**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**Design and Analysis of Algorithms**

**TERM: March - July 2022**

**QUANTUM CRYPTOGRAPHY**

# PROJECT SYNOPSIS

**PROJECT TEAM MEMBERS**

|  |  |  |
| --- | --- | --- |
| **Sl. No** | **USN** | **Name** |
| 1. | 1MS20CS098 | S D HRUDHAY |
| 2. | 1MS20CS099 | SAFWAN G A |
| 3. | 1MS20CS100 | SAI ISHWARYA S |
| 4. | 1MS20CS107 | SANSKAR R G |

SUPERVISED BY

Faculty

Dr. S. Rajarajeswari

**CONTENTS**

|  |  |  |  |
| --- | --- | --- | --- |
| **SL**  **No.** | **Topic** | **Page No.** | |
| **1** | **Problem Statement** | 3 | |
| **2** | **Objectives** | 3 | |
| **3** | **Literature Review** | 4 | |
| **4** | **Research Gaps** | 6 | |
| **5** | **Proposed System** | 7 | |
| **6** | **Algorithm pseudocode** | 8 | |
| **7** | **Analysis of algorithm** | 9 | |
| **8** | **Data structure used** | 11 | |
| **9** | **Applications** | 11 | |
| **10** | **References** | 11 | |
|  |  |  |  |

**QUANTUM CRYPTOGRAPHY**

**PROBLEM STATEMENT:**-

**“**As the foundation of modern security systems, cryptography is used to secure transactions and communications. Classical cryptography does this by employing approaches that rely on the currently true, ‘fact’ that traditional computers are incapable of factoring huge integers into their prime factors using a polynomial-time algorithm. However, this is also one of its flaws. The goal is thus to make a cryptographic solution that isn’t reliant on assumptions.**”**

* This is significant because if someone discovers a means to factorize huge prime numbers, all "safe" data will suddenly be vulnerable, and all major organizations and governments must halt all communications relying on that type of encryption until a solution is found, and quickly. This will cause substantial delays and costs, crippling any enterprises that rely on them. As a result, a solution to this impending catastrophe must be devised ahead of time.
* These issues are handled in quantum cryptography by quantum key distribution. Because this kind of encryption is based on the unchangeable principles of physics in terms of information, it is regarded absolutely secure in theory.

**OBJECTIVES:**-

The objectives for encryption moving forward are:

1. To stay relevant with the passing of time.

1. To not be dependent on a computer’s capabilities.
2. To alert the parties concerned when communication is being eavesdropped into.
3. To destroy data if it was attempted to be decrypted using the wrong key or interpreter.

