

Project Report
On
QUANTUM COMPUTING IN CRYPTOGRAPHY

Submitted in partial fulfilment of the requirements for the degree of

BACHELOR OF SCIENCE

in

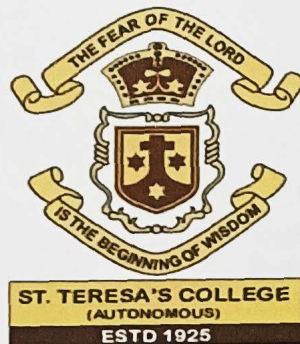
MATHEMATICS

by

SAFNA C S
(AB22BMAT043)

Under the Supervision of

NEENU SUSAN PAUL



DEPARTMENT OF MATHEMATICS AND STATISTICS

ST. TERESA'S COLLEGE (AUTONOMOUS)

ERNAKULAM, KOCHI - 682011

APRIL 2025

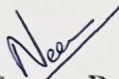


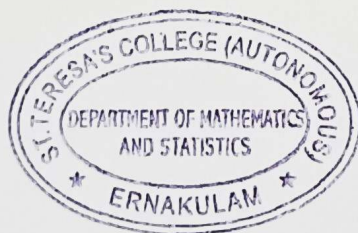
CERTIFICATE

This is to certify that the dissertation entitled, **QUANTUM COMPUTING IN CRYPTOGRAPHY** is a bonafide record of the work done by **SAFNA C S** under my guidance as partial fulfillment of the award of the degree of Bachelor of Science in Mathematics at St. Teresa's College (Autonomous), Ernakulam affiliated to Mahatma Gandhi University, Kottayam. No part of this work has been submitted for any other degree elsewhere.

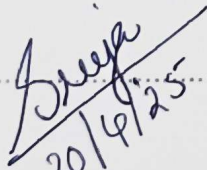
Date: 20/02/2025

Place: Ernakulam


Neenu Susan Paul
Assistant Professor,
Department of Mathematics and Statistics
St. Teresa's College (Autonomous),
Ernakulam.



External
Examiners

1: 
30/4/25

2:


Dr. Elizabeth Reshma M T
Assistant Professor and Head,
Department of Mathematics and Statistics
St. Teresa's College (Autonomous),
Ernakulam.

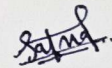
Dr. SREEJA K.U. (PEN:716628)
Assistant Professor
Department of Mathematics
Maharaja's College
Ernakulam - 682 011

DECLARATION

We hereby declare that the work presented in this project is based on the original work done by me under the guidance of Smt. NEENU SUSAN PAUL Assistant Professor, Department of Mathematics and Statistics , St Teresa's College (Autonomous) Ernakulam and has not been included in any other project submitted previously for the award of any degree.

Place : Ernakulam

Date: 20/02/2025



SAFNA C S
(AB22BMAT043)

ACKNOWLEDGEMENT

We take this opportunity to express our sincere gratitude towards Ms. Neenu Susan Paul of the Department of Mathematics and Statistics of St. Teresa's College who encouraged us to carry out this work. Her continuous invaluable knowledgeable guidance throughout this study helped us complete the work upto this stage. We will always be thankful to you in this regard. We also express our thanks to all those who have indirectly guided and helped us in the completion of this project.

Place : Ernakulam

Date: 20/02/2025


SAFNA C S
(AB22BMAT043)

Content

CERTIFICATE.....	ii
DECLARATION.....	iii
ACKNOWLEDGEMENT.....	iv
CONTENTS.....	v
1 Cryptography.....	
1.1 Introduction.....	1
1.2 History and Evolution	3
1.3 Types of Cryptography.....	5
1.3.1 Symmetric Key Cryptography	5
1.3.2 Asymmetric Key Cryptography	5
1.3.3 Hashing.....	6
1.4 Applications of Cryptography	7
1.4.1 ATM.....	7
1.4.2 Email.....	7
1.4.3 Digital Signature	8
1.4.4 HTTPS	8
1.4.5 Cryptocurrencies.....	8
1.4.6 Time Stamping.....	9
2 Quantum Computing	10
2.1 Introduction	10
2.2 Quantum Information Processing.....	11
2.2.1 Entanglement	11
2.2.2 Superposition.....	13
2.2.3 Quantum Parallelism	13
2.3 Applications of Quantum computing.....	14
2.4 Limitations of Quantum computing	15

3. Quantum Algorithms	17
3.1 Introduction.....	17
3.2 Shor's Algorithm	17
3.3 Grover's Algorithm	24
3.4 Quantum Approximation Optimization Algorithm.....	26
3.5 Quantum Fourier Transforms	26
4. Quantum Cryptography	28
4.1 Introduction.....	28
4.2 Quantum cryptography Algorithms	28
4.2.1 BB84.....	28
4.2.2 Ekert 91.....	30
4.3 Applications of Quantum Cryptography	31
4.4 Limitations of Quantum Cryptography	33
4.5 Post Quantum Cryptography	34
REFERENCES.....	36

Chapter 1

CRYPTOGRAPHY

1.1 Introduction

There is no doubt that advancements in technology, particularly in the realm of electronic communications, have revolutionized the way we interact, work, and share information in the modern age. These advancements have not only improved efficiency and connectivity but have also introduced new challenges and risks associated with data security. As the world becomes increasingly reliant on digital systems for communication, commerce, healthcare, governance, and more, ensuring the security of sensitive information has become a critical concern. The pillars of data security confidentiality, integrity, authenticity, and non- repudiation serve as the foundation for protecting data against unauthorized access, tampering, and misuse. Confidentiality ensures that sensitive information is accessible only to authorized individuals, safeguarding privacy and proprietary data. Integrity guarantees that the data remains unaltered and reliable throughout its lifecycle. Authenticity confirms the identities of parties involved in communication, ensuring that data originates from verified sources. Lastly, non- repudiation prevents entities from denying their involvement in a transaction or communication, providing accountability in digital exchanges.

Cryptography plays a vital role in upholding these principles, making it one of the most important disciplines in information technology. The term “cryptography” is derived from the Greek words *kryptos* (hidden) and *graphein* (writing), emphasizing its fundamental purpose concealing and protecting information from unauthorized parties. Cryptography is both an art and a science, involving the creation of algorithms and protocols to secure data in transit or storage, even in the presence of adversaries attempting to compromise it. Historically, cryptography was primarily used for military and diplomatic communication, with methods such as the Caesar cipher and the Enigma machine showcasing early applications of the field. In the modern digital era, cryptography

has evolved significantly, employing complex mathematical principles to create robust encryption systems.

