**A Project/Dissertation Review-2 Report**

on

**A REVIEW ON QUANTUM CRYPTOGRAPHY**

***Submitted in partial fulfillment of the***

***requirement for the award of the degree of***

B.TECH (CSE)



**Under The Supervision of**

**S JANARTHANAN**

**Assistant Professor**

Submitted By

**KARANJEET SINGH 21SCSE1011644**

**ABHINAV KUMAR CHOUDHARY 21SCSE1011615**

**SHIVANI KUMARI 21SCSE1011614**

**EBAD ZAFAR 21SCSE1011484**

**SCHOOL OF COMPUTING SCIENCE AND ENGINEERING DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**GALGOTIAS UNIVERSITY, GREATER NOIDA**

**INDIA**

**OCTOBER,2022**

**Table of Contents**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Title** | |  | | | **Page No.** |
| **Abstract** | | | | | **I** |
| **Chapter 1** | **Introduction** | | | | **1** |
|  | 1.1 | | Introduction | | **2** |
|  | 1.2 | | Methods and Concepts | | **3** |
|  | 1.3 | | Problem formulation |  |  |
| **Chapter 2** | **Literature Survey/Project Design** | | | | **5** |
|  | 2.1**References** | | | | **6** |

**ABSTRACT**

In today era of technology, a secure way of communication is very vital between sender and receiver, that is being done with the cryptographic algorithmlike RSA and DES. These are on the beneath of elliptical cryptography but there reversibility only depend on the complex functions of mathematics thatare used in algorithm. Today we have enhanced our computational power exponentially in quantumcomputer as compare to classic computer. conventional algorithm are no more uncrackable.so solution to this, we have new field that introduces quantum physics to cryptography which gives unique way of datasecurity that isuncrackable with today present technology called quantum cryptography.in our scope of this paper we made an endeavor torepresent the fundamentals of quantum cryptography and logical view on quantum key distribution with some gaps that need to be filled to implement this technology to real world

**Problem formulation**

we are mainly facing a problem in quantum cryptography that demand its own new large infrastructure and inability to make polarized photons to make move large distance with real world noise that effect quantum environment of photon. So we make an attempt to give some detail on quantum key distribution so that we can efficiently use theseprotocolsand try to find out correlation that makes photons a more secure and safe way of communication with larger distance.

**Literature Survey**

All today algorithm are based on the difficulty of mathematical concept .If we take a look back focus on era when cryptography is paving his way in the world we did not have so computational power .At the beginning of the twentieth century, 1917, the well-known One Time Pad (OTP) encryption was introduced by Verman . In 1940, the seminal paper of Shannon 15 changed the way to look at cryptography. He put forth a very fundamental idea of Information theoretic Security i.e., the cipher text should not reveal the information about the plain text. Cryptography was thereafter viewed as more applied stream of mathematics and information theory. After introducing the concept of public key cryptography in 1976 we came across a very successful algorithm called RSA in 1978.Now we came across a problem of very lengthy keys that slower the system and increase execution time .To overcome this problem the solution that came up was the elliptical curve cryptosystem. Elliptical curve cryptosystem was discovered in 1985 by Victor Miller and Neil.Moving in field of cryptography in 1983 bennett andwiesner introduced quantum coding that is recently a pervading in our society.

CHAPTER-3

Methodology /Implementation

3.1 Entanglement

A phenomenon that generates quantum state of fundamental particles in such a way that they cannot be defined independently. Firing a laser through a crystal and splitting a single photon into two can allow one to create entangled photons. Intuitively, by the laws of physics, their state is intact and disturbing one will instantly disturb the other regardless of the distance.

3.2 Photon Polarization

.Polarization is holistically, the means orientation as it originates from the Greek word ”polos”, the axis of a spinning globe. The quantum superposition of eigen states create different types of polarizations such as linear, circular or elliptical. Further, these photons carry energy, momentum as well as an angular momentum.

A phenomenon that generates quantum state of fun-

damental particles in such a way that they cannot

be deﬁned independently. Firing a laser through a

crystal and splitting a single photon into two can al-

low one to create entangled photons. Intuitively, by

the laws of physics, their state is intact and disturb-

ing one will instantly disturb the other regardless of

the distance

3.3 Heisenberg Uncertainty Principle

It says that the more accurately we know any one of this value the very less we know the other. In the combination of their uncertainty, it generates a number the is greater than or equal to half of Planck’s constant h¯. Mathematically, the uncertainty principle is depicted as,

∆x∆p >= h¯ /s.

CHAPTER- 4

Result analysis and conclusion

Technically, a photon generator placed between Alice and Bob at the same time sends pairs of entangled photons with the same polarization to Alice and Bob. Both measure the signals with an alternating random bases and after the comparison discard the bits are measured with different bases. The phenomena of entanglement allows this communication to remain ultimately secured as any activity to intrude on either one of the states will immediately affect the other allowing detection of an eavesdropping

4.1 Qubit supremecy

The strength of quantum computing lies within the basic model on which it operates “Qubits”, it works on the principle of superposition which means the qubit can take either 0 or 1 at the same time. This property brings the increment in power for computation exponentially (2𝑞) where n is number of qubits.

4.2 Quantum cryptography protocols

BB84 protocol simulation

It begins with an emitter and a receiver (connected via an optical fiber) using four different polarization states to encode bit values, a 0 deg-bit as horizontal, a 45 deg diagonal or as a 1 deg-bit value with either a vertical or a +45 deg diagonal state. The emitter sends photons with random polarization selected among the four of them. The random orientations are recorded in a list and the photons are sent along the quantum channel. For the incoming photons, random orientation of the states filter allow us to distinguish in between the two polarization states of photons. These orientations are an outcome of the detected photons.

Conclusion

Though there are imperfections and the technology still has its own constraints towards commercial implementations, it has seen a tremendous growth recently.

The future of quantum computing looks bright as quantum computing has many applications like quantum cryptography, Teleportation of information. It also can be used in development of medicines by studying molecular behaviour, It also can be used in satellite communications as well. However, we hope that the theory becomes practical someday so we can use its advantages in many other fields of science.

The conclusion of the Thesis is that quantum computing is one of the huge opportunities for the modern world to open up the doors for unanswered questions. It promises to solve problems which classical computers practically cannot. But the cost behind quantum computing is too high. The major challenges that stands right now is to reduce the cost so that it is more accessible for experiments.

Consequently, we should realize that fundamental knowledge of such systems is an important element of the future. Computer scientists must understand these fundamental laws of nature to be able to develop new algorithms and new distribution schemes for its practicality. All we need now are a few more years to finally bring the realms of this technology to the commercial and consumer world.

references