www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 6 June 2015, Page No. 12273-12277

Quantum Cryptography, its Protocols and Techniques

Manimozhi Iyer[1], Deepika Vasudevan[2], Tejaswini B. S.[3], Vidya Sri M[4],

[1]Computer Science and Engineering Department, C.M.R Institute of Technology,
A.E.C.S Layout, Bengaluru-560037, India
mani.mozhi@cmrit.ac.in

[2]Computer Science and Engineering Department, C.M.R Institute of Technology,
A.E.C.S Layout, Bengaluru-560037, India
deepikav2793@gmail.com

[3]Computer Science and Engineering Department, C.M.R Institute of Technology,
A.E.C.S Layout, Bengaluru-560037, India
tejbs.cmr@gmail.com

[4]Computer Science and Engineering Department, C.M.R Institute of Technology,
A.E.C.S Layout, Bengaluru-560037, India
sm.vidya@gmail.com

Abstract: ***Various approaches and techniques are being constantly studied to ensure a secure communication. Modern cryptographic techniques face a serious threat by the progress of computing power. They generally make use of large numbers which can be factorized. The use of this make the communication vulnerable to attacks as it is now possible to reverse the one-way functions. Motivated by this concern, Quantum Cryptography was introduced to provide secure communication. It depends on two important aspects of quantum mechanics, the Heisenberg Uncertainty principle and the principle of photon polarization. This paper focuses on the principle and working of Quantum Cryptography and compares various Quantum Key Distribution Protocols such as BB84 and B92. It also introduces other cryptographic techniques which are popularly used.***

Keywords: quantum cryptography, cryptography, quantum key distribution, BB84

1. Introduction

Cryptography[1] is a technique used to keep data 'cryptic' or hidden. It involves the study of securing highly confidential material from outside unauthorized access. The practice of securing confidential material in a network has evolved through the ages from Julius Caesar's cipher and the German Lorenz cipher machine used in World War II.

Cryptography operates on *plaintext* and *cipher text*. Plaintext is the raw message that the sender wishes to conceal from external penetration and send to another party – the receiver. Encryption algorithms operate of plaintext to keep them confidential. Cipher text is the product of this encryption algorithm on plaintext. Without proper algorithms to decrypt cipher text, it cannot be read by humans or computers.

There are two kinds of cryptography – *private key cryptography* and *public key cryptography*. In private or symmetric key cryptography, the keys used by the sender and

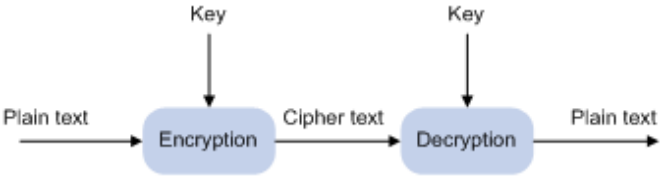

Fig: 1: Cryptography

the receiver are usually identical or a simple transformation can alter one to the other. This sharing of the key is a major drawback of symmetric key cryptography.

Public key cryptography overcomes this drawback. Public key or asymmetric cryptography includes a private key between the sender and the receiver and a public key. The public key is used to encrypt the plaintext data while the private key is used to decrypt the same.

1.1 Public Key Cryptography

Public Key Encryption[2] scheme supports a two-way communication. It supports each user with a key which is made publically available by the other person.

An arbitrary message M is subjected to encoding and decoding processes *E* and *D* respectively. This following criteria need to be satisfied while working with this scheme:

- $D(E(M)) = M$, the decryption of the encrypted message should give back the original message.
- Even if E is known, guess D should be a difficult task.

1.2 Private Key Cryptography

A *private-key encryption* scheme[3] is also known as a symmetric encryption scheme. It is regarded as a 3-tuple

algorithm **(** E = (Gen, Enc, Dec**))**,that satisfies the following criteria:

- **Gen:** This probabilistic algorithm works by taking security parameter 1_n as its input parameter and outputs a key *k* such that $len(k) \geq n$.
- **Enc:** A probabilistic or a deterministic algorithm works by taking *k*(key) and *m*(plaintext) as its input parameters and outputs a *c*(ciphertext).
- **Dec:** A deterministic algorithm that works by taking *k*(key) and *c*(ciphertext) and outputs a *m*(plaintext).
- For every key k output by Gen and every plaintext m, $Dec(k, Enc(k,m)) = m$.