These systems underpin technologies like secure messaging, e-commerce, online banking, digital signatures, and block chain, ensuring the security of billions of transactions daily. Modern cryptographic techniques can be broadly categorized into two types: symmetric-key cryptography and asymmetric-key cryptography. Symmetric-key cryptography involves a single shared key for both encryption and decryption, while asymmetric-key cryptography uses a pair of keys—one public and one private for secure communication. Advanced cryptographic methods, such as hash functions and elliptic curve cryptography, are also critical for addressing diverse security needs in an increasingly interconnected world. As cyber threats grow more sophisticated, the importance of cryptography continues to rise. It not only protects sensitive data from malicious actors but also enables the trust and reliability. Necessary for the continued advancement of digital systems. Cryptography is a cornerstone of cybersecurity and a fundamental enabler of privacy, trust, and innovation in the digital age.

Cryptography is an art of communication between two people by keeping the information not known to others. It is based upon two factors, namely encryption and decryption. Encryption means the process of transformation of information into a secret code, which hides the true meaning. On the other hand, Decryption means the transformation of the coded message original form.

Encryption and decryption require a secret code that is known only to the sender and the receiver. This secret code is called a key. Encrypted text, transformed from plain text using an encryption algorithm, is called cipher text. Cryptography Algorithm is classified mainly into two major types: Symmetric-key cryptography and public-key cryptography. In symmetric key encryption the message is encrypted using a key and the same key is used to decrypt the message, which makes it easy to use but less secure. The Data Encryption Standard (DES) and the Advance Encryption Standard (AES) are examples of Symmetric-key cryptography methods. In public-key cryptography each sender and receiver uses two different keys- public key and private key to encrypt and decrypt data, the public key is freely distributed while private key is kept secret. It is more secure than the symmetric key cryptography. The message which is to be transmitted is encrypted to cipher text at the encryption process and the secret code is obtained.

1.2 History and Evolution of Cryptography

The history of cryptography begins thousands of years ago. The art of cryptography is considered to be born along with the art of writing. From ages human had two inherent needs- to share information and to communicate selectively. These needs set off the rise of art of coding in such a way that only intended people can have the access to the information. Unauthorized people can't extract any information, even if the scrambled message is accessed by them. The first known invented cryptography was found in the 1900 BC in the main chamber of the tomb of the nobleman Khnumhotep II, in Egypt. Hieroglyphs carved into monuments from Egypt's old kingdom (4500+ year ago) is the earliest known use of cryptography found in nonstandard. In most majors early Civilization, evidences of some use of cryptography has been identified. "Risalah fi istikhraj al-mu'amma" is the book wrote by Al-kindī (manuscript for the Deciphering Cryptographic Messages), in 850 CE. He was a pioneer in crypto analysis and cryptology, and devised new methods of breaking cipher, including the frequency analysis method. Until the development of the poly alphabetic cipher, essentially all ciphers remained vulnerable to the cryptanalytic technique of frequency analysis. Leon Battista Alberti has explained, the polyalphabetic cipher, around the year 1467, for which he was called the "father of Western Cryptology". Kautilya has written a state craft named "Arthashastra" which describe the assignment given to spice in secret writing. Edgar Allan Poe used systematic methods to solve cipher in the 1840s. He placed a notice of his abilities in the Philadelphia paper, inviting submissions of cipher, of which he proceeded to solve almost all. It created a public stir for some months. Later he wrote an essay on methods of cryptography which is useful in proved introduction for novice British cryptanalysts codes and German codes and cipher during World War I. Teletype cipher which is introduced by Gilbert Vernam in 1917, kept a paper tape, is combined character with plaintext message to produce the cypher text. This led to the development of electromechanical devices as cipher machines.

Mechanical and electromechanical machines were widely used during World War II, although where such machines were impractical-manual systems continued in use. Nazi Germany widely used the Enigma machine, where as SIGABA was used by British army. The earlier invented method of cryptography is a Roman method popularly known as Ceaser shift method. Around 100 BC, Julius Caesar used a form of encryption, which was later known as Caesar cipher to convey

secret message to army generals in war front. During the beginning of the 19th, Century Hebern developed an electro mechanical contraption which was known as Hebern rotor machine. A single router was used in the encryption in which the secret key is embedded in a rotating disc.

Later the Enigma machine was invented by a German Engineer Arthur Scherbius during the end of World War 1 which used three or more rotators for its functioning. This Enigma machine was heavily used by the German forces during the Second World War. In the early 1970s, due to the high demand for encryption, IBM formed a group called the “Crypto Group,” headed by Horst Feistel. They developed a cipher named Lucifer, which eventually gained worldwide acceptance and was standardized as DES (Data Encryption Standard). Later, in 2000, AES (Advanced Encryption Standard) was developed.

After the European Renaissance, various Italian and papal states led the rapid proliferation of cryptographic techniques. Attack techniques and various analyses were researched in this era to break secret codes. Coding techniques also improved, with the Vigenère cipher emerging in the 15th century. This cipher shifted letters in messages by a variable number of positions, instead of shifting them by the same number of places each time. A technique for encrypting alphabetic text is the Vigenere Cipher. It employs a straightforward method of polyalphabetic substitution. Any substitution-based encryption that employs numerous substitution alphabets is referred to as a polyalphabetic cypher. With the Vigenère square or Vigenère table, the original text is encrypted. The table has the 26 potential Caesar Ciphers written out 26 times in various rows. With each alphabet shifting cyclically to the left in comparison to the previous alphabet. The cipher switches to an alphabet from one of the rows at various stages of the encryption process. Each point's alphabet is determined by a keyword that appears repeatedly. After 19th century, cryptography approaches to encryption to the more sophisticated art and science of information security. At the close of World War I, German engineer Arthur Scherbius created the Enigma machine. There were several distinct Enigma models made, but the German military versions with a plugboard were the most intricate. Models from Italy and Japan were also in use. Enigma gained widespread recognition in the military after being adopted (in a somewhat modified version) by the German Navy in 1926 and the German Army and Air Force shortly after. German military strategy prior to World War I focused on quick, mobile units and blitzkrieg tactics, which rely on radio transmission for command and coordination. Radio signals had to be encrypted securely since enemies would probably try to intercept them. The Enigma machine satisfied that need by being small and

portable. In the period of World War II, cryptography and cryptanalysis became excessively mathematical. Government organizations, military units, and some corporate houses started adopting the applications of Cryptography. They use cryptography to guard their secrets from others. The arrival of computers and the internet has brought effective cryptography within the reach of common people. These innovative breakthroughs and discoveries in cryptography are fostering a promising future for the discipline. The biggest shift that's supposedly coming is quantum computing. The computer capacity at our disposal can be exponentially increased via quantum computing, which uses the characteristics of the superpositioned particles. This implies that the cryptographic operations that are currently too complex to operate on silicon chips could be made. Feasible on a quantum device, potentially rendering current encryption obsolete.