**LITERATURE REVIEW:**-

|  |  |  |  |
| --- | --- | --- | --- |
| **Title, Author and Year** | **Technique used** | **Result** | **Remarks** |
| Paper title: Quantum cryptography.  Author: Maneesh Yati.  Journal name: researchgate.  Year: 2020. | Quantum Key  Distribution | The result is a mutual key known uniquely to them is created, which can be utilized as a key to scramble and decode messages. | In the research paper, Quantum cryptography and its advantage over conventional cryptography are explained in detail with concepts like cryptanalysis which can help immensely when quantum cryptography is accepted completely. |
| Paper title: Quantum Cryptography for the Future Internet and the Security Analysis.  Author: Tianqi Zhou.  Journal name: Hindawi. Year: 2018 | Quantum Key  Distribution protocol | The unconditional security and sniffing detection of quantum cryptography, which makes it suitable for future Internet. | This research paper presents benefits that quantum  cryptography brings to the future Internet and analyse the security of it. |
| Paper title: Quantum Cryptography using Quantum Key Distribution and its Applications. Author: N.Sasirekha.  Journal name: Blue Eyes  Intelligence Engineering & Sciences Publication Pvt. Ltd.  Year: 2014. | Quantum Key  Distribution,  One-time pad | The result is implementation of Quantum Key  Distribution. | This paper concludes that to transmit sensitive information between two or more points, some stronger technique is needed which is Quantum Key Distribution. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Paper title: Post Quantum cryptography.  Author: Shipra Srivastava.  Journal name: Academia.  Year: 2021. | | Shor’s  Algorithm, Grover’s Algorithm, quantum-safe symmetric algorithm | The result is that classical encryption methods isn’t completely resistant. | This paper explains in detail the devastating impact of Shor’s and Grover and explains how it works. This paper also focuses on the quantumsafe symmetric algorithm such as 256 bit in details. This paper can help upcoming researchers to understand the differences and perform better in their respective research fields. | |
| Paper title: Eavesdropping  Detectable Data Transmission by Applying Quantum Cryptography.  Author: TAKUMI Ichi.  Journal name: The Institute of Electronics, Information and Communication Engineers.  Year: 1999. | | Quantum entanglement and bell  inequalities,  Quantum Key  Distribution | The result proposes a secure data transmission scheme in which an eavesdropping can be  detected | In this paper, we study the properties of the data transmission scheme by applying various eavesdropping schemes. Furthermore, we improve this data transmission scheme. | |
| Paper title:Quantum cryptography: An emerging technology in network security**.**  Author: [Mehrdad S. Sharbaf.](https://ieeexplore.ieee.org/author/37313938100)  Journal name: IEEE.  Year: 2011. | | Quantum Key  Distribution | The result is the implementation of Quantum Cryptography to contribute for network securities. | This research paper concentrates on quantum cryptography, and how this technology contributes to the network security. The scope of this research paper is to cover the weaknesses, and the security pitfalls in modern cryptography, fundamental concepts of quantum cryptography,  the real - world application implementation of this technology, finally the future direction in which the quantum cryptography is headed forwards. | |
| Paper title: Post Quantum  Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research.  Author: Ritik Bavdekar.  Journal name: researchgate.  Year: 2022. | | Shor’s  Algorithm,  Quantum Key  Distribution | The result is that classical encryption methods isn’t completely resistant and it’s only a matter of time they become broken. | This paper analyzes the vulnerability of the classical cryptosystems in the context of quantum computers, discusses various postquantum cryptosystem families,  discusses the status of the NIST post-quantum cryptography standardization process, and finally provides a couple of future research directions in this field. | |
| Paper title: Quantum Cryptography for Internet of Things Security.  Author: Anand Sharma.  Journal name: [Electronic Science and Technology.](https://www.sciencedirect.com/journal/journal-of-electronic-science-and-technology)  Year: 2019. | | Quantum Key  Distribution | The result is that the distance which quantum communications can be done is very less due to the properties of photons, which restrict them to travel long distances. If these issues are resolved, we can have successful IoT systems with quantum cryptography applied to them, making them the most secure systems to date. | In this research paper the analysis has been carried out in terms of the pros and cons of implementing quantum cryptography for IoT security. | |
|  |  | |  |  |  |

**RESEARCH GAPS IDENTIFIED:**-

Quantum key distribution has a few disadvantages in practice, such as:

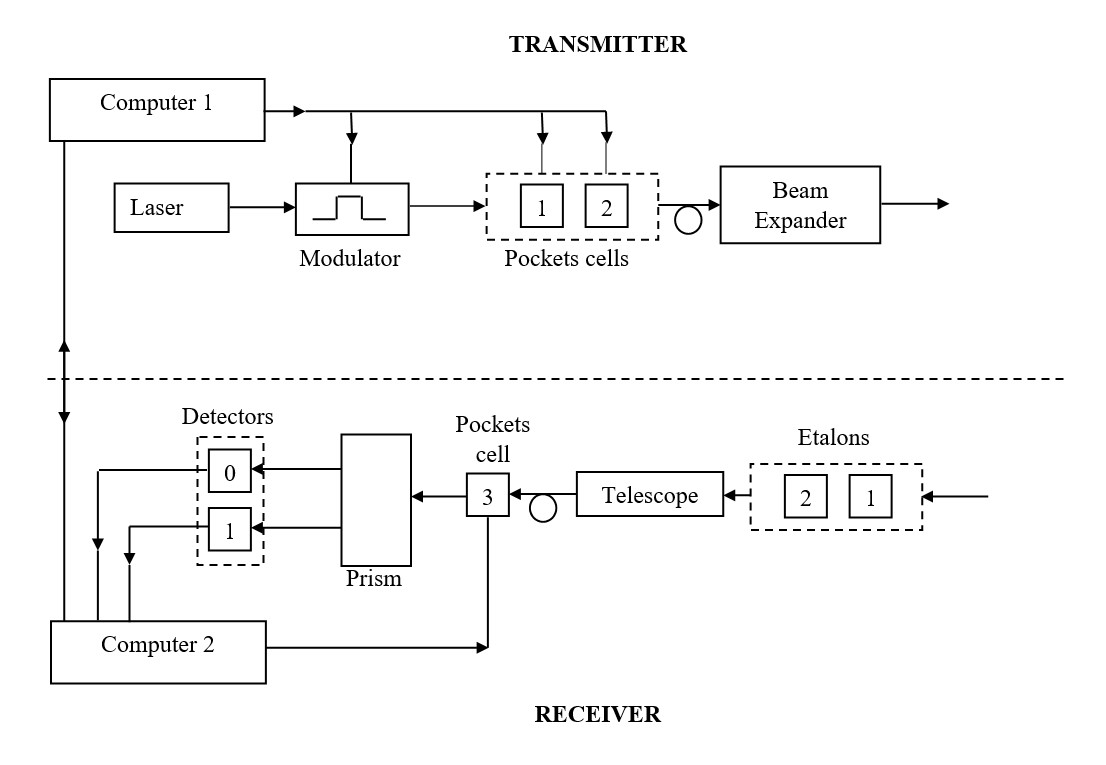
1. Changes in polarization and error rates: Photons may change polarization in transit, which potentially increases error rates.

2.Range: The maximum range of quantum cryptography has typically been around 400 to 500 km.

3.Expense: Quantum cryptography typically requires its own infrastructure, using fiber optic lines and repeaters.

4.Number of destinations: It is not possible to send keys to two or more locations in a quantum channel.

**PROPOSED SYSTEM:**-



Here the devices are for the following uses:

* Laser is the photon projector; modulator modulates it to a given bit .
* Pocket cells align it with a certain random polarizer .
* Beam expander makes the beam of photons detectable by distributing it over a larger area.
* Prism separates different spectrums of photons, to make it possible that the detector only detects photons of a given frequency. Detector detects photons.
* The controlling computers on each send instructions to the laser and pocket cells and communicate among themselves about the polarizer they used during the entire communication of key.
* The etalon is a device consisting of two reflecting glass plates, employed for measuring small differences in the wavelength of light using the interference it produces. It is used to make sure only the right wavelength is being measured.

**SIMPLE PSEUDOCODE OF ALGORITHM:**-

*GenerateQuantumKey(N)*

*//Input: N, an integer max length of key*

*//Output: Qk[] binary key of length k*

*Initialize Qk1[], Qk2[], Qk[]*

*// Qk1 is the transmitted key via sender, Qk2 is the received key via receiver for i ← 0 to N-1*

*Qk1[i].polarisation ← randomOf(diagonal, vertical and horizontal)*

*Qk1[i].value ← randomOf(0,1)*

*Endfor //sender now has initialised value for themselves*

*i ← 0*

*while(i<N)*

*Qk2[i].polarisation ← randomOf(diagonal, vertical)*

*If Qk2[i].polarisation = Qk1[i].polarisation*

*Qk2[i].value ← Qk1[i].value*

*Else*

*Qk2[i].value ← randomOf(0,1)*

*i++*

*Endif*

*Endwhile*

*//this portrays the values received by the receiver after randomizing the polariser*