1.3 Quantum Cryptography

Quantum cryptography[4] is one such type of public key cryptography technique which puts to use the principles of quantum mechanics. This means that encoding and decoding information applies the laws of physics. The data is encoded using *photons.* This usage of photons minimizes the chances deciphering the codes. Mathematical formulae and hacking algorithms cannot be put to use to penetrate the hidden network.

One of the prime applications of quantum cryptography is *Quantum Key Distribution (QKD*). QKD involves the interaction of three parties – Alice, Bob and Eve. Here, Alice and Bob use quantum communication to share a key between them. Eve acts as the outside party trying to infiltrate the network and attempts to learn the details of the shared key.

2. History of Quantum Cryptography

Stephen J. Wiesner made fundamental discoveries in the field of quantum cryptography in the early 1970's. He wrote a paper that used quantum mechanics to support two inventions. One was to design a theoretical bank note that would be physically impossible to counterfeit, and the other, to explain how two messages can be combined together, where reading one message would spoil the other. However, Wiesner's ideas was given little importance. This paper was not published for 13 years.

Charles H. Bennett, a college classmate of Weisner, was interested to know what additional things could be done with information when information carriers which are small enough to obey quantum laws are used. By the early 1980's, Bennett and Gilles Brassard took the ideas of Wiesner and used them in a new cryptosystem design. This system has gone through several transformations and is now considered unbreakable.

3. Fundamentals

Photons are the fundamental particles of light. They exhibit properties of both a particle and a wave. They have no mass but have some characteristics like angular momentum, but their frequency is independent of the influence of mass. In quantum mechanics each photon has characteristic quantum energy.

In quantum mechanics and particle physics, spin is an intrinsic form of angular momentum carried out by elementary as well as composite particles. The existence of a spin angular momentum can be inferred from experiments like the Stern-Gerlach experiment. Spin is like a vector, it possesses a definite magnitude and direction. A spin quantum number is assigned to each elementary particle to indicate it's angular momentum. Spin quantum numbers may take half-integer values.

Although the direction of spin can be varied, the speed with which a particle spins cannot be changed. A photon has only two spin states, +1 and -1. The spin angular momentum of a physical system is quantized and the possible values can be obtained using the following equation

The no-cloning theorem forbids the creation of identical copies of an arbitrary unknown quantum state. Cloning is a process that results in a separable state with identical factors. It was stated by Wootters, Zurek and Dieks.

The no-cloning theorem can be used in a quantum key distribution scheme. The idea is for the sender, Alice, to transmit many photons to the receiver, Bob, ultimately creating a shared, secret, random string of zeroes and ones. An eavesdropper, Eve, would like to get a copy of each photon for herself but at the same time wants to send an accurate copy of it to Bob so that her presence is not detected. But this is not possible due to no-cloning theorem.

Quantum information is represented in the form of qubit or quantum bit. It is a two state quantum mechanical system. Quantum mechanics allows qubit to be in a superposition of two states at the same time unlike classical bits. A pure qubit state is a superposition of the basis states i.e.; it can be represented as a linear combination of |0> and |1>. Various operations can be performed on qubit states like quantum logic gate operations and standard basis measurements.

4. Setup

Quantum mechanics have peculiar properties, trying to measure one may have effects on others. Heisenberg's uncertainty principle revolves around this idea. The rectilinear and diagonal polarization of light is are examples of these. The polarization of a light wave can be in any direction. The direction of the light polarization can be made to be a specific angle by passing light through a polarizing filters. A combination of different filters can be used to achieve a desired direction.

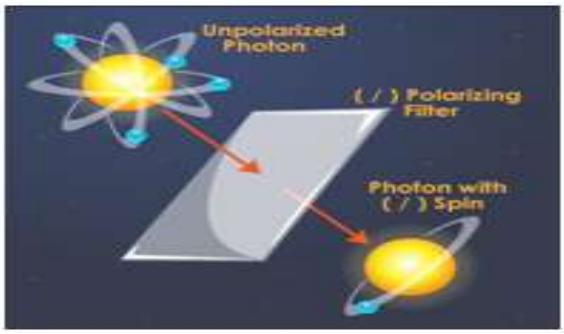

Fig 2: Polarisation of photon

The setup of the quantum cryptosystem[5] has three basic entities, Alice(Sender) , Bon(Receiver) and Eve(Intruder).

Alice uses a combination of filters to obtain a random sequence of polarization bases. This can either be rectilinear or diagonal. She uses this to encrypt her string message. She sends Bob a sequence of photons, each of which represents one bit of the encrypted message with reference to the polarization bases. A

horizontal or 45-degree photon corresponds to a binary zero while a vertical of 135-degree photon refers to a binary one.

