Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 12, December 2014, pg.231 – 235

RESEARCH ARTICLE

Enhancement of Network Security by Quantum Cryptography

[1]**P. B. Kalpande**
ME(CSE)
Jagdambha College Of Engineering Yavatmal
priyakalpande99@gmail.com

[2]**Prof. J.S.Karnewar**
Assistant Professor Comp.Engg
Jagdambha College Of Engineering Yavatmal
jay.skumar9@gmail.com

Abstract-

The Security of data and data communication is a top priority because the consequences of insecure data can have grave effects on both the economy and national security. Cryptography is used to secure the information transmitted over telecommunication lines through appropriate encryption techniques. Quantum Cryptography provides more security level then any classical cryptosystem as quantum computing works according to the laws of quantum physics and does not depend on hard mathematical functions. Hence, the resulting Quantum Cryptosystem is more secure and cannot be cracked easily. The quantum cryptography relies on two important elements of quantum mechanics-the Heisenberg uncertainty principle and the principle of photon polarization. The Heisenberg uncertainty principle states that, it is not possible to measure the quantum state of any system without distributing that system. The principle of photon polarization states that, an eavesdropper cannot copy unknown qubits i.e. unknown quantum states, due to quantum no-cloning Theorem. We are using a BB84 protocol for Quantum cryptography.This paper summarizes the current state of Quantum cryptography and exploration of quantum cryptography in Network Security.

Keywords:- Quantum Cryptography, Existing approaches in Classical Cryptography, protocol, Key generation, Securing Key Distribution

I. INTRODUCTION

The Cryptography is a method of storing and transmitting data in a form so that it can no more be interpreted or understand. It is a science of protecting information by encoding it into an unreadable format. Cryptography is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths. Quantum Cryptography is composed of two words: Quantum and Cryptography.

Quantum is the smallest discrete quantity of some physical property that a system can possess and Cryptography enables to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient.

© 2014, IJCSMC All Rights Reserved

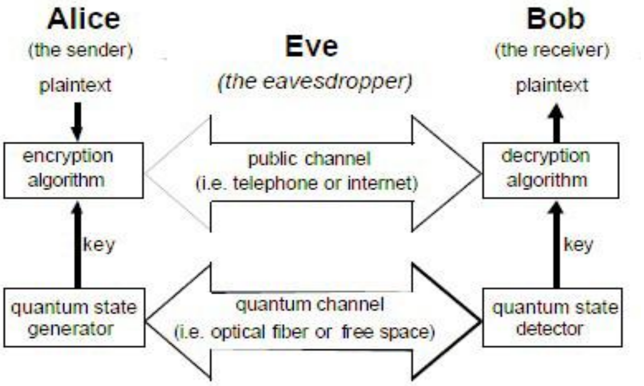


Figure 1: A Quantum Cryptographic Communication System for Securely Transferring Random Key

The quantum cryptography relies on two important elements of quantum mechanics the Heisenberg uncertainty principle and the principle of photon polarization. According the Heisenberg Uncertainty principle, it is not possible to measure the quantum state of any system without disturbing that system.[3]. This principle plays a critical role in thwarting the attempts of eavesdroppers in a cryptosystem based on quantum cryptography. Secondly, the photon polarization principle describes how light photons can be oriented or polarized in specific directions. Moreover, a polarized photon can only be detected by a photon filter with the correct polarization or else the photon may be destroyed. It is Heisenberg's uncertainty principle that makes quantum cryptography an attractive option for ensuring the privacy of data and defeating eavesdroppers.

Quantum Key Distribution (QKD) is used in quantum cryptography for generating a secret key shared between two parties using a quantum channel and an authenticated classical channel.

In the past few years, a remarkable surge of interest from international scientific and business communities has propelled QC into mainstream computer science and physics. Furthermore, new developments are making QC increasingly practical.

II. LITERATURE REVIEW

History

Originally, the security of a cryptogram depended on the secrecy of the entire encrypting and decrypting procedures. Today, however, we use ciphers in which the algorithm for encrypting and decrypting could be revealed to anybody without compromising the security of a particular message. The main practical problem with secret key encryption is exchanging a secret key.

By the year 1976 Symmetric encryption or secret key cryptography is the use of only a key, both in the encryption and decryption of data.

In 1978 the first public-key cryptosystem that appeared in the open literature is the RSA system, named after its three inventors, Ron Rivest, Adi Shamir, and Leonard Adleman.

In 1982 Wootters and Zurek introduces no cloning theorem, this is used in quantum cryptography that a qubit cannot be copied or amplified without disturbing its original state.

In 1997 Peter Shor proposed his celebrated polynomial-time algorithms for factoring integers and computing discrete logarithms with quantum computers all cryptosystems whose security is based on the hardness of solving these mathematical problems have become (at least theoretically) vulnerable.

