ISTANBUL UNIVERSITY –
JOURNAL OF ELECTRICAL & ELECTRONICS ENGINEERING

YEAR : 2008 (503-510)
VOLUME : 8
NUMBER : 1

QUANTUM CRYPTOGRAPHY AND COMPARISON OF QUANTUM KEY DISTRIBUTION PROTOCOLS

Ergün GÜMÜŞ[1] **G.Zeynep AYDIN[2]** **M.Ali AYDIN[3]**

[1, 2, 3] İstanbul University, Computer Engineering Department, Avcılar – İstanbul, TURKEY
[2] E-mail : zeynepg@istanbul.edu.tr [3] E-mail: aydinali@istanbul.edu.tr

ABSTRACT

Even though there have been various proposed and wideley used ciphering techniques in cryptography, main improvements in this field came out with the idea of "super computing". Till now, popular methods like DES, AES and RSA which can be mathematically cracked in a duration of universe's age, have been proposed. But all of these methods's future is at risk because of the studies in production of "Quantum Computer"s of which computation speed is estimated to be very high so that no other existing super computers compete with them. At this stage, by using quantum mechanics a new method called "Quantum Key Distribution" and its protocols for the process of building cipher key, are proposed instead of determining new mathematical solutions for securing the data. In this study, a simulation project based on previously proposed Quantum Key Distribution protocols BB84 and B92, will be explained. At the end of the project by using BB84 and B92 protocols, a comparison of quantum bit error rates and detection rates of eavesdropping according to protocols, is done and results are obtained.

Keywords: *Quantum Cryptography , Quantum Key Distribution Protocols , BB84 , B92*

1.INTRODUCTION

For popular encryption algorithms like DES, AES, RSA etc., it is inevitable to be cracked in hours by rising computation speed of computers in the future. Rise of this computation speed will peak with production of quantum computers. By the way, quantum physics which threats today's encryption algorithms with the idea of "quantum computing" also brings the solution to the problem. According to this, if encryption algorithms depending on the principle of mathematical computation difficulty are to be easily cracked by quantum computers then a new method must be proposed. This method must generate encyrption keys in a %100 secure way and the generated key must be used in an encrypiton method proven to be uncrackable mathematically.

This new method is "Quantum Cryptography" which anticipates generation and distribution of encryption key over optical lines with eavesdropping detection. And firstly suggested encryption algorithm for this method is OTP (One Time Pad) of which reliabilty is proven by Shannon Theory.

In this study, "Quantum Key Distribution" (QKD) subject which concerns with generation

Received Date:19.11.2007
Accepted Date: 25.03.2008

and distribution of encryption key is dealed with. At second part of study, some terms and basis about Quantum Cryptography are mentioned. At third part, two QKD protocols BB84 and B92 are explained. Steps of QKD process are mentioned on fourth part. At fifth part, some information about simulation work including BB84 and B92 protocols, and at sixth part graphical results of this simulation work are given. Lastly at seventh part, comments on results of the simulation are done and simulated QKD protocols are compared.

2.QUANTUM CRYPTOGRAPHY

2.1. Some Terms About Quantum Cryptography

Before further reading, some terms about Quantum Cryptography are presented :

- **Quantum :** Smallest unit of energy. Quantum is named as "Quanta" in plural form.
- **Photon :** Smallest unit of energy that can be transmitted in a wavelength. It is referred as quantum of light. Photons are massless particles with energy.
- **Polarisation :** The direction of electomagnetic field that a quantum particle has. For Quantum Cryptography, polarisation of a photon is a characteristic feature that is used for secure transmission.
- **Qubit :** Bit value of a photon that is assigned according to photon's polarisation. Quantum bit.
- **Bases :** Special filters with polarisation angles of 0,45,90 or 135 degrees which are used to polarize a photon generated by a beam source like a laser.

Fig. 2.1 *Polarisation bases with 0, 45, 90 and 135 degree polarisation angles in order*

- **Filter :** A form that is constituted of two crosswise bases. It is used to read last polarisation of a polarized photon. There exists two filters : " Diagonal Filter " and " Rectilinear Filter ".

