**A PROJECT REPORT**

**ON**

**FUTURE AND SCOPE OF QUANTUM COMPUTING CRYPTOGRAPHY**

Submitted in partial fulfillment of the requirement for the III semester

**Bachelor of Technology**

**By**

# Shrinkhal

## **2019123**



**DEPARTMENT OF COMPUTER SCIENCE &****ENGINEERING**

**GRAPHIC ERA DEEMED UNIVERSITY**

### DEHRADUN

**2022-2023**

# CERTIFICATE

This is to certify that the project report entitled “Future and Scope of Quantum Computing Cryptography” is a bonafide project work carried out by Shrinkhal, roll number- 2019123, in partial fulfillment of award of B.Tech degree of Graphic Era Deemed University, Dehradun during the academic year 2022-2023. It is certified that all corrections / suggestions indicated for internal assessment have been incorporated. The project has been approved as it satisfies the academic requirements associated with the degree mentioned.

**Dr. Devesh Pratap Singh**

**HOD (Computer Science)**

# ACKNOWLEDGEMENT

Here by I am submitting the project report on **“Sentiment Classification of news headlines”** as per the scheme of Graphic Era Deemed University, Dehradun.

I would like to express our sincere gratitude to **Dr. Devesh Pratap Singh,** Head of Dept. of Computer Science, for providing a congenial environment to work in and carry out our project.

I consider it my cardinal duty to express the deepest sense of gratitude to Dr. Manoj Kumar Sir for the invaluable guidance extended at every stage and in every possible way. Finally, I am very much thankful to all the faculty members of the Department of Computer Science and Technology, friends and our parents for their constant encouragement, support and help throughout the period of project conduction.

## Shrinkhal Roll no. 2019123

**Problem Statement:**

Future and Scope of Quantum Computing Cryptography.

**Motivation:**

Quantum Computing Cryptography is a science that applies the principles of Quantum mechanics to data encryption and data transmission so that data cannot be accessed by hackers-even those malicious actors that have quantum computing of their own.

Theoretically , this kind of computer aid the development of new , stronger , more efficient systems that are impossible using the existing , traditional computing and communication architectures .

So, being interested in this field, I also explored this topic and tried to build a project of my own.

**Abstract:**

Quantum Computers are not just powerful supercomputers . Instead of computing with the traditional bits of a 1 or 0,quantum computers use quantum bits or q-bits . A classical processor uses bits to perform its operations . A quantum Computers runs q-bits . These q-bits make it possible for the Cryptography to be done by these computers . This project is based on the Future and Scope Of Quantum Computing Cryptography .

**Introduction**

* Cryptography is the process of converting the original text,encrypting it via key after rearranging or manipulating its text without any change in its initial information.
* Only person with the same key can open it.
* Classical computers have been around for long time , played a significant role in the scientific breakthrough.
* In the modern era , quatum computing bears the promising results , solving the complex problems .
* Classical Computers manipulate individual bits whereas the quantum computers use the probability of state’s object before it is measured .
* This survey paper will give the reader a perspective of the “Future And Scope Of Quantum Computing” .

**METHODOLIGIES**

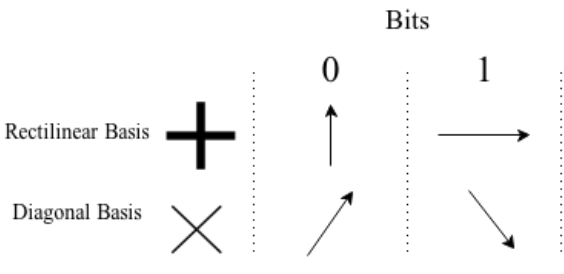
**I] HEISENBERG’S UNCERTAINITY PRINCIPLE**

* In 9127 German researcher Werner Heisenberg proposed the Heisen uncertainty Principle.
* It said , it will not be possible to accurately determine both the position and velocity at the same time.
* It works when you observe anything.
* Diagram

