UNIT 3

Quantum Computing

CONTENTS COVERED

- Quantum Error Correction and Cryptography:
  - Types of quantum errors and noise
- Quantum Error-Correcting Codes:
  - Shor and Steane error-correcting codes
- Security advantages of quantum cryptography
- Quantum key distribution
- BB84 protocol.

WHAT IS QUANTUM ERROR?

- There is currently no preferred qubit technology; a variety of physical systems are being explored for use as qubits, including **photons , trapped ions , superconducting circuits and spins in semiconductors**
- It is difficult to sufficiently isolate the qubits from the effects of external noise, meaning errors during quantum computation are inevitable.
- In contrast, bits in a classical computer are typically realized as the robust on/off states of transistor switches. This provides classical CPUs with high error margins that near-eradicate failures at the physical level.
- For quantum computers, where qubits are realized as fragile quantum systems, there is no such security against errors. As such, any circuit-model quantum computer based on current and future qubit technologies will require some form of active error correction.

TYPE OF QUANTUM NOISE

Types of Quantum Noise

Amplitude Damping

Energy loss to environment

Effect: `|1⟩ → |0⟩ decay`

Example: Spontaneous emission

`$T_1$ (relaxation time)`

Phase Damping

Loss of phase coherence

Effect: `Superposition → Mixed state`

Example: Dephasing noise

`$T_2$ (coherence time)`

Bit Flip

Computational basis flip

Effect: `|0⟩ ↔ |1⟩`

Example: Cosmic rays, thermal fluctuations

`px (bit flip probability)`

Phase Flip

Relative phase change

Effect: `|+⟩ ↔ |-⟩`

Example: Magnetic field fluctuations

`pz (phase flip probability)`

Depolarizing

Random Pauli errors

Effect: `Pure → Maximally mixed`

Example: White noise

`p (depolarizing probability)`

Measurement Error

Incorrect readout

Effect: `Wrong measurement outcome`

Example: Detector imperfections

`pm (measurement error rate)`

QUANTUM ERROR CORRECTION

- Quantum error correction (QEC) is a technique that allows us to protect quantum information from errors.
- Error correction is especially important in quantum computers, because efficient quantum algorithms make use of large-scale quantum computers, which are sensitive to noise.
- The basic principle behind quantum error correction is that the number of bits used to encode a given amount of information is increased.
- This redundancy allows the code to detect and correct errors.
- The error rates for quantum computers are typically higher than classical computer's errors due to the challenges associated with building and operating quantum systems.
- Noise, decoherence, and imperfections in quantum gates can cause errors in quantum computations.
- Current quantum computers have error rates in the range of 1% to 0.1%.
- In other words, this means that on average one out of every 100 to 1000 quantum gate operations results in an error.

TYPES OF QUANTUM ERRORS AND NOISE

- There are two fundamental types of quantum errors:
  - Bit flips
  - Phase flips.
- Bit flip errors occur when a qubit changes from |0> to |1> to or vice versa.
- Bit flip errors are also known as - σ_x errors, because they map the qubit states $\sigma_x|0\rangle = |1\rangle$ and $\sigma_x|1\rangle = |0\rangle$

PHASE FLIP ERROR

- Phase flip errors occur when a qubit changes its phase. They are also known as σ_z errors, because they map the qubit states $\sigma_z|0\rangle = |0\rangle$ and $\sigma_z|1\rangle = -|1\rangle$
- This type of error has no classical analog.

- In quantum computing, quantum errors can manifest as bit flips, phase flips, or a combination of both.
- https://mgx.dev/app/0250a43e40f14e879c00756a7ebf7ff5

QUANTUM ERROR-CORRECTING CODES

- **Repetition code:** The simplest quantum error correction code, where a single qubit is encoded into multiple qubits by repeating it multiple times. The repetition code can correct bit flip errors, but not phase flip errors.
- **Shor code:** The first quantum error correction code, developed by Peter Shor. It encodes one logical qubit into nine physical qubits. Shor code can correct one-bit flip error or one phase flip error, but it can't correct both types of errors at the same time.
- **Steane code:** This is a seven-qubit code that can correct both bit flip and phase flip errors. It has the advantage of being fault-tolerant, meaning that the error correction process itself doesn't introduce extra errors.
- **Surface code:** This is a topological error correction code that uses a two-dimensional lattice of qubits to encode logical qubits. It has a high error correction threshold and is considered one of the most promising techniques for large-scale, fault-tolerant quantum computing.
- **Hastings-Haah code:** This quantum error correction code offers better space-time costs than surface codes on Majorana qubits in many regimes. For gate-based instruction sets, the overhead is larger, which makes this approach less efficient than the surface code.