Fig. 2.2 *"Diagonal" and "Rectilinear" filters in order*

2.2. Physical Basis Of Quantum Cryptography

Quantum Cryptography is related to Heisenberg's "Uncertainity Principle" which issues that a measurement process on a quantum particle randomizes results of following measurements. For instance, a photon passing through a polarisation filter with 0 degree polarisation angle, is 0 degree polarized and if this photon is directed to a second polarisation filter which has such a polarisation angle like $\theta = 45^{\circ}$ then it may pass through it with the probability of %50. In this situation it can be said that the first measurement randomized the result of second measurement [1].

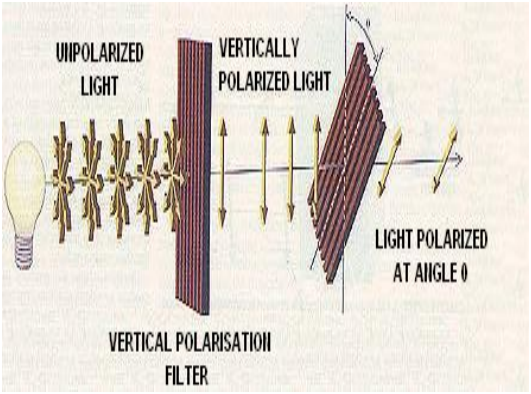

Fig.2.3 *Unpolarized photons pass through first filter and gain a polarisation angle of 0 degree. This measurement randomizes these photons's pass through second fitler[1]*

All along this study, measurements which are done using bases/filters will be named as "reading" processes.

In Quantum Cryptography, reading process occurs by the way shown at Figure 4 according to different polarisation angles :

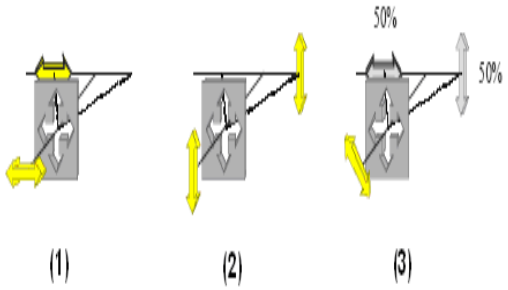

Fig. 2.4 *Reading process with rectilinear filter and photons with polarisation angles of 0 , 90 and 135 degrees*

3.QUANTUM KEY DISTRIBUTION (QKD) PROTOCOLS

Till today, many Quantum Key Distribution protocols like BB84, B92, EPR, SARG etc. are proposed. All of these protocols's main aim is to form an encryption key and distribute it to both sides in such a secure way that a probable eavesdropping attempt can be detected. Today, in commercial models of Quantum Key Distribution, BB84 protocol is the widely used one. In scope of this study, BB84 and B92 protocols are used. Common working principle of these protocols for sending / receiving process is like that :

Sending Side

- In each time slot, generate one bit of encryption key randomly.
- In order to represent the same qubit value with the generated bit, polarize a photon with one of 4 bases in suitable polarisation angle.
- Send the polarized photon to receiving side over optical line.
- Note down sent qubit value and type of base that is used in polarisation process.

Receiving Side

- In order to read polarisation of the photon coming over optical line, choose either a diagonal or a rectilinear filter randomly and read incoming photon's polarisation.
- Note down used filter type and qubit value after reading process.

3.1. Bennett & Brassard 1984 (BB84) Protocol

This protocol is proposed by Charless Bennett from IBM Research and Gilles Brassard from Montreal University in 1984 after Stephen Wiesner's study about "Conjugate Coding" during 70's. Bennett and Brassard carried out this protocol in 1991 by lightwave transmission from a distance of 32 centimeters [3]. BB84 became a foundation of many subsequent QKD protocols.

In this protocol, sending side can use two of four different polarisation angles in order to send a 0 or 1 valued qubit [4]. Qubit – Polarisation matching of BB84 protocol is shown at Figure 3.1.