1.3 Types of Cryptography

Cryptography is broadly classified into three :

1.3.1 Symmetric Key Cryptography

The cryptographic method in which same key is used for both encryption and decryption of information is called symmetric key cryptography. Therefore the sender and the receiver will be having access for the key. Since both the parties have access to the secret key, it is considered as a main drawback of the symmetric key encryption compared to the public key encryption. Symmetric key Cryptography is commonly used in today's internet. AES and DES are the common Encryption Algorithm used in symmetric key cryptography. It is faster than asymmetric key cryptography. Symmetric key encryption either uses stream cipher or block cipher. The stream cipher encrypt digits or letters of a message there as block cipher consider bits as a single unit and encrypt them as a whole. Payment applications, generation random number generation or hashing are some of the applications of symmetric key cryptography.

1.3.2 Asymmetric Key Cryptography

Asymmetric key Cryptography is a public key cryptographic scheme which requires two different keys. One key is used for the encryption process and other is use for the decryption of the cipher

text. One of the key in the asymmetric key encryption is a public key which is accessible to the public and the other is kept private which is known as private key. Asymmetric key encryption is also known as public key cryptography. The advantage of asymmetric Cryptography compared to symmetric key cryptography is the non-Reliance on a single point of failure of key. Asymmetric key cryptography increases data security. Since asymmetric key encryption uses a longer key for the encryption process, it results in a slower encryption speed. Digital signature, TLS or SSL handshake, crypto currency are some of the application of asymmetric key cryptography.

1.3.3 Hashing

Hashing is the process of transforming any given key or a string of characters into another value. This is usually represented by a shorter, fixed-length value or key that represents and makes it easier to find or employ the original string. The most popular use of hashing is for setting up hash tables. A hash table stores key and value pairs in a list that's accessible through its index. Because the number of keys and value pairs is unlimited, the hash function maps the keys to the table size. A hash value then becomes the index for a specific element. A hash function generates new values according to a mathematical hashing algorithm, known as a hash value or simply a hash. To prevent the conversion of a hash back into the original key, a good hash always uses a one-way hashing algorithm.

Hashing is relevant to but not limited to data indexing and retrieval, digital signatures, cybersecurity, and cryptography. Hashing is used in data structures to efficiently store and retrieve data. Hashing is a one-way process that turns data into a fixed-length hash value using a hash function. The primary goal of hashing is to ensure data integrity and validate the original data. Hash functions are intended to be fast and efficient, generating unique hash values for each input. Hashing is irreversible, which means it's computationally impractical to recover the original data from the hash value and is often used to store passwords, create digital signatures and verify data integrity.

1.4 Applications of Cryptography

Cryptography has been used in our daily life. Cryptography plays an important role in each time when we make an online purchase, making an online transaction, sending an email withdrawing money from ATM and so on. Cryptography secures all the information that we transmit through the internet. Cryptographic techniques like digital signature protect our information from forgeries and fraud. It ensures authentication of identity, prevents document tampering and establishes the trust between servers. Most of the communication platforms have been encrypted. Social media like WhatsApp, Instagram, Telegram has made use of the idea of encryption for transmitting the messages keeping it secure. Cryptography also helps in encrypting company devices, protecting sensitive data, encrypting databases and securing a website. HTTPS or Secure Hyper Text Transfer Protocol is used for securing websites.

14.1 ATM

Authorized cardholders can withdraw cash and carry out other financial operations at an ATM without having to go to a bank branch because of the convenient and secure service it offers. A secure communications network, is used by banks to authorize each ATM transaction. This network encrypts data so that only the sender and the intended recipient can decipher it.

1.4.2 Email

Email encryption is a method of authentication that stops messages from being read by an unauthorized or unintended person. The original communication is scrambled and put into an unintelligible or unreadable format. When sending sensitive material over email, encryption is required. In order to commit crimes like identity theft and fraud, hackers target victims via email and steal data, including personal information names, addresses, and login credentials. Additionally, while the majority of sent emails are encrypted during transmission, the data is retained in clear text, allowing email providers to access the content. End-to-end encryption is often not offered by well known free email services, making it simple for hackers to intercept delivered messages. Public-key cryptography and digital signature technologies are used by email encryption solutions to encrypt email messages. By following this procedure, you may be sure that

only the intended recipient will be able to open your emails. You can encrypt emails when transmitting important information in them. When is encrypted for email, it is transformed from plain text to scrambled cipher text. Only the receiver has access to the private key and this key will be used to decode the email which enable to view it.

1.4.3 Digital Signature

Just like signature on paper, digital signature has become an important tool in business with the development of technology. Digital signature also has the legal power as hand written signature. Digital signature is a cryptographic value calculated from the data and a secret key known only by the signer. The message belongs to the sender should be assured to the receiver. This is crucial in business as the chance of dispute over the data exchanges are high.

1.4.4 HTTPS

Hyper Text Transfer Protocol Secure or https helps to set the information free on a web. It is an everyday application of cryptography. It is a primary protocol which is used to send data between a browser and a website. It is important to be encrypted as transmit sensitive data such as details of bank account, mail service and so on. A website which require login credential should use https. A browser which does not use https are flagged as non secure.

1.4.5 Cryptocurrencies

Cryptocurrency uses three different cryptographic methods for encryption. Symmetric encryption asymmetric Encryption and hushing has been used in Crypto currencies. The Bitcoin network uses hash functions to ensure the security of the block chain and the immutability of the transactions. Cryptocurrencies use cryptography to make transactions anonymous, secure, and trustless. The identity of the person is not required for the transaction, and details of banks or credit card companies are not collected for the transactions

1.4.6 Time Stamping

Time Stamping is the technique which certify the time when an electronic document or communication was existed or delivered. The encryption model uses a blind signature scheme. The scheme of blind signature helps the sender to receive a message receipted by another person without revealing the information about the message to others. The possible applications of time stamping include patent application, copyright archives and contracts.

Chapter 2

QUANTUM COMPUTING

2.1 Introduction

Quantum computing is a revolutionary technology that has the potential to transform the way we approach complex problems in various fields, including physics, chemistry, Materials science, and machine learning. Quantum computing is a type of computing that uses the principles of quantum mechanics to perform calculations and operations on data. Unlike classical computers, which use bits to represent information, quantum computers use quantum bits or qubits, which can exist in multiple states simultaneously. This property allows quantum computers to process vast amounts of information in parallel, making them potentially much faster than classical computers for certain types of calculations. Quantum computing theory firstly introduced as a concept in 1982 by Richard Feynman, has been researched extensively and is considered the destructor of the present modern asymmetric cryptography. In addition, it is a fact that symmetric cryptography can also be affected by specific quantum algorithms; however, its security can be increased with the use of larger key spaces. Furthermore, algorithms that can break the present asymmetric crypto schemes whose security is based on the difficulty of factorizing large prime numbers and the discrete logarithm problem have been introduced. It appears that even elliptic curve cryptography which is considered presently the most secure and efficient scheme is weak against quantum computers.