SHOR AND STEANE ERROR-CORRECTING CODES

- The Shor code was the first quantum error-correcting code, demonstrating that quantum information could be protected against errors. It uses a concatenated approach, first protecting against bit-flip errors and then against phase-flip errors, requiring 9 physical qubits to encode 1 logical qubit.

- The Steane code is a CSS (Calderbank-Shor-Steane) code based on the classical [7,4,3] Hamming code. It is more efficient than the Shor code, requiring only 7 physical qubits to encode 1 logical qubit while maintaining the same error-correcting capability. It can correct any single-qubit error.

COMPARISION

Aspect	Shor Code	Steane Code
Physical Qubits	9	7
Logical Qubits	1	1
Code Distance	3	3
Error Correction	Bit-flip and Phase-flip	All single-qubit errors
CSS Code	No	Yes
Stabilizer Code	Yes	Yes
Fault-Tolerant	Yes	Yes
Year Introduced	1995	1996
Efficiency	Lower (more qubits)	Higher (fewer qubits)
Implementation	Concatenated codes	Based on Hamming code

SECURITY ADVANTAGES OF QUANTUM CRYPTOGRAPHY

1.Detection of Eavesdropping

- Any attempt to measure quantum states (e.g., photons) inevitably **disturbs the system** due to the **Heisenberg Uncertainty Principle**.
- Such disturbances can be detected, allowing legitimate users to **identify and discard compromised keys**.
- Guarantees **communication integrity**.

2.Quantum Key Distribution (QKD) Security

- Keys are shared securely using quantum channels (e.g., BB84 protocol).
- Even if an attacker intercepts part of the transmission, they **cannot reproduce or copy** the quantum states (**no-cloning theorem**).
- Provides a **secure method of key exchange** immune to interception.

3.Resistance to Future (Quantum) Attacks

- Classical encryption methods may become obsolete with quantum computers (e.g., Shor’s algorithm can break RSA).
- Quantum cryptography remains **secure even in a post-quantum world**, as it’s protected by **laws of physics**, not algorithms.

4.No Dependence on Mathematical Complexity

- Traditional cryptography’s security depends on hard mathematical problems (factorization, discrete logs).
- Quantum cryptography bypasses this limitation, **eliminating the risk of algorithmic breakthroughs** or computational advances compromising security.

5. Long-Term Data Protection

- Even if encrypted data is stored and quantum computers are developed later, **past QKD-protected communications remain secure**.
- Provides **forward secrecy** and future-proof confidentiality.

6.Provable Randomness

- Quantum processes generate **truly random numbers**, essential for secure key generation.
- Prevents predictability and reduces the risk of pseudo-random vulnerabilities.

7.Unconditional Security

- Based on the fundamental principles of quantum mechanics rather than computational assumptions.
- Even with infinite computing power, an eavesdropper cannot break the encryption without detection.
- Ensures **information-theoretic security**, unlike traditional cryptosystems (RSA, ECC) that rely on mathematical complexity.

Authentication and Integrity Assurance

- Ensures that both sender and receiver are genuine and the transmitted message hasn’t been altered.
- Quantum authentication techniques can **detect impersonation or tampering** immediately.

QUANTUM KEY DISTRIBUTION

Definition:
A secure communication method that uses quantum mechanics to generate and distribute cryptographic keys between two parties.

•**Core Principle:**
Any attempt to eavesdrop on a quantum channel alters the quantum states being transmitted instantly revealing interception attempts.

•**Common Protocols:**
➢ **BB84 Protocol:** First and most widely used QKD protocol.
https://mgx.dev/app/d04bb5547adc45808d69921a3a60878c

➢ **E91 Protocol:** Based on quantum entanglement principles.

UNIT 4

- Von Neumann entropy
- Fidelity and quantum mutual information.
- Quantum teleportation.
- No-cloning theorem and superdense coding.
- Real-world applications .
- Quantum-Safe and Post-Quantum Cryptography.