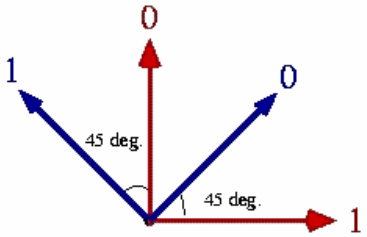

Fig. 3.1 *Qubit – Polarisation matching of BB84 protocol for sending / receiving process*

Each qubit is represented by one of two non-perpendicular polarisation angles. For matching rule at Figure 3.1, polarisation angles of 0 and 135 degrees represents a qubit with value of 1 and polarisation angles of 45 and 90 degrees represents a qubit with value of 0.

Same matching rule must be chosen by both sides for a flawless transmission process.

In a system that is using BB84, if an eavesdropper tries to read polarisation of a photon with a filter which contains a base with the same polarisation angle of this photon then photon's polarisation remains unchanged. Otherwise, if the eavesdropper uses the wrong type of filter for reading process, photon's original polarisation angle changes ± 45 degrees.

This change at photon's polarisation can be realized when sending and receiving sides compare their chosen base/filter types for each

photon and a small amount of revealed (sacrificed) qubit values after transmission process over a public channel like telephone, fax, e-mail etc. By this way they can compute an error rate and compare it with a threshold value in order to determine eavesdropping.

3.2. Bennett 1992 (B92) Protocol

This protocol is proposed by one of BB84 developers Charles Bennett in 1992 for designing easier implemented QKD systems. In this protocol sending side uses two non-perpendicular polarisation angles of four polarisation angles and receiving side uses remaining two polarisation angles for reading process [5].
Qubit – Polarisation matching for B92 protocol's sending side is shown at Figure 3.2.

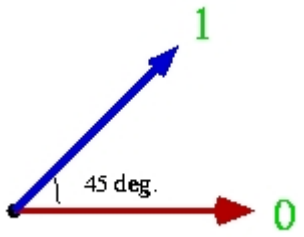

Fig. 3.2 *Qubit – Polarisation matching for B92 protocol's sending side*

Sending side polarizes the photon with 0 degree in order to send a qubit with value of 0 and with 45 degree in order to send a qubit with value of 1.

Qubit – Polarisation matching for B92 protocol's receiving side is shown at Figure 3.3.

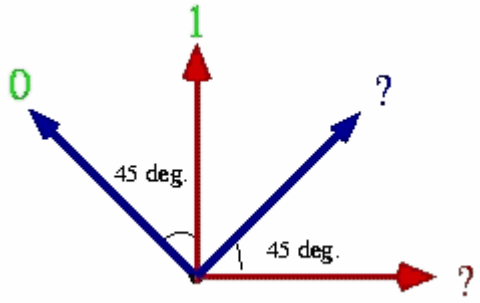

Fig. 3.3 *Qubit – Polarisation matching for B92 protocol's receiving side*

According to this, to make a valid read process, receiving side must read polarisation of the photon with a filter that does not contain a base having same polarisation with the photon. Otherwise, read photon and its qubit value is considered as invalid (shown with ?).

Similar to BB84 protocol, in B92 protocol eavesdropping can be detected after comparing a small amount of revealed (sacrificed) qubit values but chosen base types for sending process are not revealed.

4.STEPS OF QUANTUM KEY DISTRIBUTION PROCESS

In order to generate final key that will be used in any encryption method, four steps are applied. These steps are as follows :

4.1. Raw Key Extraction

This step deals with elimination of erroneous transmitted bits and it is carried over public channels like telephone, fax, e-mail etc. which are vulnerable to eavesdropping. Its application shows differences from protocol to protocol.

For BB84 protocol, at this step sending and receiving sides compare filter types which they used during sending/reading process for each photon. If they have used different types of filters for a photon's transmission then they eliminate the bit value corresponding to this photon. For BB84, sharing the type of filters used in reading/sending process over a public channel does not reveal any side's bit sequence. Because by using both filter types, polarized photons with any qubit value can be produced.