Consequently, a need for cryptographic algorithms robust to quantum computations arose.

Data in a quantum computer are stored in qubits, and manipulated by gates. A qubit is a device whose state can be represented by a unit vector in a 2-dimensional complex vector space.

The qubit state can be visualized as a point on the unit circle: The horizontal axis represents the real part of the state and the vertical axis represents the imaginary part of the state.

2.2 Quantum Information Processing

Quantum Information Processing focuses on information processing and computing based on quantum mechanics. While current digital computers encode data in binary digits (bits), quantum computers aren't limited to two states. They encode information as quantum bits, or qubits, which can exist in superposition. Qubits can be implemented with atoms, ions, photons or electrons and suitable control devices that work together to act as computer memory and a processor. Because a quantum computer can contain these multiple states simultaneously, they provide an inherent parallelism. This will enable them to solve certain problems much faster than any classical computer using the best currently known algorithms, like integer factorization or the simulation of quantum many-body systems. Right now the quantum computer is still in its infancy. First steps on that road are the simplest building blocks such as quantum logic gates and memory based on genuine quantum effects such as superposition and entanglement. Qubits provide the foundation for storing, manipulating, and entangling quantum information.

The fundamental features of quantum Information processing (QIP) are different from that classical computing and can be summarized into the following three:

2.2.1 Entanglement

Entanglement is a fundamental concept of quantum mechanics that describes the interconnection of particles at a subatomic level. When two particles are entangled, their properties, such as spin, momentum, and energy, become correlated. A group of particles being generated, interacting, or sharing spatial proximity in such a way that the quantum state of each particle of the group cannot be described independently of the state of the others, including when the particles are separated by a large distance. The topic of quantum entanglement is at the heart of the disparity between classical physics and quantum physics: entanglement is a primary feature of quantum mechanics not present in classical mechanics. Just as energy is a resource that facilitates mechanical operations, entanglement is a resource that facilitates performing tasks that involve communication and computation. The use of entanglement in communication and computation is an active area of research and development. An example of entanglement is a subatomic particle that decays into an entangled pair of other particles.

Entanglement Properties

1. Correlation: Entangled particles are correlated, meaning their properties are connected.
2. Non-Locality: Entangled particles can be separated by large distances, yet still be correlated.

Entanglement Generation

1. Quantum Gates: Entanglement can be generated using quantum gates, such as the CNOT gate.
2. Quantum Measurement: Entanglement can be generated through quantum measurement, such as projective measurement.
3. Spontaneous Parametric Down-Conversion (SPDC): Entanglement can be generated through SPDC, a process that creates entangled photon pairs.

Entanglement-Based Quantum Cryptographic Protocols

1. BB84 Protocol: Uses entangled photons to create secure keys.
2. Ekert Protocol: Employs entangled particles to detect eavesdropping.
3. Quantum Secure Direct Communication (QSDC): Enables secure communication using entangled particles.

The mathematical representation of quantum entanglement is represented by the density matrix, which describes the state of a composite quantum system.

A simple example of quantum entanglement is the polarization of two photons, where the polarization of one photon is entangled with the polarization of the other photon, meaning that measuring the polarization of one photon will instantaneously determine the polarization of the other photon, regardless of the distance between them.

2.2.2 Quantum Superposition

Superposition is a fundamental principle of quantum computing that allows qubits to represent multiple states at once, which gives quantum computers their ability to process information in parallel. Quantum computers can process many inputs simultaneously because of the superposition of qubits. This allows them to represent complex problems in ways and perform operations that classical computers can't. Qubits can represent a combination of 0 and 1 with different probabilities. Researchers use precision lasers or microwave beams to manipulate qubits into superposition. The final result of a calculation emerges when the qubits are measured, which causes their quantum state to “collapse” to either 1 or 0. Groups of qubits in superposition can create complex, multidimensional computational spaces. Complex problems can be represented in new ways in these spaces. This superposition of qubits gives quantum computers their inherent parallelism, allowing them to process many inputs simultaneously. Controlling the superposition of qubits is a central challenge in quantum computation.

The mathematical representation of quantum superposition is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers and $|0\rangle$ and $|1\rangle$ are the states of a quantum bit (qubit).

Example of quantum superposition is the spin of an electron, which can be in a state of “spin up” and “spin down” simultaneously. Another example is the famous Schrödinger’s cat thought experiment, where a cat in a sealed box can be in a state of being both alive and dead simultaneously until observed.

This Superposition property is utilized by the quantum algorithms such as Shor’s and Grover’s etc.

2.2.3 Quantum Parallelism

Quantum parallelism is the heuristic that quantum computers can be thought of as evaluating a function for multiple input values simultaneously. This can be achieved by preparing a quantum system in a superposition of input states and applying a unitary transformation that encodes the function to be evaluated. The resulting state encodes the function’s output values for all input values in the superposition, allowing for the computation of multiple outputs simultaneously. This property is key to the speedup of many quantum algorithms. However, “parallelism” in this sense is insufficient to speed up a computation, because the measurement at the end of the computation gives only one value. To be useful, a quantum algorithm must also incorporate some.

In quantum computing, the entanglement of each additional qubit exponentially grows the state space. The application of even one single-qubit operation on any of those entangled qubits can affect the entire state space in a kind of massive quantum parallelism. Quantum computers are remarkably inefficient at solving simple problems. However, they can be remarkably efficient at solving classically intractable problems that cannot be solved efficiently with classical computers. Quantum parallelism leverages these mathematical concepts to enable the simultaneous evaluation of multiple possibilities, leading to exponential speedup over classical computation for certain problems.

2.3 Applications of Quantum Computing

Quantum computers are not yet practical for real work. Physically engineering high-quality qubits has proven challenging. If a physical qubit is not sufficiently isolated from its environment, it suffers from quantum decoherence, introducing noise into calculations. National governments have invested heavily in experimental research that aims to develop scalable qubits with longer coherence times and lower error rates. Example implementations include superconductors (which isolate an electrical current by eliminating electrical resistance) and ion traps (which confine a single atomic particle using electromagnetic fields). In principle, a classical computer can solve the same computational problems as a quantum computer, given enough time. Quantum advantage comes in the form of time complexity rather than computability, and quantum complexity theory shows that some quantum algorithms are exponentially more efficient than the best-known classical algorithms. A large-scale quantum computer could in theory solve computational problems unsolvable by a classical computer in any reasonable amount of time. This concept of extra ability has been called “quantum supremacy”. While such claims have drawn significant attention to the discipline, near-term practical use cases remain limited. Quantum computing has significant applications across various fields due to its ability to solve complex problems more efficiently than classical computers. Key areas include:

1. Artificial Intelligence (AI): Enhancing machine learning and optimization tasks by enabling faster data processing and model training.