Von Neumann entropy

- Classical information theory uses **Shannon entropy**

$$H(X) = -\sum p(x) \log p(x)$$

  To measure uncertainty of a random variable.
- In **quantum systems**, information is stored in **density matrices** (mixed states).
- The classical definition no longer works.
- So we need a quantum generalization: **Von Neumann Entropy**

“Why can’t we use Shannon entropy directly for quantum states?”

Because quantum states include ***superpositions****,* ***coherences****, and* ***entanglement****, which classical probability distributions cannot capture.*

WHY DO WE NEED VON NEUMANN ENTROPY ?

- To measure how much **quantum information** is present
- To quantify **entanglement**
- To know how much **noise or disturbance** a quantum state has
- To optimize **quantum algorithms**
- To understand **quantum thermal systems**

DENSITY MATRICES

Pure states

- A pure qubit: $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$
- Density matrix: $\rho=|\psi\rangle\langle\psi|$

Properties:

- $\rho 2=\rho$
- $Tr(\rho 2)=1$

DENSITY MATRICES

- **Mixed states**

A statistical mixture:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

Properties:

- $\rho 2 \neq \rho$
- $Tr(\rho 2) < 1$

DEFINITION OF VON NEUMANN ENTROPY

$$S(\rho) = -\mathrm{Tr}(\rho \log \rho)$$

$$S(\rho) = -\sum_i \lambda_i \log \lambda_i$$

WHY THIS DEFINITION?

- It reduces to **Shannon entropy** for diagonal (classical) states.
- It is invariant under basis changes:
- $S(U\rho U\dagger)=S(\rho)$
- It captures **quantum uncertainty**, including:
  - Mixture uncertainty
  - Decoherence
  - Entanglement

EXAMPLE 1: PURE STATE

$\rho = |\psi\rangle\langle\psi|$

Eigenvalues: 1, 0

$S(\rho) = -1\log 1 - 0\log 0 = 0$

- **Interpretation:**
  A pure state has no uncertainty → zero entropy.

EXAMPLE 2: MAXIMALLY MIXED QUBIT

$$\rho = \frac{1}{2} I = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

Eigenvalues: ½, ½

$$S(\rho) = -\left(\frac{1}{2} \log \frac{1}{2} + \frac{1}{2} \log \frac{1}{2} \right)$$

$$= \log 2 = 1 \quad \text{(in bits)}$$

Interpretation:

Maximum uncertainty (completely random qubit).

EXAMPLE 3: ENTANGLED STATE

Consider Bell state:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Full state entropy:

- The state is pure → **S = 0**

Reduced state (trace out one qubit):

$$\rho_A = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

$$S(\rho_A) = 1$$

Interpretation:

Entropy can measure **entanglement:**

Applications

- Measuring Entaglement
- Quantifying Decoherence
- Quantum channel capacities
- Quantum thermodynamics

RELATIVE ENTROPY

- **Definition**
- Quantum relative entropy measures how “different’’ two quantum states are.
- **$S(\rho \| \sigma)=Tr(\rho(\log\rho-\log\sigma)$**

Where:

- ρ and σ are density matrices
- It is **not symmetric** → not a distance, but a divergence

Intuition

- In classical information theory, relative entropy = KL divergence.
- It measures how costly it is to assume the state is σ when it is actually ρ.
- Bigger values → states are more distinguishable.

Key properties

- $S(\rho\|\sigma)\geq 0$ (non-negativity)
- Equality only if $\rho=\sigma$

QUANTUM CONDITIONAL ENTROPY

Definition

For a bipartite state ρ_{AB}:

$$S(A|B) = S(\rho_{AB}) - S(\rho_B)$$

Intuition

It quantifies the uncertainty about subsystem **A** given subsystem **B**.

Quantum twist

Quantum conditional entropy can be **negative**.

Example: For maximally entangled state $|\Phi^+\rangle$:

- $S(AB) = 0$ (pure)
- $S(B) = 1$

Thus:

$$S(A|B) = -1$$

Negative conditional entropy indicates **entanglement**:

B gives *more* information than is classically possible.

MUTUAL INFORMATION

Definition

$$I(A:B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$$

Intuition

Measures **total correlations** (classical + quantum) between A and B.