*i ← 0*

*k ← 0*

*while(i<N)*

*if Qk1[i].polarisation = Qk2[i].polarisation*

*Qk[k++]=Qk1[i].value*

*Endif i++*

*Endwhile*

*returnQk[]*

*//only storing values where polarizers used are same, discarding others*

*randomOf(a1,a2)*

*//Input: two unknown values*

*//Output: one or the other value selected randomly i ← randomInt()*

*if i%2 = 0*

*return a1*

*else*

*return a2*

*Endif*

**ANALYSIS OF CHOSEN ALGORITHM:**-

This algorithm is the quantum key distribution algorithm. It relies on the following postulates of quantum theory:

* Measuring a particle alters its state
* It is impossible to generate a complete copy of a particle after measuring it

The transmission of data happens through a fiber optic cable, via photons. One photon per signal is preferably used. The sender uses a random polarizer and sends a random bit through it via a map similar to the one below:

* If polarizer is vertical (in the shape of +), then polarized light pointing up is 1 and sideways is 0.
* If polarizer is diagonal (in the shape of x), then polarized light pointing right-up is 1 and right-down is 0.

The receiver chooses a random polarizer on their end and puts their received photon through it. They store the obtained data along with the polarizer used side by side in an array, as did the sender while sending it.

They now compare their polarizers via communication in a public channel, and for each transmitted bit where their polarizers used were same, they retain the data, otherwise they delete it. They use the remaining bits as a key to send data via classical cryptographic means.

The advantage of this algorithm, is that if someone manages to eavesdrop on the quantum key communication, it will alter the photon being transmitted. This will cause the receiver not receiving the data, and will alert both the sender and receiver. If the eavesdropper tries to replicate the photon, since they don’t know which polarizer to use, their chances of accurately measuring the qubit are 50%, before they send it to the receiver.

The receiver has also chosen the polarizer randomly, and thus it is very likely that the bits measured by the eavesdropper and receiver may not align, and they may thus send it in wrong polarization and bit. This will cause the key received by the receiver to be different than the one sent by the sender, and thus the sender won’t be able to decode the data they later receive, alerting them. In any case, since while the communicators are comparing polarizers, they only choose the ones they got the same, which the eavesdropper may not have gotten, the eavesdropper will not have the complete key, and can’t thus decode the information being transmitted through public channel encrypted with that key. So the eavesdropper doesn’t get the key either.

The chances the eavesdropper got the key wrong is thus:

**P(wrong) = 1 – (1/2)^n**

Where n is the number of qubits being transmitted. We can see that it nears 100% when n is large enough.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Statement** | **S/E** | **Average**  **Frequency** | **Total steps** |
| **1** | Initialize Qk1[], Qk2[], Qk[] | 0 | - | **0** |
| **2** | for i ← 0 to N-1 | 1 | N+1 | **N+1** |
| **3** | Qk1[i].polarisation ← randomOf(diagonal, vertical and horizontal) | 6 | N | **6N** |
| **4** | Qk1[i].value ← randomOf(0,1) | 6 | N | **6N** |
| **5** | Endfor | 0 | - | **0** |
| **6** | i ← 0 |  |  |  |
| **7** | while(i<N) | 1 | N+1 | **N+1** |
| **8** | Qk2[i].polarisation ← randomOf(diagonal, vertical and horizontal) | 6 | N | **6N** |
| **9** | If Qk2[i].polarisation = Qk1[i].polarisation | 1 | N | **N** |
| **10** | Qk2[i].value ← Qk1[i].value | 1 | N/2 | **N/2** |
| **11** | Else | - | - | **0** |
| **12** | Qk2[i].value ← randomOf(0,1) | 6 | N/2 | **6N/2** |
| **13** | i++ | 1 | N | **N** |
| **14** | Endif | 0 | - | **0** |
| **15** | Endwhile | 0 | - | **0** |
| **16** | i ← 0 | 1 | 1 | **1** |
| **17** | k ← 0 | 1 | 1 | **1** |
| **18** | while(i<N) | 1 | N+1 | **N+1** |
| **19** | if Qk1[i].polarisation = Qk2[i].polarisation | 1 | N | **N** |
| **20** | Qk[k++]=Qk1[i].value | 2 | N/2 | **N** |
| **21** | Endif | 0 | - | **0** |
| **22** | i++ | 1 | N | **N** |
| **23** | Endwhile | 0 | - | **0** |
| **24** | return Qk[] | 0 | - | **0** |
|  |  |  |  |  |
| **25** | randomOf(a1,a2) | 0 | - | **0** |
| **26** | i ← randomInt() | 1 | 1 | **1** |
| **27** | If i%2 = 0 | 2 | 1 | **2** |
| **28** | return a1 | 1 | 1 | **1** |
| **29** | Else | - | - | **0** |
| **30** | return a2 | 1 | 1 | **1** |
| **31** | Endif | 0 | - | **0** |
| **Total Steps for Algorithm** | | | **(59N/2)+3**  **(:.Time complexity is O(N))** | |