2. **Data Science and Analysis:** Quantum algorithms can manage and process vast amounts of structured and unstructured data for insights and decision-making.
3. **Drug Discovery and Medical Research:** Revolutionizing pharmaceutical development through rapid simulations of molecular interactions and improved precision in drug design.
4. **Materials Science:** Predicting properties and behavior of new materials at the atomic level, aiding innovations in nanotechnology and advanced materials.
5. **Climate Modeling and Weather Forecasting:** Enhancing simulation accuracy by handling complex climate systems and their interactions.
6. **Finance:** Performing high-speed portfolio optimization, fraud detection, and risk assessment.
7. **Cryptography:** Strengthening encryption methods and breaking existing cryptographic systems for secure communication.

These applications demonstrate the transformative potential of quantum computing in solving real world challenges.

2.4 Limitations of Quantum Computing

Quantum computing has several limitations, including:

- 1) **Error correction:** Quantum computers are more likely to have computational faults than classical computers, and it's difficult to correct these errors.
- 2) **Scalability:** Quantum computers are still relatively small compared to classical computers.
- 3) **Hardware development:** It's challenging to develop high-quality quantum hardware, such as qubits and control electronics.

- 4) Software development: There's a need for new programming languages, compilers, and optimization tools
- 5) Environmental sensitivity: Quantum computers need to be kept at or around absolute zero, under no atmospheric pressure, and insulated from the earth's magnetic field.
- 6) Lack of standards: There are currently no standards for quantum programming languages and software tools.
- 7) Trained talent: There aren't many people who are properly educated and trained to work in quantum computing.
- 8) Overall expense: Quantum computers are expensive.

Chapter 3

QUANTUM ALGORITHMS

3.1 Introduction

Quantum computing has the potential to revolutionize the way we approach complex computational problems. At the heart of this revolution are quantum algorithms, a set of instructions that harness the unique properties of quantum mechanics to solve problems that are intractable or inefficiently solved by classical computers.

Quantum algorithms are designed to exploit the principles of superposition, entanglement, and interference, allowing them to explore an exponentially large solution space simultaneously. This property, known as quantum parallelism, enables quantum algorithms to solve certain problems exponentially faster than their classical counterparts. From Shor's algorithm for factorizing large numbers to Grover's algorithm for searching unsorted databases, quantum algorithms have the potential to transform fields such as cryptography, optimization, and machine learning. This discussion will delve into the world of quantum algorithms, exploring their underlying principles, applications, and implications for the future of computing.

3.2 Shor's Algorithm

Shor's Algorithm, named after mathematician Peter Shor, is a quantum algorithm designed to efficiently factorize large composite numbers. It's one of the most famous and impactful algorithms in quantum computing, as it provides an exponential speedup over the best-known classical algorithms for factoring. The ability to factor large numbers has significant implications for

Department of Mathematics and Statistics , St Teresa's College (Autonomous), Ernakulam

cryptography, particularly RSA encryption. Shor's Algorithm can factor a composite number in polynomial time, specifically, compared to the exponential time required by classical algorithms.

This efficiency has made Shor's Algorithm a symbol of the potential power of quantum computing and has spurred interest in post-quantum cryptography, which seeks cryptographic methods resistant to quantum attacks. It's a foundational result that has shaped the field of quantum computing and also inspired further research into quantum algorithms, complexity theory, and the development of quantum-resistant cryptographic protocols.

This showcasing the potential of quantum algorithms to solve problems previously considered intractable. Its discovery has had a profound impact on both the theoretical and practical aspects of quantum computing and cryptography. Shor's factoring algorithm finds one of two unknown variables that are crucial for efficiently factoring an integer. With two unknowns in one equation, finding both values quickly becomes classically intractable as the target integer gets larger. There are classical algorithms to find one of those values, but they become increasingly inefficient as the target integer gets larger. With Shor's quantum algorithm finding that value efficiently, it then becomes considerably easier to find the other value. The core of Shor's Algorithm is the Quantum Fourier Transform (QFT), a quantum analog of the classical Fourier Transform. The QFT allows the algorithm to find the period of a specific mathematical function related to the number being factored. Once the period is found, the prime factors can be efficiently extracted using classical methods. The problem of factoring a large composite number into its prime factors is classically hard, meaning that the time required to solve it grows rapidly with the size of the input. RSA encryption, widely used in secure data transmission, relies on the difficulty of factoring large numbers. Shor's Algorithm, by efficiently solving this problem, poses a potential threat to RSA and similar encryption schemes. Shor's algorithm complexity is exponentially more efficient than known classical algorithms. Shor's factoring algorithm also highlights the computational power of quantum phase estimation (QPE) and QFT, which have applications beyond integer factorization. One of the most talked about potential applications of quantum computing, for example, is quantum chemistry. QPE can compute the ground state energies of molecules with the same exponential efficiency advantage as it bestows upon integer factorization. While Shor's Algorithm is theoretically efficient, its practical implementation on current quantum computers is challenging. It requires a significant number of qubits and error corrected operations. Efforts to implement

Shor's Algorithm have led to valuable insights into quantum error correction, algorithm optimization, and hardware development.

Not all numbers can be factorized by Shor's Algorithm.

The number should :

- Not be a prime number
- Not be an even number
- Not be of form n^x (n^x)

This is a Step-By-Step explanation of the whole process with an example Step

1

Let the number to be factorized be N . Make sure it fulfills all conditions.

Eg - Let's factorize 15. So $N=15$.

Step 2

Choose randomly a number between 1 and N . Call this number ' k '.

Eg- We have to choose a number between 1 and 15. Let's take 7. So, $k=7$.

Step 3

Find GCD (N, k). You could calculate it using Euclid's Division Algorithm. If GCD is not equal to one, then congratulations! The GCD is a factor of N , so we are done.

If, however, $\text{GCD} = 1$, then proceed to Step 4.

Eg- $\text{GCD}(15, 7) = 1$

Step 4

We need to find smallest positive integer r such that if

$$F(x) = k^x \bmod N, \text{ then } f(a) = f(a+r)$$

The following steps to find r :

Step 4.1

Define a new variable $q = 1$.

Step 4.2

Find $(q \times k) \bmod N$.

If the remainder is 1, proceed to Step 4.3. If not, set the value of ' q ' to the value of the remainder we got. Repeat this step till you get remainder = 1 and keep track of how many times you did the transformation. Remember to change the value of ' q ' every time. Eg-

$1 \times 7 \bmod 15 = 7$	...1
$\downarrow$	
$7 \times 7 \bmod 15 = 4$	...2
$\downarrow$	
$4 \times 7 \bmod 15 = 13$	...3
$\downarrow$	
$13 \times 7 \bmod 15 = 1$	...4

We did the transformation 4 times.

