**A Project/Dissertation Review-1 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 algorithm like RSA and DES. These are on the beneath of elliptical cryptography but there reversibility only depend on the complex functions of mathematics that are used in algorithm. Today we have enhanced our computational power exponentially in quantum computer 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 data security that is uncrackable with today present technology called quantum cryptography.in our scope of this paper we made an endeavor to represent 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 these protocols and try to find out correlation that makes photons a more secure and safe way of communication with larger distance.

**METHODS AND CONCEPTS**

Quantum superposition : Every quantum state can be represented as a sum of two or more other distinct states .A quantum bit can exist in superposition, which means that it can exist in multiple states at once. Compared to a regular bit, which can exist in one of two states, 1 or 0, the quantum bit can exist as a 1, 0 or 1 and 0 at the same time. This allows for very fast computing and the ability to do multitudes of calculations at once, theoretically .

Quantum state replication limit : we can not measure any quantum state without disturbing the quantum environment so if any eve dropper tries to stole/replicate our quantum state we can easily guess that so that makes the quantum cryptography secure.

Heisenberg uncertainty principle: Two conjugate variables that are supposed to measure in a experiment have a inherent uncertainty in their measurement in simple words

**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 and wiesner introduced quantum coding that is recently a pervading in our society.

**References:**

* + Bennett ch quantum cryptography :letter 1992,68(21):3121-24
  + quantum cryptography –research gate
  + IEEE journal on quantum cryptography
  + [www.quantlr.com](http://www.quantlr.com)
  + www.goooglescholar.com