Since the number of qubits sent and of which polarization was verified are the same, and since n is the input size, the basic step is executed 2n times, which puts it in time complexity O(n) which concludes the fact that the algorithm runs in polynomial-time.

**DATA STRUCTURE USED:**-

The data structure being used is an array. The sender and receiver both have to maintain the data about what bit they received and what polarizer they used while receiving it. By using an array with two compartments, such as one defined on a structure or two different arrays entirely on each side, they can store the information for the time they will get around to comparing the polarizers.

Since the data structure is simple, the data storage throughout the transmission doesn’t need a lot of storage to work, which is especially useful since modern techniques like the One-Time-Pad use a key longer the data itself to encrypt the data and they key might become very big, to store.

**APPLICATIONS:**-

Quantum key distribution has been successfully applied in various areas in the current world, such as:

1. It is used to safeguard banking information.

1. It can be used to encrypt sensitive information like government files during transmission. In which case it is preferred to delete files rather than let them fall into the hands of the enemy.

1. Mis-trustful quantum key cryptography: when one party is unsure of the goodwill of the others.

**REFERENCES:**-

1. Bennet, C.H., and Brassard. Quantum public key distribution reinvented. Sigact news 18(4) (1987), 51-53.

1. Bennett, C.H., and DiVincenzo, D.P. quantum information and computation. Nature 404 (2000), 247-55.

1. Bennett, C.H, Brassard. And Ekert, A.K. Quantum cryptography. Sci. Am. 267, 4 (Oct, 1992), 50

1. Bennett, C. H., and Shor, P. W. Quantum information theory. IEEE Transactions on Information Theory 44, 6 (1998), 2724–42.

1. Brassard, G. Cryptology column — 25 years of quantum cryptography. Sigact News 27(3) (1996), 13–24.

1. Tianqi Zhou, Jian Shen , Xiong Li, Chen Wang ,and Jun Shen; Quantum Cryptography for the Future Internet and the Security Analysis, Hindawi Security and Communication Networks Volume 2018.
2. Maneesh Yati, Deakin University; Quantum Cryptography; November 2020.
3. N.Sasirekha, M.Hemalatha; Quantum Cryptography using Quantum Key Distribution and its Applications; International Journal of Engineering and Advanced Technology (IJEAT); April 2014.
4. Shipra Srivastava, Dr. Anoop Tiwari, Dr. Ramveer Singh; Post Quantum Cryptography: A Literature Review; ISSN: 0974-5823; Vol. 6 No. 3 December, 2021.
5. KUDO Takamitsu,SASAKI USUDA Tsuyoshi,TAKUMI Ichi,HATA Masayasu; Eavesdropping Detectable Data Transmission by Applying Quantum Cryptography; Technical report of IEICE. ISEC 99 (584), 151-158, 2000-01-25.
6. Mehrdad S. Sharbaf; Quantum cryptography: An emerging technology in network security; 2011 IEEE International Conference on Technologies for Homeland Security (HST).
7. Ritik Bavdekar, Eashan Jayant Chopde, Ashutosh Bhatia, Kamlesh Tiwari, Sandeep Joshua Daniel, Atul; Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research; Birla Insitute of Technology and Science Pilani; 6 Feb 2022.
8. Alekha Parimal Bhatt, Anand Sharma; Quantum Cryptography for Internet of Things Security; Electronic Science and Technology, Volume 17, September 2019.