Step 4.3

The number of transformations you did in Step 4.2 is the value of r .

Eg- We did Step 4.2 four times. So, $r = 4$

Step 5

If r is odd, go back to Step 2 and choose a different value of k .

Eg- $r = 4$ is even, so we move on.

Step 6

Define $p = \text{remainder in } (r/2)\text{th transformation.}$

If $p + 1 = N$, then go back to Step 2 and choose a different value of k .

If not, proceed to Step 7.

Eg- P will be the remainder in $(4/2)\text{th}$, i.e., 2^{nd} transformation.

$P = 4$

$4 + 1 = 5$ is not equal to 15. So we can proceed.

Step 7

This is the final step. The factors of N are

$$F_1 = \text{GCD}(p+1, N)$$

$$F_2 = \text{GCD}(p-1, N)$$

$$\text{Eg- } F_1 = \text{GCD}(p+1, N) = \text{GCD}(5, 15) = 5 \quad F_2 =$$

$$\text{GCD}(p-1, N) = \text{GCD}(3, 15) = 3 \quad \text{Therefore, } 3$$

and 5 are factors of 15.

Another Example (chosen such that it covers all possible situations) :

Let's factorize $N = 357$

We randomly pick $k = 205$

$$\text{GCD}(357, 205) = 1$$

We did the transformation 3 times.

$$\begin{array}{ll}
 1 \times 205 \bmod 357 = 205 & \dots 1 \\
 \downarrow & \\
 205 \times 205 \bmod 357 = 256 & \dots 2 \\
 \downarrow & \\
 256 \times 205 \bmod 357 = 1 & \dots 3
 \end{array}$$

Therefore, $r = 3$

R is odd. So, we need to choose another value of k .

We randomly pick $k = 152$

$$\text{GCD}(357, 152) = 1$$

$$\begin{array}{ll}
 1 \times 152 \bmod 357 = 152 & \dots 1 \\
 \downarrow & \\
 152 \times 152 \bmod 357 = 256 & \dots 2 \\
 \downarrow & \\
 256 \times 152 \bmod 357 = 356 & \dots 3 \\
 \downarrow & \\
 356 \times 152 \bmod 357 = 205 & \dots 4 \\
 \downarrow & \\
 205 \times 152 \bmod 357 = 101 & \dots 5 \\
 \downarrow & \\
 101 \times 152 \bmod 357 = 1 & \dots 6
 \end{array}$$

Therefore, $r = 6$.

R is even. So, we can move on.

P will be the remainder in $(6/2)$ th, i.e., 3^{rd} transformation.

$$P = 356$$

Now we check if $p + 1 = N$

$$356 + 1 \text{ is equal to } 357$$

So, we need to choose another value of k .

We randomly pick $k = 52$

$$\text{GCD}(357, 52) = 1$$

$1 \times 52 \bmod 357 = 52$	...1
$\downarrow$	
$52 \times 52 \bmod 357 = 205$	...2
$\downarrow$	
$205 \times 52 \bmod 357 = 307$	...3
$\downarrow$	
$307 \times 52 \bmod 357 = 256$	...4
$\downarrow$	
$256 \times 52 \bmod 357 = 103$	...5
$\downarrow$	
$103 \times 52 \bmod 357 = 1$	...6

We did the transformation 6 times.

Therefore, $r = 6$

R is even. So, we can move on.

P will be the remainder in $(6/2)$ th, i.e., 3rd transformation.

$$P = 307$$

Now we check if $p + 1 = N$.

$307 + 1$ is not equal to 357.

So, now we can do the final step.

$$F_1 = \text{GCD}(308, 357) = 7$$

$$F_2 = \text{GCD}(306, 357) = 51$$

Therefore, 7 and 51 are factors of 357.

3.3 Grover's Algorithm

In quantum computing, Grover's algorithm, also known as the quantum search algorithm, is a quantum algorithm for unstructured search that finds with high probability the unique input to a black box function that produces a particular output value, using just $O(\sqrt{N})$ evaluations of the function, where N is the size of the function's domain. It was devised by Lov Grover in 1996, the analogous problem in classical computation cannot be solved in fewer than $O(N)$ evaluations (because, on average, one has to check half of the domain to get a 50% chance of finding the right input). Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani proved that any quantum solution to the problem needs to evaluate the function $\Omega(\sqrt{N})$ times, so Grover's algorithm is asymptotically optimal. Since classical algorithms for NP-complete problems require exponentially many steps, and Grover's algorithm provides at most a quadratic speedup over the classical solution for unstructured search, this suggests that Grover's algorithm by itself will not provide polynomial time solutions for NP-complete problems (as the square root of an exponential function is still an exponential, not a polynomial, function).

Unlike other quantum algorithms, which may provide exponential speedup over their classical counterparts, Grover's algorithm provides only a quadratic speedup. However, even quadratic speedup is considerable when N is large, and Grover's algorithm can be applied to speed up broad classes of algorithms. Grover's algorithm could brute-force a 128-bit symmetric cryptographic key in roughly 2^{64} iterations, or a 256-bit key in roughly 2^{128} iterations. It may not be the case that Grover's algorithm poses a significantly increased risk to encryption over existing classical algorithms, however.

Here's a step-by-step explanation of Grover's algorithm:

Step 1: Initial state

Step 2: Oracle Application Step

3: Diffusion operator

Step 4: Grover iteration

Step 5: Optimal iteration

Step 6: Measurement

The quantum system starts in a superposition of all possible states.

This is achieved using Hadamard gates, which ensure every state has an equal probability of being the solution.

1. The initial state is:

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$$

where N is the total number of possible states.

2. Oracle Function

The oracle marks the target state (the one you're searching for) by applying a phase shift of -1 to it. Think of it as a “black box” that tags the correct answer without revealing how it works.

3. Diffusion Operator

The diffusion operator increases the likelihood of the target state by amplifying its probability: It reflects all states' amplitudes about their average. This makes the marked state's probability larger while reducing others.

4. Iterative Amplification

The algorithm alternates between:

- Oracle application: Marks the target state.
- Diffusion operator: Amplifies the marked state's probability.

This process is repeated approximately $\pi/4\sqrt{N}$ times, where N is the total number of states. This ensures the target state's probability is maximized.

5. Measurement

After the iterations, the state is measured. The superposition collapses, and the marked state is returned with high probability.

Grover's algorithm finds a target item in $\sqrt{N}$ steps instead of N steps (classical search).

Example: Searching a 1,000-item database takes 32 steps instead of 1,000!