- If independent → $I(A:B) = 0$
- If perfectly correlated → maximal

Equivalent form:

$$I(A:B) = S(A) - S(A|B)$$

SUBADDITIVITY

Statement

For any bipartite state:

$$S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$$

Interpretation

Entropy of the whole is **not more** than the sum of parts.

Physical meaning:

- There is "shared information" between A and B that avoids double counting.

Equality → when $\rho_{AB} = \rho_A \otimes \rho_B$ (no correlations).

This inequality is equivalent to saying:

$$I(A:B) \geq 0$$

STRONG SUBADDITIVITY (SSA)

Statement

For tripartite state ρ_{ABC}:

$$S(\rho_{ABC}) + S(\rho_B) \leq S(\rho_{AB}) + S(\rho_{BC})$$

Equivalent form:

$$S(A|BC) \leq S(A|B)$$

Intuition

Having more information (B + C) cannot increase uncertainty about A.

It formalizes the idea:

> "Conditioning on more information never hurts."

MONOTONICITY OF RELATIVE ENTROPY

Statement (Data Processing Inequality)

For any quantum channel $\mathcal{E}$:

$$S(\rho\|\sigma) \geq S(\mathcal{E}(\rho)\|\mathcal{E}(\sigma))$$

Intuition

Processing data through a noisy channel **never makes states more distinguishable.**

Equivalent to:

> You can never gain information by throwing information away.

Why important?

- Foundation of quantum cryptography
- Justifies that eavesdropping creates disturbance
- Used in proving strong subadditivity

FIDELITY AND QUANTUM MUTUAL INFORMATION

- **Fidelity in Quantum Information**
- **Fidelity** is a measure of how close two quantum states are.
  It is widely used to evaluate:
- Accuracy of quantum communication
- Success of quantum cloning
- Quality of quantum gates
- Performance of quantum error correction

DEFINITION

For quantum states ρ and σ, the fidelity is:

$$F(\rho, \sigma) = \left(\mathrm{Tr} \sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}} \right)^2$$

For pure states

If $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$:

$$F(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle|^2$$

INTERPRETATION AND APPLICATION

- Fidelity close to **1** → high similarity, high success probability
- Fidelity close to **0** → states are highly distinguishable\

Applications

- Quantum teleportation fidelity
- Quantum error correction performance
- Benchmarking quantum circuits
- Verifying entangled-state generation

QUANTUM MUTUAL INFORMATION

Quantum Mutual Information measures **total correlations** (classical + quantum entanglement) between two quantum subsystems A and B.

Definition

$$I(A:B)=S(\rho A)+S(\rho B)-S(\rho AB)$$

Neumann entropy:

$$S(\rho)=-Tr(\rho log \rho)$$

Meaning

- QMI quantifies **how much information A and B share**.
- Includes both **classical correlations** and **quantum entanglement**.

RELATIONSHIP BETWEEN FIDELITY AND QUANTUM MUTUAL INFORMATION

- **Fidelity** measures **similarity** between states.
- **QMI** measures **correlation** between subsystems in a composite state.

Intuition:

- If fidelity of shared entangled states is high (close to the ideal Bell state), then mutual information is also high.
- Low fidelity states produce lower correlation and reduced QMI.

QUANTUM TELEPORTATION

- Quantum teleportation is a protocol that allows the transfer of an unknown quantum state from one location (Alice) to another (Bob) without physically sending the particle itself.

IT USES:

- Quantum entanglement
- Classical communication
- The original qubit is destroyed in the process, ensuring no cloning.

- https://in.video.search.yahoo.com/search/video;_ylt=Awr1Td2yMydpOtQvQKm9HAx.?p=star+trek+transporter+ship&type=E211IN1357G0&fr=mcafee&fr2=p%3As%2Cv%3Ai%2Cm%3Apivot#action=view&id=2&vid=caefba72c42dfb4b82d14f2cbabcceaf

WHY TELEPORTATION WORKS?

- Entanglement provides a non-local correlation link
- Classical communication ensures no faster-than-light signaling
- Bell-state measurement collapses the combined system
- Bob applies corrections to reconstruct the state exactly

APPLICATION

- Quantum networks
- Quantum repeaters
- Distributed quantum computers
- Secure quantum communication
- Quantum error correction
- Quantum memory transfer

Steps in quantum teleportation

Step1: Combine unknown qubit will bell pair.

Step2: Alice applies CNOT on first 2 qubits.