Basis	Representation	Random Bit 0	Random Bit 1
Rectilinear	+		
Diagonal	X		
Circular	O		

Fig 3: Polarisation of Bits

Bob after receiving the photons, decides to measure either the rectilinear or diagonal polarization. He does so to interpret the message in the form of binary zeroes and ones. Since only one kind of polarization is measured, he is able to obtain data meaningful data from only those photons whose polarization he guessed correctly.

Alice and Bob now communicate over a normal insecure channel to communicate the bits Bob interpreted. These values are now a secret key to Alice and Bob.

Eve can observe the photons as they go by. She requires a set of filters to interpret the associated values. Let us assume that Alice sends Bob a photon that is 90 degrees. Eve might decide to use a diagonal polarizing filter to measure the polarization. Because she is using the wrong filter, the value she measures could be either 45-degree or 135-degree.

Assuming she measures 135 degrees, she records a 1 and then sends this value along to Bob. Bob then measures the photon using a rectilinear polarizing filter and could observe either a 1 or a 0. When Bob and Alice communicate which bits he used the correct polarizing filter for, this bit will be among that set.
Eve's interference will result in Bob interpreting a wrong bit. Alice and Bob while checking for errors will be aware of the presence of Eve because of the result of her interference in Bob's message.

5. BB84 Protocol

The *BB84*[5,7] is the first Quantum Key Distribution protocol proposed by Bennett and Brassard in 1984. In this scheme, Alice begins with two n bit strings, 'a' and 'b'. She encodes these two strings as a string of n quantum bits using the polarization bases.

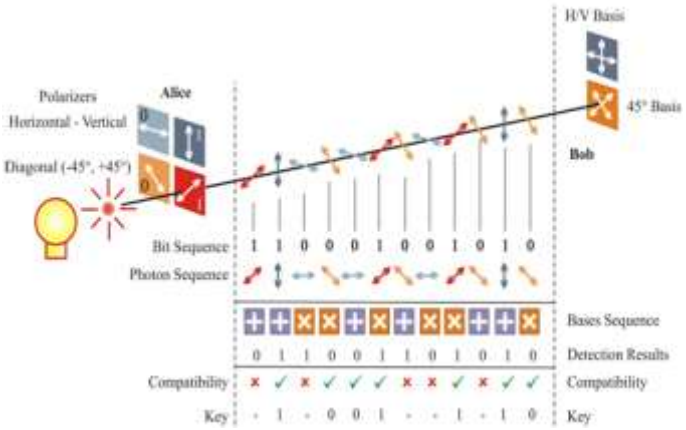

Fig 4: Generalisation of Qubit

Alice can produce photons with 4 different polarization and using a random generator she chooses the basis for each photon. She sends a stream of randomly polarized photons to Bob. Hence this protocol is termed Prepare and Measure (P & M).

Bob has to detect and measure the received photons. He passes the photons through filters which will modify the original orientation of the photons. The interpreted results are recorded in photon counters. Initially Alice and Bob's choice of basis is independent of the other's.

6. B92 Protocol

A quantum key distribution protocol can provide real time key distribution over a quantum channel between Alice and Bob in order to communicate secretly. Alice and Bob can share the secret key using a four state quantum key distribution protocol BB84 and a two state protocol *B92*[8], with idealized maximum efficiencies 50% and 25% over quantum channel respectively.

In a B92 protocol, Alice sends a random sequence of photons |h>-photon and |rcp>-photon. Bob randomly chooses one of his detector basis, |lcp>-basis and |rcp>-basis and records his measurement results (Yes or No). Bob sends a copy of his results to Alice through public channel. The bits where the results are "Y" are kept and the rest are discarded.

(1) Alice sends a random sequence of photons, |h⟩-photon and |rcp⟩-photon.

(2) Bob randomly chooses his detector basis from |lcp⟩-basis or |v⟩-basis to measure each photon, and the bases are interpreted as a binary sequence.

(3) Results of Bob's measurement. Alice and Bob will share the bits where the measurement results are "Y", discarding all other bits.

7. Comparison between Steganography, Elliptic Curve Cryptography and Quantum Cryptography

7.1 Steganography

Steganography [9,10] is a form of cryptography that embeds data into other mediums in an unnoticeable way, instead of employing encryption. Mediums used for steganography are typically human viewable objects such as picture, audio, and video files.

Other steganographic mediums can include web pages, communication protocols, data streams, and many more. A very simple implementation of steganography could be invisible ink written between visible lines of text in a document.