3.4 Quantum Approximation Optimization Algorithm

A quantum algorithm that produces approximate solutions for combinatorial optimization problems. The algorithm depends on a positive integer p and the quality of the approximation improves as p is increased. The quantum circuit that implements the algorithm consists of unitary gates whose locality is at most the locality of the objective function whose optimum is sought. The depth of the circuit grows linearly with p times (at worst) the number of constraints. If p is fixed, that is, independent of the input size, the algorithm makes use of efficient classical preprocessing. If p grows with the input size a different strategy is proposed. We study the algorithm as applied to MaxCut on regular graphs and analyze its performance on 2-regular and 3-regular graphs for fixed p . For $p=1$, on 3-regular graphs the quantum algorithm always finds a cut that is at least 0.6924 times the size of the optimal cut.

3.5 Quantum Fourier Transforms (QFT)

In quantum computing, the quantum Fourier transform (QFT) is a linear transformation on quantum bits, and is the quantum analogue of the discrete Fourier transform. The quantum Fourier transform is a part of many quantum algorithms, notably Shor's algorithm for factoring and computing the discrete logarithm, the quantum phase estimation algorithm for estimating the eigenvalues of a unitary operator, and algorithms for the hidden subgroup problem. The quantum Fourier transform was discovered by Don Coppersmith. With small modifications to the QFT, it can also be used for performing fast integer arithmetic operations such as addition and

Department of Mathematics and Statistics , St Teresa's College (Autonomous), Ernakulam

multiplication. The quantum Fourier transform can be performed efficiently on a quantum computer with a decomposition into the product of simpler unitary matrices. The discrete Fourier transform on 2^n amplitudes can be implemented as a quantum circuit consisting of only $O(n^2)$ Hadamard gates and controlled phase shift gates, where n is the number of qubits. This can be compared with the classical discrete Fourier transform, which takes $O(n^2 \cdot n)$ gates (where n is the number of bits), which is exponentially more than $O(n^2)$.

The quantum Fourier transform acts on a quantum state vector (a quantum register), and the classical Discrete Fourier transform acts on a vector. Both types of vectors can be written as lists of complex numbers. In the classical case, the vector can be represented with e.g. an array of floating point numbers, and in the quantum case it is a sequence of probability amplitudes for all the possible outcomes upon measurement (the outcomes are the basis states, or eigenstates). Because measurement collapses the quantum state to a single basis state, not every task that uses the classical Fourier transform can take advantage of the quantum Fourier transform's exponential speedup. The best quantum Fourier transform algorithms known (as of late 2000) require only $O(n \log n)$ gates to achieve an efficient approximation, provided that a controlled phase gate is implemented as a native operation.

Chapter 4

QUANTUM CRYPTOGRAPHY

4.1 Introduction

In the realm of cryptography, the pursuit of unbreakable codes has been an ongoing quest. With the advent of quantum mechanics, a new paradigm for secure communication has emerged: quantum cryptography. This revolutionary technology harnesses the fundamental principles of quantum mechanics to create secure encryption keys, ensuring confidentiality and integrity in data transmission. Quantum cryptography, also known as quantum key distribution (QKD), enables two parties to share a secure encryption key, without physically meeting or relying on a trusted third party. By exploiting the unique properties of quantum mechanics, such as entanglement and superposition, QKD systems can detect any attempt to eavesdrop or tamper with the communication channel.

4.2 Quantum Cryptography Algorithms

4.2.1 BB84 – Protocol

The BB84 protocol, developed by Charles Bennett and Gilles Brassard in 1984, is the first quantum key distribution (QKD) scheme. It securely shares a private key using the quantum properties of photons. Alice sends photons through a fiber optic cable, with each photon representing a bit (0 or 1) based on its polarization. She chooses random bases (rectilinear or diagonal) to encode each bit. Bob Measures the photons using randomly chosen bases. If his basis matches Alice's, he correctly detects the bit; otherwise, the result is random. Bob tells Alice which bases he used for each measurement. Alice tells Bob which bases matched hers. They keep the bits with matching bases

and discard the rest, forming the shared key. To detect an eavesdropper (Eve), Alice and Bob publicly compare a few random bits from the key. If any bits don't match, it indicates Eve's interference since measuring photons disturbs their state. If interference is detected, they discard the key and try again. The no-cloning theorem ensures Eve cannot copy photons without introducing detectable errors, making BB84 secure as long as errors in the quantum channel are low.

1. State Preparation (Alice sends photons)

Alice sends photons in one of four possible polarization states:

$|0\rangle$ (0°), $|1\rangle$ (90°), $|+\rangle$ (45°), or $|-\rangle$ (-45°).

These correspond to the rectilinear basis ($|0\rangle, |1\rangle$) and diagonal basis ($|+\rangle, |-\rangle$).

2. Encoding (Mapping bits to photons)

Alice encodes her classical bit sequence into photons:

Bit 0 $\rightarrow |0\rangle$ or $|+\rangle$ (depending on the chosen basis).

Bit 1 $\rightarrow |1\rangle$ or $|-\rangle$.

3. Measurement (Bob measures photons)

Bob receives the photons and measures them using one of two random bases:

Rectilinear basis: $\{|0\rangle, |1\rangle\}$.

Diagonal basis: $\{|+\rangle, |-\rangle\}$.

If Bob uses the same basis as Alice, he measures the correct bit.

If Bob uses the wrong basis, his result is random.

4. Classical Post-Processing

Alice and Bob publicly compare which bases they used for each photon (but not the actual bit values). They discard measurements where Bob used the wrong basis.

5. Key Extraction

The remaining measurements (where bases match) form the shared secret key.

Example: If Alice and Bob's bases match for a photon, they keep the corresponding bit for the key.

Random Bases: The use of random bases ensures eavesdroppers cannot extract meaningful information without being detected.

Quantum Properties:

- The no-cloning theorem states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state,
- Heisenberg uncertainty principle states that it is impossible to know the exact position and velocity of a particle at the same time.

ensure that measurements disturb the photons, revealing any eavesdropping attempts.

The BB84 protocol enables Alice and Bob to securely generate a shared secret key using photons, quantum properties, and public communication.

4.2.2 Ekert 91 – Protocol

The Ekert Protocol, proposed by Arthur Ekert in 1991, uses quantum entanglement and Bell's theorem to securely distribute cryptographic keys.

A central source (e.g., a satellite) produces pairs of entangled particles and sends one to Alice and one to Bob. These particles are in a spin-singlet state:

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)$$

The spins are anticorrelated, if Alice measures spin-up, Bob will measure spin-down, and vice versa. Both Alice and Bob randomly choose one of three measurement bases (angles).

