to be very hard to implement it in practice.

Another problem is that for distances beyond 50 kilometres or so, the noise becomes so great that error rates skyrocket. This not only leaves the channel very vulnerable for eavesdroppers, but also makes it virtually impossible to send information. However, it is potentially possible for quantum keys to be exchanged through the air in the future. Tiny telescopes would then have to be aligned to detect the signal. Some calculations even suggest that photons could be detected by a satellite, which would allow communication between continents!

6. CONCLUSION

We presented an aspect of the workings of quantum cryptography and quantum key distribution technology. This technology is basically depends upon the polarization of photons, which is not a well regulated quantity over long distances and in multi-channel networks. Quantum cryptography could be the first attention of quantum mechanics at the single quanta level. Quantum cryptography promises to reform secure communication by providing security based on the elementary laws of physics, instead of the current state of mathematical algorithms or computing technology. The devices for implementing such methods exist and the performance of demonstration systems is being continuously improved. Within the next few years, such systems could start encrypting some of the most valuable and important secrets of government and industry.

7. ACKNOWLEDGMENT

We would like to thank our respected Executive Director Prof. S. N. Basu, Administration of Technique Polytechnic Institute, specially respected Chairman (GB) Mr. Tapas Kumar Saha and R&D Cell of this institute for motivating us in this research work. We would also like to thank all the members of Technique Polytechnic Institute for their support and co-operation. We thank all mighty God and our parents for their blessings in our life.

8. REFERENCES

[1] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance of two quantum key- distribution Protocols," Phys. Rev. A vol. 73, 2006.

[2] Simmon, G. J. ,"Symmetric and asymmetric encryption", ACM Computing Surveys, 11(4), 1979, pp. 305-330.

[3] Bennett, C. H., Brassard, G., and Ekert, A. K.Quantum cryptography. Sci. Am. 267, 4 (Oct.1992), pp. 50.

[4] C. Elliott, D. Pearson and G. Troxel, "Quantum Cryptography in Practice", Preprint of SIGCOMM 2003 paper [5] D.R. Stinson, Cryptography, Theory and Practice, CRC Press, Inc., Boca Raton, p. 4(1995).

[6] Mehrdad S. Sharbaf, "Quantum Cryptography: A New Generation of Information Technology Security System". 2009, pp. 1644-1648.

[7] C.H.Bennett and G. Brassard, "QuantumCryptography: Public Key Distribution and Coin Tossing",In Proceedings of IEEE International Conference onComputers Systems and Signal Processing, Bangalore,India, pp. 175-179, December 1984. (Bennet-Brassard protocol)

[8] W. K. Wooters and W. H. Zurek, "A single quantum cannot be cloned", Nature 299, 802 (1982) (no-cloning theorem)

[9] N. J. Cerf and J. Fiurasek, "Optical quantum cloning - a review", Prog. Opt. 49, 455 (2006).

[10] Young, A., "The future of cryptography: Practice and theory", IEEE IT Professional Journal, 2003, pp. 62-64.

[11] Vishnu Teja, Payel Banerjee, N. N. Sharma and R. K. Mittal, "Quantum Cryptography: State-of-Art,Challenges and Future Perspectives". 7th IEEE International Conference on Nanotechnology, 2007, pp. 1296-1301.

[12]Bennett, C.H. and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International

Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984.

[13] Ekert. A. Physical Review Letters, 67, pp.661-663, (1991)

[14] Kak, S., A three-stage quantum cryptography protocol. Foundations of Physics Letters, vol. 19, pp.293-296, 2006.