For B92 protocol, sending side does not reveal his/her used filter types because he/she can produce only two different types of polarized photon. Instead only receiving side announces indices of bits he/she read as "valid".Invalid bits are deleted from both sides's bit sequences.

4.2. Error Estimation

If sides are using a QKD protocol over a noisy channel, this situation turns into an advantage for

an eavesdropper. Because at any time slot, if both sides use same type of filter for sending/reading process and they do not have the same qubit value this can be due to not only existence of an eavesdropper but also physical noise of transmission medium. This situation prepares a suitable environment for attacks on QKD systems over physical channel's noise.

To avoid such attacks, both sides determine an error threshold value "Rmax" when they are sure that there is no eavesdropping on transmission medium. Then after each QKD session, they compare (sacrifice) some bits of their raw keys in order to calculate a transmission error percentage "R". By that way, for $R > Rmax$ case they can be sure about existence of an eavesdropper.

4.3. Key Reconciliation

Even for $R \leq Rmax$ case, there can be erroneous bits in uncompared parts of keys. At this situation sides apply an error minimization step called "Key Reconciliation". This step includes those sub-steps:

a) Sending and receiving sides reorder their bit sequences by a common permutation function on which they agreed over public channel. By this way they distribute erroneous bits uniformly.

b) Bit sequences are divided into blocks of k bits. To reduce the possibility of more than one erroneous bit's existence in each block, k must be chosen ideal.

c) For each block, sending and receiving sides calculate a parity value and announce it. Last bit of each block of which parity value is annonunced, is deleted.

d) Both sides divide each matching block with different parity values into sub-blocks and compare parity values of these sub-blocks to find erroneous bits [6]. This method is like "Binary Search". Last bit of each sub-block of which parity value is annonunced is also deleted.

e) There can be more than one erroneous bit in any block, for this reason first 4 sub-steps are reapplied by increasing k.

f) In order to detect remaining erroneous bits, both sides calculate the parity value of half of their bit sequences by announcing bit indices. If those values are still different then sides start "Binary Search" method in fourth sub-step again.

4.4. Privacy Amplification

Privacy Amplification is the fourth step which is applied to minimize the number of bits that an eavesdropper knows in the final key [7]. Sending and receiving sides apply a shrinking method to their bit sequences in a way that eavesdropper can not apply properly to his/her bit sequence.

Let's assume that we have a bit sequence of n bits after application of first 3 steps. And also let's assume that eavesdropper knows m (m is a value derived from Rmax) bits of final this bit sequence. Then a number of n-m-s (s is a constantly chosen security parameter) sub-blocks are extracted from final bit sequence without revealing their contents and union of these sub-blocks's parity values form the final key. By this way number of bits that an eavesdropper may know is reduced to $2 - s / \ln 2$ and length of final key since start of QKD session is reduced to n-m-s bits.

Quantum Key Distribution decision steps after Raw Key Extraction can be shown like at Figure 4.1 :

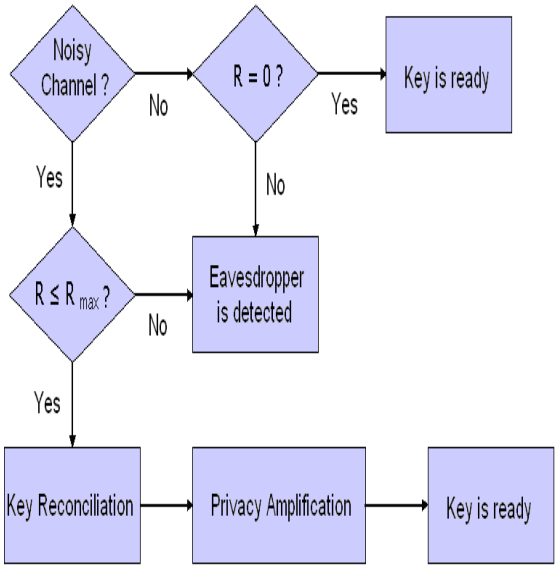

Fig. 4.1 *Quantum Key Distribution Decision Scheme*

5.SIMULATION

In developed simulation work, final key generation steps and transmission visualisation according to BB84 and B92 QKD protocols are implemented. At second part of work, relationships between protocols – error rates and increasing eavesdropping – error rate is observed.

