Topic

“A REVIEW ON QUANTUM CRYPTOGRAPHY USING ENCRYPTION AND DECRYPTION ”

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 their 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.

Table of Contents

CHAPTER-1

Introduction

Basically in simple words you can understand as the transformation of information(data) in unreadable form(meaning less) by some rule is called cryptography .The process of converting the message into some disguised form is called Encryption . The encrypted data is called ciphertext. The logic(or extra thing)used in encryption in called key. In secret key cryptography, a key is common to both end called symmetric cryptography and if key is not symmetric is called Asymetric cryptography. Limitations of symmetric key cryptography, particularly, key distribution was the reason that the asymmetric cryptography started gaining the importance over the time period. Eventually, elliptical curve cryptography known as modern cryptography is being used extensively for securing financial transactions. Advances in quantum computing, can easily break this security by reverse computing keys faster than the conventional computer. Quantum cryptography was originated by Bennett , Bassard and Wiesner13. Quantum coding was first introduced by Wiesner15 in 1983. Then Bennet and et.al.17 used quantum coding in conjunction with public key cryptographic techniques to yield several schemes for unforgeable subway tokens. Several others contributed to quantum cryptography and quantum key distribution. Though quantum computing is not that feasible, quantum cryptography is achievable over shorter distance.

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.

Literature Survey

All today algorithm are based on the difficulty of mathematical concept. If we take a look back to focus on that 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 crypto-system. 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.

CHAPTER-3

Methodology /Implementation

3.1 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.

3.2 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.

3.3 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.

3.4 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 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.

3.5 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,

$$\Delta x.\Delta p >= h^{-} /s.$$

CHAPTER- 4

Result analysis

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 supremacy

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.

Chapter 5

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

- Minor thesis quantum heap nov 2020:by Manish Y
- Research paper on quantum cryptography from
- googlescholar.com
- Brassard, G. Cryptology column — 25 years of quantum cryptography. Sigact News 27(3) (1996), 13–24.
- Gottesman, D., and Lo, H.-K. From quantum cheating to quantum security. Physics Today 53, 11 (Nov. 2000), 22.
- Lo, H.-K. Quantum Cryptology. World Scientific, 1998.
- Singh, S., 1999, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (Fourth Estate, London).
- Stanford university research paper: J. Aditya, P. Shankar Rao {Dept of CSE, Andhra University} Conference paper 2020 november: by azeem iqbalSahar nayab

This project is contributed by Vikas Singh, Ghanshyam Kumar and Ritik Singh