7.2 Elliptical Curve Cryptography

Elliptic Curve Cryptography (ECC)[11] has technically already been invented but is considered by the author to be a future technique of cryptography because its advantages and disadvantages are not yet fully understood. ECC is an approach to encryption that utilizes the complex nature of elliptic curves in finite fields. ECC typically uses the same types of algorithms as that of Diffie-Hellman Key Exchange and RSA Encryption. The difference is that the numbers used are chosen from a finite field defined within an elliptic curve expression.

7.3 Quantum Cryptography

Quantum computation[12] is performed in a quantum computer or processor, which is a processor that makes use of quantum mechanical phenomena, such as quantum superposition and quantum entanglement. Modern computers store data using a binary format called a "bit" in which a "1" or a "0" can be stored. The computations in modern computers typically work in a bit by bit fashion. Quantum computers store data using a quantum superposition of multiple states. These multiple valued states are stored in "quantum bits" or "*qubits*". Depending on the quantum design, each qubit can store a set number values simultaneously (Jones 2009). This allows the computation of numbers to be several orders of magnitude faster than traditional transistor processors.

8. Conclusion

In an era where popular cryptographic techniques such as DES, AES and RSA can mathematically cracked over a period of time, Quantum Cryptography has the potential to be the savior for cryptography. Since it is based on Physics Laws, it is virtually impossible to crack.

As given in this paper, BB84 and B92 are popular protocols that have been proposed previously, each with its own drawbacks and advantages.

Quantum Cryptography, in its comparison with current Cryptographic techniques such as Elliptical Cryptography and Steganography, emerges to be the best, purely because of the concepts on which it is used.

Although experts claim that Quantum Cryptography implementations can also be cracked, they also say that it requires high computation power and high complexity to do so.

9. References

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

[2] Michael Willett, "A Tutorial on Public Key Cryptography" , North-Holland Publishing Company,Computers & Security 1 (1982) 72-79.

[3] J. L. Gómez Pardo," Introduction to Cryptography with Maple, Private Key Encryption, Springer"-Verlag, pg. 196-214 (Chapter 3).

[4] Thi Mai Trang Nguyen, Mohamed Ali Sfaxi and Solange Ghernaouti-Hélie, "802.11i Encryption Key Distribution Using Quantum Cryptography", JOURNAL OF NETWORKS, VOL. 1, NO. 5, SEPTEMBER/OCTOBER 2006.

[5] V. Scarani, H.Bechmann- Pasquinucci, N.J. Cerf, N. Lütkenhaus, M. Peev, "The security of practical quantum key distribution", Reviews of modern physics vol. 81, pp. 1301-1310, 2009.

[6] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing" in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE, New York, pp.175-179, 1984.

[7] *A. Ruiz-Alba, D. Calvo, V. Garcia-Muñoz, A. Martinez, W. Amaya, J.G. Rozo, J. Mora,"*Practical Quantum Key Distribution based on the BB84 protocol",Waves 3, pg. 4-14.

[8] C.H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on the Computes, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), p.g. 175-181.

[9] Neils Provos and published by IEEE Computer Society,pg. 32-44 2003.

[10] R.J. Anderson and F.A.P. Petitcolas, "On the Limits of Steganography," J. Selected Areas in Comm., vol. 16, no. 4, 1998, pp. 474–481.

[11] Elaine Brow, "Elliptic Curve Cryptography", Math 189A: Algebraic Geometry, p.g. 1-5 December 2010.

[12] Ergün Gümüs, G.Zeynep Aydin and M.Ali Aydin, "Quantum Crytpgraphy and comparison of Quantum Key DistributionProtocols", Istanbul University-Journal of Electrical and Electronics Engineering, Vol 8, No. 1, 2008,pg. 503-510.

10. Author Profile

Manimozhi Iyer is currently working as an Assistant prof. in Computer Science Engineering department in CMRIT, Bangalore. Her research interests are Networking, Security in wireless Network, Software Engineering and Image Processing.

Deepika Vasudevan is a final year student of CMR Institute of Technology who is an IEEE member with a strong interest in networking.

Tejaswini B.S is to receive her Bachelor's degree in Computer Science and Engineering from CMR Institute of Technology. She is interested in Networking and Web designing.

Vidya Sri M, a final year student in CMR Institute of Technology is to receive her Bachelor's degree in Computer Science and Engineering in the year 2015. Her interests include Algorithms, Networking and Artificial Intelligence.