5.1. Simulation Work

For visual simulation, at first stage of program parameters like :

- Total number of bits to transmit,
- Eavesdropping rate,
- Rate of photons that will change polarisation due to channel's noise,
- Rmax threshold value,
- Minimum and maximum values of k which will be used in Key Reconciliation step,
- Protocol type to implement (BB84 or B92)

are taken. According to these parameters visual photon transmission session is carried out by a loop which generates polarized photons with 4 or 2 different polarisation angle according to chosen protocol type. This loop ends after total number of bits to transmit is reached.

Then Raw Key Extraction step at which only receiving side or both sides (according to chosen protocol) announce used filter types to send/receive is performed. After this step sides announce and compare the parity value of their bit sequences's %1 part. By that way they calculate the error rate R to compare with maximum error rate Rmax. For R > Rmax case, existence of an eavesdropper is detected and following steps of QKD are not performed.

Otherwise, Key Reconciliation step is started. Remaining bits are reordered by a randomly generated permutation and erroneous bits are deleted with binary search and parity check method in a recursive function. For the last step (Privacy Amplification), sides divide their bit sequences into sub-blocks and take their parity values as bits of final key.

At the second part of program which deals with comparative results ;

1) Effects of %100 eavesdropping (10.000 transmitted photons) on error rate in a noiseless channel according to BB84 and B92 protocols,
2) Effects of increasing eavesdropping rate on error rate in a noisy channel according to BB84 and B92 protocols (total number of bits to transmit , rate of photons that will change polarisation due to channel's noise and Rmax threshold value are taken from user)

are observed and results are graphically presented to user.

6.SIMULATION RESULTS

6.1. Relationship Of Error Rates To Protocols With %100 Eavesdropping Rate

For both protocols, eavesdropping on all of 10.000 transmitted photons increases the error rate R and for an ideally chosen Rmax threshold value this leads to detection of eavesdropper

easily.

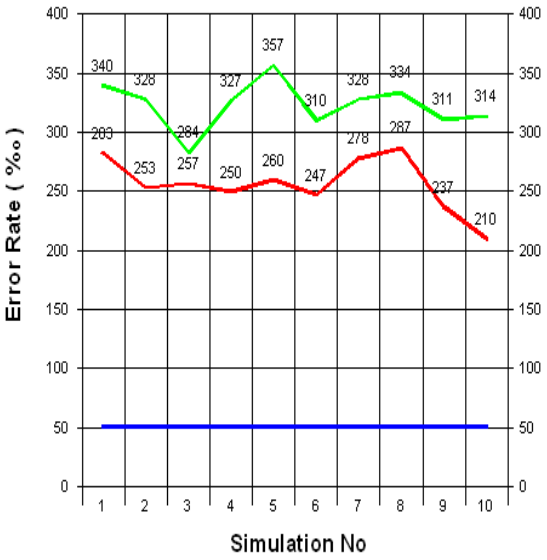

Fig. 6.1 *Relationship between protocols and error rates*

For 10 consecutive simulations on a noiseless channel with a Rmax threshold value of ‰ 50, each time eavesdropper could be detected. By the way it is observed that B92 protocol gives higher average error rates than BB84 protocol. This is shown at Figure 6.1.

6.2. Relationship Of Error Rates To Protocols With Increasing Eavesdropping Rate

As the number of photons that eavesdropper reads increases, the number of photons that lose their original polarisation permanently, increases. This leads to an increase in error rate R and for an ideal Rmax threshold value eavesdropper will be detected.