Step3: Alice applies hadamard on qubit 1.

Step4: Alice measures qubit 1 and 2.

Step5: Alice sends 2 classical bits to Bob.

Step 6 : Bob applies correction operation .

Step 7. Bob applies correction operation.

SUPER DENSE CODING

- Superdense coding is a fundamental quantum communication protocol that lets one party send **two classical bits** of information to another by transmitting **only one qubit**, provided they share an entangled pair beforehand.
- It’s a great example of how entanglement quantum operations beat classical limits.

HOW SUPERSDENSE CODING WORKS

- **Bob** prepares or receives an entangled Bell pair and sends one qubit to **Alice**.
- **Alice** encodes *2 classical bits* by applying quantum gates on her qubit.
- Alice sends **just one qubit** back to Bob.
- **Bob** measures both qubits in the Bell basis and recovers the **2-bit message**.

TELEPORTATION AND SUPERDENSE CODING

TELEPORTATION

- Alice → Bob: **2 classical bits**
- No qubit is sent during communication
- Bob reconstructs **a quantum sta**

SUPER DENSE CODING

- Alice → Bob: **1 qubit**
- Bob decodes **2 classical bit**

QUANTUM TELEPORTATION AND SUPER DENSE CODING

FEATURE	QUANTUM TELEPORTATION	SUPERDENSE CODING
Purpose	Transmit an *unknown quantum state* using classical bits + entanglement	Transmit *classical bits* using fewer qubits + entanglement
What is sent physically?	2 classical bits from Alice to Bob	1 qubit from Alice to Bob
How many bits of info effectively transmitted?	1 qubit (state) → using 2 classical bits	2 classical bits → using 1 qubit
Resource required beforehand	Shared Bell pair	Shared Bell pair
Who performs main quantum operation?	Alice performs Bell-state measurement	Alice performs local gate (I, X, Z, XZ)
Effect on the quantum state	Original quantum state is destroyed at Alice and reconstructed at Bob	No new quantum state is created; classical info encoded in entanglement
Direction of communication	Classical bits go from Alice → Bob	One qubit travels from Alice → Bob
Role of classical and quantum channels	Classical channel is essential (2 bits)	Quantum channel is essential (1 qubit)
What Bob does	Bob applies a unitary operation to reconstruct the quantum state	Bob performs Bell-basis measurement to read Alice's 2-bit message
Core idea	Entanglement + classical bits → move a quantum state	Entanglement + quantum gate → send 2 bits over 1 qubit
Does it violate no-cloning?	No — original qubit is destroyed	No — only classical bits are transmitted

APPLICATION

1. High-capacity classical communication using fewer qubits.
2. Quantum internet protocols.
3. Secure communication systems.
4. Bandwidth-efficient satellite communication.
5. Quantum network coding.

CONTINUED

APPLICATION AREA	WHY SUPERDENSE CODING HELPS
Quantum networks	Higher classical capacity
Satellite communication	Fewer qubits → less loss
Secure communication	Tamper detection, entanglement security
Bandwidth-limited channels	Doubles throughput
Network coding	Efficient routing and broadcasting
Quantum internet	Core component of communication stack
Education & research	Simple and demonstrative protocol

NO CLONING

- "Can we copy a classical bit? Y

Ans:?

- "Can we copy a quantum state $|\psi\rangle$?

Ans:?

- "Why might copying be difficult in quantum world?"

Take a superposition $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

“If a device could duplicate this unknown state exactly, what happens to superposition?”

DEFINITION

- The **no-cloning theorem** states that *it is impossible to create an identical copy of an arbitrary unknown quantum state.*
- **Classical copying vs. quantum copying**

Classical: $x \rightarrow (x, x)$

Quantum: would need a unitary U such that:

$$U\,|\psi\rangle\,|0\rangle = |\psi\rangle\,|\psi\rangle \text{ for } \textit{all}\ |\psi\rangle$$

Why “unknown state” matters:

- Known orthogonal states can be cloned (e.g., measuring 0 or 1).
- Arbitrary non-orthogonal states cannot.

NO CLONING IN QUANTUM COMPUTING

Qubit: A qubit (quantum bit) is the fundamental unit of quantum information.
Unlike a classical bit, which is either 0 or 1, a qubit can be in a combination (superposition) of both states.