Existing Approaches In Classical Cryptography

There are two kinds of cryptosystems: **symmetric** and **asymmetric[4]**.Symmetric cryptosystems use the same key (the secret key) to encrypt and decrypt a message, and asymmetric cryptosystems use one key (the public key) to encrypt a message and a different key (the private key) to decrypt it. Symmetric cryptosystems are also called as ***private key*** cryptosystems and asymmetric cryptosystems are also called as ***public key*** cryptosystems. The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are the common approaches that come under symmetric key cryptography.

RSA belongs to asymmetric cryptosystems. It is the first algorithm known to be suitable for signing as well as encryption. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. But all these techniques of classical cryptography suffer from problems of less security and more complexity.

III. Problem Analysis

Every process of encryption and decryption is necessarily associated with a key, the combination used for encryption and or decryption and an algorithm .The requirement of same key as in case of symmetric key cryptography leads to a common problem called a problem of key distribution and in the case of asymmetric key cryptography, it is problematic to get the key pair generated for the encryption.

There are three main problems with encryption schemes:

1. ***Key distribution***:

It requires a secure mechanism to deliver keys properly.

2. Key management:

Here the number of keys required in a system with a large number of principals does not scale well.

3. Security of message

As computing power increases, and new classical computational techniques are developed, the length of time that a message can be considered secure will decrease, and numerical keys will no longer be able to provide acceptable levels of secure communications.

IV. Proposed Work

Key Generation

The most widely used public key system is RSA, which relies on the fact that factoring two large prime numbers is an NP hard problem [5]. Factoring a number that is hundreds of digits long will take millions of years using even the fastest supercomputer. Relying on the hardness of mathematical problems has been the crutch of classical cryptography because whenever computers make gains in terms of computing power, classical cryptography can simply increase the key length, which effectively doubles the key space with each bit.

Quantum computers, uses the laws of quantum physics and could possibly be able to crack any of the most sophisticated encryptions in use today in a year rather than millions of years. Quantum computers can be in multiple states at once as well as act on all of its states simultaneously [9].

In Quantum Cryptography, quantum property of light is used to generate key. Photon has a property called polarization**,** which is the plane in which the electric field oscillates. Their polarization state can be linear or circular, or it can be elliptical, which is anywhere in between of linear and circular polarization. We can use photons of different polarizations to represent quantum states. Each of these photons is in a state denoted by one of the four following symbols:—, |, /, \ The first two photon states are emitted by a polarizer which is set with a rectilinear orientation and the other two states are emitted by a polarizer which is set with a diagonal orientation.

In order to communicate, a coding system is necessary. State | codes 1, while— codes 0, and State \ codes 0, while / codes 1+(0)= —, +(1)= | , x(0)= \ , x(1)= /

For example: If Alice wants to transmit the conventional bit 0 or 1, she may choose to use + and consequently send out over the quantum channel —, |, or choose to use x and consequently send out /, \

If Alice is sending only | and— to Bob, the coding system shall identify that Alice is using the base +. For example, if Alice sends sequence of photons: | , | ,— ,— ; the binary number represented with these states is 1100. Now, if Bob wants to obtain a binary number sent by Alice, he needs to receive each photon in the same basis. In this case, this is + basis. A device called a polarizer allows us to place a photon in a particular polarization. The polarization basis is the mapping we decide to use for a particular state.

QUANTUM KEY DISTRIBUTION

Quantum mechanics has multiple cryptographic applications as well. The best known is quantum key distribution (QKD) which enables Alice and Bob to create a secure classical secret key despite the potential presence of an eavesdropper. QKD requires only an insecure quantum channel and authenticated classical channels, but unfortunately requires multiple rounds of back and forth communication between Alice and Bob.

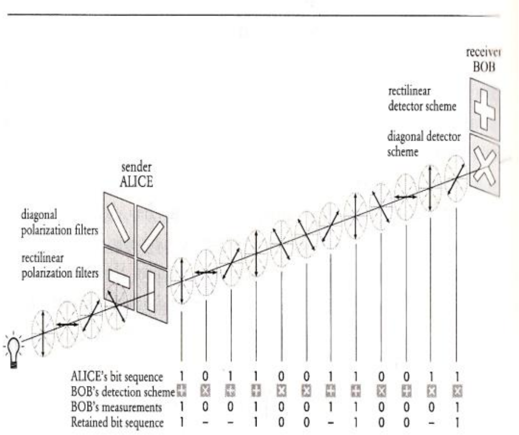
QKD is a means of distributing keys from one party to another, and detecting eavesdropping. It always two parties to establish a common random secret key by taking advantage of the fact that quantum mechanics does not allow for distinguishing non-orthogonal states with certainty.

The primary proposed application of QKD is to create a secret key, which is then used with the one-time pad to send unconditionally secure messages. One of the best-known protocols for quantum key distribution is usually called BB84.