Alice : 0° , 45° , 90°

Bob : 45° , 90° , 135°

If they choose the same or compatible bases, their results will be perfectly correlated or anticorrelated. If an eavesdropper (Eve) intercepts the particles she must measure the particles, collapsing their quantum states. Eve's measurement disturbs the system and introduces errors in Alice and Bob's results. After measurements, Alice and Bob compare their bases publicly and discard results from incompatible bases. If errors exceed a threshold, Eve's presence is detected. From the results of compatible bases, Alice and Bob generate a sifted key, where spin-up = 1 and spin-down = 0.

In a glimpse a central source sends entangled particles to Alice and Bob. Both measure the particles in random bases. Alice and Bob publicly compare bases to sift out compatible measurements. Any errors in the correlated results reveal Eve's interference. The sifted results are converted into a shared cryptographic key. This protocol ensures secure key distribution by leveraging the principles of quantum entanglement and the no-cloning theorem, making eavesdropping detectable.

4.3 Applications of Quantum Cryptography

1. Secure Communication- Quantum Key Distribution (QKD) enables secure sharing of encryption keys by detecting eavesdropping. For example, protocols like BB84 ensure key security through quantum mechanics. Used in defense, government, and banking sectors to protect communications.

2. Secure Cloud Computing – Protects data stored in cloud systems using quantum encryption, ensuring security against future quantum computing threats.
3. Internet of Things (IoT) Security Ensures secure communication between IoT devices, which are often vulnerable to cyberattacks.
4. Banking and Financial Transactions Prevents fraud and data breaches in digital transactions by securing payment gateways and financial networks,
5. Military and Defense Applications Protects sensitive military communications. Ensuring encrypted messaging and secure data exchange.
6. Secure Voting Systems – Ensures integrity and anonymity in electronic voting systems by preventing tampering and data breaches.
7. Healthcare Data Security -Protects sensitive patient information and ensures privacy in telemedicine and digital health records.
8. Intellectual Property Protection-Secures sensitive information, such as trade secrets, patents, and R&D data, against industrial espionage.
9. Satellite Communication Used in secure communication networks for satellites (e.g., China's quantum satellite Micius), enabling ultra-long-distance secure communication.
10. Future-proof Security Provides solutions resistant to attacks from quantum computers, which could render traditional encryption obsolete.

These applications are rapidly evolving, with more industries exploring quantum cryptograph to address emerging cybersecurity challenges.

4.4 Limitations of Quantum Cryptography

Quantum cryptography offers strong security based on the principles of quantum mechanics, but it also comes with several limitations:

1) Technological Challenges –

Infrastructure: Quantum cryptography often requires specialized hardware, like quantum key distribution (QKD) systems, which are expensive and complex to implement and maintain.

Distance Limitations: For technologies like QKD, the transmission of quantum information over long distances is difficult. Quantum signals are prone to attenuation and noise, making it hard to maintain the integrity of the signal over large distances, though advancements like quantum repeaters may address this in the future.

2) Scalability: Quantum cryptographic systems are still in their early stages, and scaling up these systems to cover large networks or operate over the internet requires substantial advancements in both quantum technologies and classical network infrastructures.

3) Vulnerability to Practical Implementation: While quantum cryptography itself offers theoretically unbreakable encryption, real-world implementations are still susceptible to issues like side-channel attacks, where information can be leaked through imperfections in the physical implementation of the quantum system.

4) Key Management: In quantum key distribution, the secure exchange of cryptographic keys is key, but managing and securely storing these keys across distributed systems becomes a challenge, especially as the number of users increases.

5) Quantum Resource Requirements: The processing power required to implement quantum cryptography is significant. This includes both the need for specialized quantum computers or devices and the infrastructure to handle the quantum states.

- 6) **Compatibility with Existing Systems:** Quantum cryptography is not directly compatible with current cryptographic protocols, meaning existing systems would need to be upgraded or replaced. This transition period could be costly and time-consuming.
- 7) **Quantum Computing Threat:** While quantum cryptography is designed to protect against the threats posed by quantum computers, quantum computing itself is still in development. When large-scale quantum computers become available, they could potentially break classical encryption methods, but they are not yet advanced enough to impact most quantum cryptographic protocols.

These limitations indicate that quantum cryptography is promising but faces hurdles before it can be widely adopted.

4.5 Post Quantum Cryptography

Post-quantum cryptography (PQC), sometimes referred to as quantum-proof, quantum-safe, or quantum-resistant, is the development of cryptographic algorithms (usually public-key algorithms) that are currently thought to be secure against a cryptanalytic attack by a quantum computer. The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks. Most widely-used public-key algorithms rely on the difficulty of one of three mathematical problems: the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem. All of these problems could be easily solved on a sufficiently powerful quantum computer running Shor's algorithm or even faster and less demanding (in terms of the number of qubits required) alternatives. The rumoured existence of widespread harvest now, decrypt later programs has also been seen as a motivation for the early introduction of post-quantum algorithms, as data recorded now may still remain sensitive many years into the future.

In contrast to the threat quantum computing poses to current public-key algorithms, most current symmetric cryptographic algorithms and hash functions are considered to be relatively secure

against attacks by quantum computers. While the quantum Grover's algorithm does speed up attacks against symmetric ciphers, doubling the key size can effectively block these attacks. Thus post-quantum symmetric cryptography does not need to differ significantly from current symmetric cryptography. The U.S. National Institute of Standards and Technology (NIST) released final versions of its Post Quantum Crypto Standards. They are

- Lattice based
- Hash based
- Multivariate
- Code based
- Super singular isogeny based

REFERENCES

1. Peter W. Shor, SIAM Journal on Computing, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”. 1997
2. Daniel J. Bernstein, Post-Quantum Cryptography, “Introduction to post- quantum cryptography”, 2009
3. Anna Kramer, Scientific American, “Surprising and super cool. Quantum algorithm offers faster way to hack internet encryption”, 2023
4. Lov K Grover, Proceedings. 28th Annual ACM Symposium on the Theory of Computing, “A fast quantum mechanical algorithm for database search”, 1996
5. Lov K Grover, American Journal of Physics, “From Schrödinger’s equation to quantum search algorithm”, 2001
6. Lov K Grover, The Sciences, “QUANTUM COMPUTING: How the weird logic of the subatomic world could make it possible for machines to calculate millions of times faster than they do today”. 1999
7. Michael Nielsen, Isaac L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000
8. Lov K Grover, Lucent Technologies, “What’s a Quantum Phone Book?”
9. Valerio Scarani, Hele. Bechmann-Pasquinucci, Nicolas J. Cerf, Miroslav Dušek, Norbert Lütkenhaus, Momtchil Peev, Reviews of Modern Physics, “The security of practical quantum key distribution”, 2009
10. William Stallings, Cryptography and network security principles and practice. 6th edition
11. Simon Rips and Michael J. Hartmann, Quantum Information Processing with Nano mechanical Qubits, November 5, 2018