  Description automatically generated

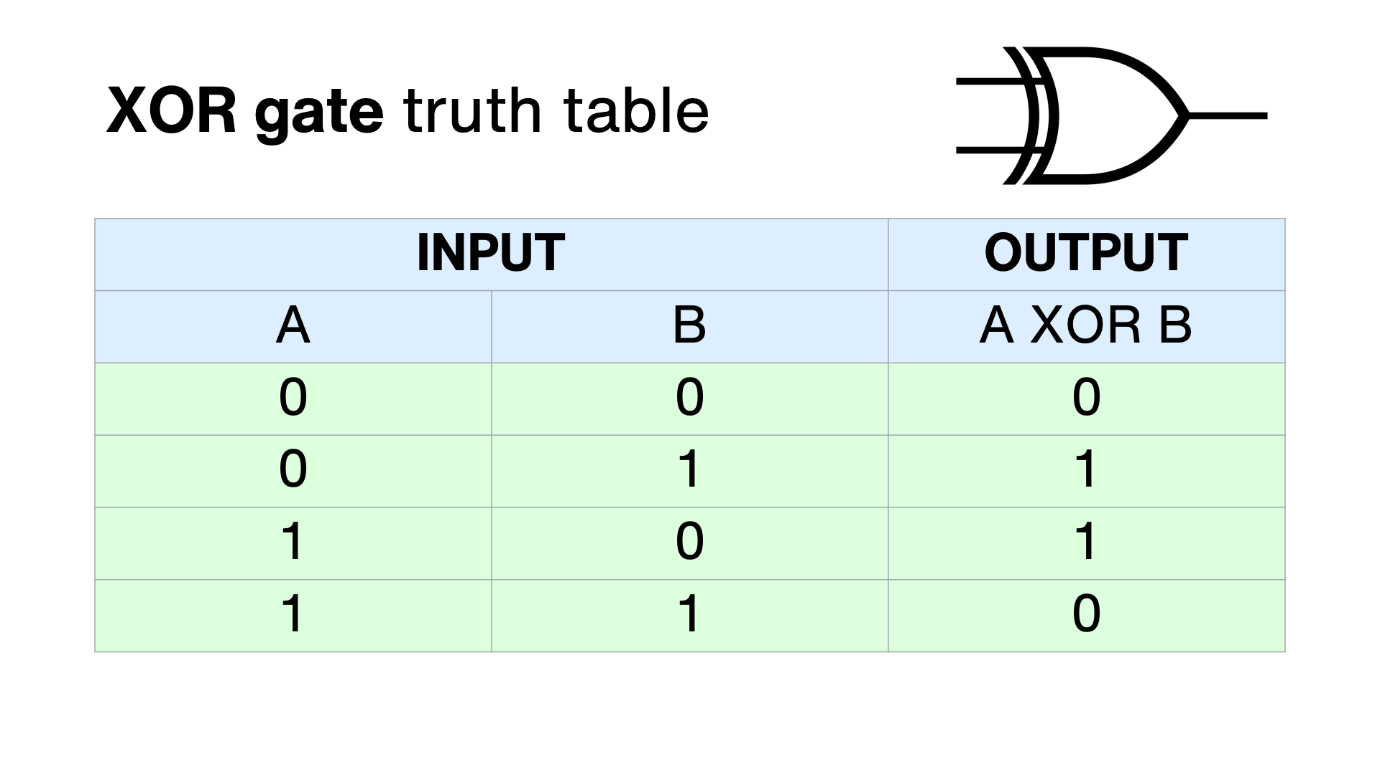
**II] PHOTON POLARISATION PRINCIPLE**

* This principle uses non-cloning methods to ensure that the attacker does not copy unique quantum bits
* This creates a quantum state which cannot be recognized and distorts other information if anyone tries to measure the bit.



**III] PRESENT CRYPTOGRAPHY**

**A] SYMMETRIC CRYPTOGRAPHY**

* User and sender use the same cryptographic algorithm and secret key to encrypt and decrypt data.
* In Symmetric Key Encryption , for convenience , all ciphers utilize the XOR gate.
* **MERIT:**

1. Security :

* Symmetric key encryption is essentially unbreakable.
* It requires the user to keep the track of one key only.
* For e.g. , AES Cipher is 256 bits in size even with a supercomputer a brute force through encryption needs millions of years to crack it.

1. Speed :

* Symmetric Key Encryption is simple as it requires only one key to break it and that also of a shorter length.
* Thus , it is much faster to execute.
* Hence , no burden on the server of encryption and decryption therefore ,
* Efficient handling of data.