Securing Key Distribution

The representation of bits through polarized photons is the foundation of quantum cryptography that serves as the underlying principle of quantum key distribution [10]. Thus, while the strength of modern digital cryptography is dependent on the computational difficulty of factoring large numbers, quantum cryptography is completely dependent on the rules of physics and is also independent of the processing power of current computing systems. Since the principle of physics will always hold true, quantum cryptography provides an answer to the uncertainty problem that current cryptography suffers from, it is no longer necessary to make assumptions about the computing power of malicious attackers or the development of a theorem to quickly solve the large integer factorization problem. Keys can be distributed using quantum cryptography [6] in the following manner. The sender will send the message to the receiver using a photon gun.

The stream of photons will be in one of the four polarization that corresponds to vertical, horizontal or diagonal in opposite directions (0,45,90.135 degree).At the receiver's end the receiver will randomly choose a filter and count and measure the correct photon polarization. Now, receiver will communicate with sender (out-of-band) about their correct measurement (without sending actual measurement values).



ALICE's bit sequence	1	0	1	1	0	0	1	1	0	0	1	1
BOB's detection scheme	⊞	⊠	⊞	⊞	⊠	⊠	⊞	⊞	⊠	⊞	⊠	⊠
BOB's measurements	1	0	0	1	0	0	1	1	0	0	0	1
Retained bit sequence	1	–	–	1	0	0	–	1	0	0	–	1

Figure:2 Working of Quantum Cryptography

The photons that were incorrectly measured will be discarded and the correctly measured photons will be translated into bits based on their polarization. Now, sender and receiver will generate one time pad combining their results. This one-time pad will be used in one time information exchange between them. None of them can know the actual key in advance because the key is the product of both their random choices. Now, if an attacker tries to eavesdrop, he must select the correct filter otherwise the photon will get destroyed. Even if attacker is able to successfully eavesdrop, the information which he will get will be of little use unless he has the knowledge of correct polarization of each particular photon. As a result attacker will not correctly interpret meaningful keys and thus be thwarted in his endeavors.

V. BB84 Protocol

Although several exist, a single quantum cryptography protocol will be discussed here. This is sufficient to illustrate the principle of quantum cryptography. The BB84 protocol was the first to be invented in 1984 by Charles Bennett of IBM Research and Gilles Brassard of the University of Montreal. An emitter and a receiver can implement it by exchanging single-photons, whose polarization states are used to encode bit values over an optical fiber. This fiber, and the transmission equipment, is called the quantum channel. They use four different polarization states and agree, for example, that a 0-bit value can be encoded either as a horizontal state or a –45° diagonal one . For a 1-bit value, they will use either a vertical state or a +45° diagonal one.

For each bit, the emitter sends a photon whose polarization is randomly selected among the four states. Here fords the orientation in a list.

- The photon is sent along the quantum channel.
- For each incoming photon, the receiver randomly chooses the orientation – horizontal or diagonal – of a filter allowing distinguishing between two polarization states. He records these orientations, as well as the outcome of the detections – photon deflected to the right or the left.

VI. CONCLUSION

Quantum cryptography promises to revolutionize secure communication by providing security based on the fundamental laws of physics, instead of the current state of mathematical algorithms or computing technology. Hence, the resulting Quantum Cryptosystem is more secure and cannot be cracked easily. Within the next few years, such systems could start encrypting some of the most valuable secrets of government and industry.

REFERENCES

[1]*Feynman, R.P.* Simulating physics with computers // International Journal of Theoretical Physics. — 1982. — V. 21. — Number 6. — P. 467—488

[2] Inoue, K. 2006, "Quantum Key Distribution Technologies", IEEE journal of selected topics in quantum electronics, 12, (4), 888 - 896 .

[3] Homer, Iliad 6.213, transl. Ian Johnston (in English), Malaspina University-College, Nanaimo, BC, Canada (2000).

[4]P. Shor, J. Priskill, “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol”, Physical Review Letters, Vol. 85, pp. 441 - 444, 2000.
[5] Adleman, L., Rivest, R., Shamir, A 1978., “A method for obtaining digital signatures and public key cryptosystems”, Communications of the Association for Computing Machinery.
[6] Nicolas Gisin, Gr´egoire Ribordy, Wolfgang Tittel and Hugo Zbinden." Quantum cryptography" (April 1, 2007; submitted to Reviews of Modern Physics)
[7]W. Stallings. *Network and internetwork security: principles and practice*. Prentice-Hall, Inc.,1995.
[8]Bennett, C. H.1992, “Quantum cryptography using any two non orthogonal states”, Physical Review Letters, 68, (21), 3121–3124.
[9] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Physical Review Letters*, **95**(1):010503, 2005. DOI:10.1103/PhysRevLett.95.010503.
[10]Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, **78**(17):3414–3417, April 1997. DOI:10.1103/PhysRevLett.78.3414.
[11]Goel, R., Garuba, M., Girma, A. 2007, “Research directions in quantum cryptography”, Information Technology 2007 ITNG '07 Fourth International Conference, 779-784.

© 2014, IJCSMC All Rights Reserved