For 10 consecutive simulations with an increasing eavesdropping rate of ‰ 100 in each try, ‰ 200 channel noise and an Rmax threshold value of ‰ 250 , 10.000 photons are transmitted each time. As a result increasing eavesdropping rate caused error rate R , pass Rmax limit inevitablly (Figure 6.2).

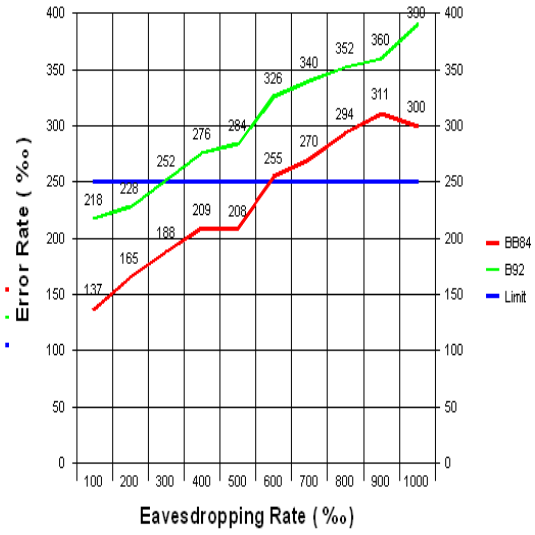

Fig. 6.2 *Relationship between error rate and increasing eavesdropping rate*

If we compare average error rates of protocols, we again see that B92 protocol has a higher average error rate than BB84 protocol and this leads to detection of eavesdropping at lower eavesdropping rates.

7.CONCLUSIONS

Quantum Cryptography is presented as a %100 secure cryptographic method because of eavesdropping detection and being a physics based method rather than a mathematical method. Unless physics laws on which Quantum Cryptography depends are defeated, method is regarded as impossible to crack. This is a relatively correct approach but like every improperly applied method if Quantum Cryptography is applied improperly, it can turn into a very insecure method too.

For instance, according to simulation results one can suggest that B92 protocol is a better protocol than BB84 because of detecting eavesdropping at lower rates. But the same B92 protocol is more vulnerable to “intercept – resend” type attacks than BB84 [8][9] because of polarizing a photon with only two types of polarisation angles. So, main simplifying idea behind B92 protocol turned out to be a weak point.

It also must be stated that for QKD systems Rmax threshold value must be ideally chosen such that it is not smaller than percentage of

photons of which polarisations are spoiled due to transmission channel's or hardware's noise and not great to allow eavesdropping attempts. An improper choice can lead to reveal of secret data or false alerts. This ideal threshold value will keep on decreasing as physical noise of today's transmission lines and hardwares decreases and eventually it will be so hard to eavesdrop on QKD systems by hiding behind physical noise.

REFERENCES

[1]Vittorio, S., 2002, "Quantum Cryptography: Privacy Through Uncertainty" http://www.csa.com/discoveryguides/crypt/overview.php
[2]Id Quantique White Paper, 2005, "Understanding Quantum Cryptography" http://www.idquantique.com/products/files/vectis-understanding.pdf
[3]Ford, J., 1996, "Quantum Cryptography Tutorial" http://www.cs.dartmouth.edu/~jford/crypto.html #1
[4]Bennett, C.H., Brassard, G., 1984, "Quantum Cryptography: Public Key Distribution and Coin Tossing"
[5]Bennett, C.H., 1992,"Quantum Cryptography: Uncertainty in the Service of Privacy"
[6]Papanikolaou, N., 2004, "Techniques For Design And Validation Of Quantum Protocols"
[7]Goldwater, S., 1996, "Quantum Cryptography and Privacy Amplification" http://www.ai.sri.com/~goldwate/quantum.html
[8]Gisin, N., Ribordy, G., Tittel, W., Zbinden, H., 2004 , "Quantum cryptography"
[9]Fuchs, C. A., Gisin, N., Grıffiths, R. B., Niu, C. S., Peres, A. , 1997, "Optimal Eavesdropping In Quantum Cryptography. I. Information bound and optimal strategy"