**DEMERIT:**

1. Key Distribution :

* To read the message sender and receiver must have the key.
* The safest is too meet face to face and share the key.
* If sent through the internet , it opens the possibility of man in the middle attack.

2 . Key management :

* + - Once encrypted , message can be decrypted only by that particular symmetric encryption key.
    - Attacker gains the key , then he does a software based attack thus , all the encrypted messages get compromised.

**B] ASYMMETRIC CRYPTOGRAPHY**

* There is a private key and a public key , message is encrypted with a public key and it can be decrypted only with the private key.
* Also called public key Cryptography ,where keys come in pair.
* A screenshot of a computer screen

  Description automatically generated with low confidence

**MERIT:**

* Key distribution eliminated , no need to exchange keys.
* Security increased , private key don’t need to be revealed to anyone.
* Allows for the non replication so sender can deny the sending a message.

**DEMERIT:**

* Slow compared to the symmetric cryptography.
* If encryption key is lost the message can never be encrypted.
* There is a possibility that makes the actor identify a person’s key , making individual’s message visible to the attacker.

**C] HASH FUNCTION**

* It is a unique identifier for any given piece of context.
* It is a process that takes plain text of any size and converts it into a unique cipher text of specified length.
* Diagram

  Description automatically generated

**MERIT:**

* Helps in authentication of server and stores the hash values of the passwords , this ensures no sniffing.
* Even Rabin-Karpin algorithm uses hashing to find any pattern in a string.

**DEMERIT:**

* Its is inefficient due to high number of collisions.
* It does not allow NULL Values.

**IV] POST QUANTUM CRYPTOGRAPHY A]QUANTUM KEY DISTRIBUTIION**

* Quantum key distribution utilizes unique property of quantum key mechanics to generate and distribute and distribute cryptographic keying material sing special purpose key technology.

**MERIT:**

* Allow detection of eavesdropping as error level comparatively more when eavesdropper connected to quantum channel.
* Utilization of supreme key permitted by additional encryption using traditional algorithm hence , data security increased.

**DEMERIT:**

* Complete solution of distributing key not provided by in system it supports.
* The Data transfer rate decreases immediately with the rise of channel length.
* Most researched mathematical based implications are as follows :

1. **LATTICE BASED CRYPTOGRAPHY**

* Widely known public – key schemes RSA , Diffie-Hellman elliptic curve cryptosystems get defeated theoretically using the Shore’s algorithm on a quantum computer , lattice based construction is resistant to attack by both classical and quantum computer.

**MERIT:**

* Offers improved security as lattice more difficult to break than any other mathematical striucture.
* Computation is faster than other cryptographic algorithm hence applied in streaming media or online gaming.

**DEMERIT:**

* It is quite difficult to give estimation of security on these systems for an existing software and hardware platforms.
* The implementation on these platforms are vulnerable to physical attack- timming ttack , fault attack etc.

### RESULT AND DISCUSSION

* With **quantum** **computing**, new encryption algorithms can be created which are many times more powerful than the classical **cryptography** we use today. While **quantum** **computing** can have many advantages for **cryptography**, it can also be used by threat actors to create new malware that can break classical **cryptographic** algorithms in half the time or less.

### PROJECT LIMITATIONS

* The concept of Quantum computers is still highly theoretical . The transfer of data still relays on the physical constraints and hence can be tempered in between . All the data transfer relays and repeaters which are quite vulnerable to the tampering.

### CONCLUSION

There are many aspects of quantum computers and applying it in cryptography is one of them. When the quantum computers would change the way of digital transfer of money . Some well prepared business would be able to fully embrace this new technology .This would probably be a revolutionary change .

SOURCE:

* [SSL Certificate Authority & PKI Solutions | Sectigo® Official](https://sectigo.com/)
* [IBM - India | IBM](https://www.ibm.com/in-en)
* [Home - Springer](https://link.springer.com/)
* [Share and Discover Knowledge on SlideShare](https://www.slideshare.net/)
* [Microsoft Research Security & Cryptography, Author at Microsoft Azure Quantum Blog](https://cloudblogs.microsoft.com/quantum/author/microsoft-research/)
* [What is Quantum Cryptography? (techtarget.com)](https://www.techtarget.com/searchsecurity/definition/quantum-cryptography)