Superposition: Superposition means that a qubit can exist in multiple states simultaneously until measured.

LINEARITY OF QUANTUM OPERATIONS

Quantum operations (including gates) are **linear transformations** on quantum states.
This means if an operation U acts on two basis states, it must act on their superposition **linearly**.

$$\textbf{If} \quad U|0\rangle=|a\rangle, U|1\rangle=|b\rangle,$$

for any superposition:

$$U(\alpha|0\rangle+\beta|1\rangle)=\alpha U|0\rangle+\beta U|1\rangle=\alpha|a\rangle+\beta|b\rangle.$$

WHY LINEARITY IS IMPORTANT

- Ensures predictability and consistency
- Crucial for no-cloning theorem
- Basis of quantum interference effects
- **Non-linear operations would break quantum mechanics** (e.g., allow perfect cloning, signal faster than light).

BASICS OF UNITARY EVOLUTION

- Isolated quantum systems evolve through **unitary operators**.
  A unitary operator U satisfies

$$U^\dagger U = I$$

This means the transformation:

- **Preserves inner products** (probabilities)
- **Is reversible**
- **Represents valid quantum time evolution**

EXAMPLES

Quantum gates = unitary operators
Examples:

- Hadamard (H)
- Pauli-X, Y, Z
- Rotation gates Rx,Ry,Rz
- CNOT
- Each gate must preserve probabilities → **must be unitary**.

APPLICATIONS & IMPLICATIONS

Quantum Teleportation

- Teleportation does NOT clone the state.
- Original is destroyed → consistent with no-cloning.

Quantum Cryptography (QKD)

- Eavesdropper cannot copy qubits in transit.
- Ensures security through disturbance.

Quantum Error Correction

- Works through entanglement, not cloning.
- Redundancy is encoded globally, not by copying qubits.

Measurement Disturbance

- You cannot “peek” at a quantum state without altering it.

???

- Give two states:
  (i) $|0\rangle$ and $|1\rangle$
  (ii) $|+\rangle$ and $|0\rangle$

- Which pairs can be cloned?

THEOREM

STATEMENT:

“**THERE IS NO UNITARY OPERATOR THAT CAN CLONE ARBITRAY QUBIT**”

Refer written notes for proving theorem

REAL WORLD APPLICATIONS

- **Drug Discovery & Healthcare:** Simulating molecular interactions for faster drug design, protein folding, and personalized medicine.
- **Finance:** Portfolio optimization, advanced risk modelling, fraud detection, and algorithmic trading.
- **Logistics & Supply Chain:** Optimizing complex routes, fleet management, and inventory, like improving delivery schedules.
- **Materials Science & Energy:** Designing new materials, improving battery technology (faster charging, longer life), creating better catalysts for green energy, and enhancing nuclear fusion.
- **Cybersecurity:** Developing quantum-resistant encryption (post-quantum cryptography) and secure communication (Quantum Key Distribution - QKD).
- **AI & Machine Learning:** Speeding up complex training for AI models and analysing massive datasets in new ways.
- **Climate & Environment:** High-resolution climate modelling, optimizing smart grids, and designing efficient carbon capture processes.
- **Manufacturing:** Optimizing production scheduling and quality control, such as Volkswagen's use for vehicle testing.
- **Telecommunications:** Enhancing mobile network performance and stability during peak usage, as demonstrated by NTT DOCOMO.

QUANTUM SAFE POST QUANTUM CRYTOGRAPHY

- **Post-Quantum Cryptography (PQC)** refers to a set of cryptographic algorithms designed to remain secure **even in the presence of large-scale quantum computers**.

- These algorithms are built on mathematical problems that are believed to be **hard for both classical and quantum computers**, unlike RSA and ECC which can be broken by quantum attacks.

NEED FOR POST-QUANTUM CRYPTOGRAPHY

1. **Quantum computers break current public-key cryptosystems**
2. **Shor's algorithm** can factor large integers and solve discrete logarithms in polynomial time.

This breaks **RSA**, **Diffie–Hellman**, and **ECC**, which secure most communication today.

3.Long-term data security ("Harvest Now, Decrypt Later" attacks)

- Attackers can store encrypted data today and decrypt it in the future once quantum computers mature.
- Sensitive data like medical records, Aadhaar data, defense messages, and financial transactions require 10–20+ years of security.

4.Security of global digital infrastructure

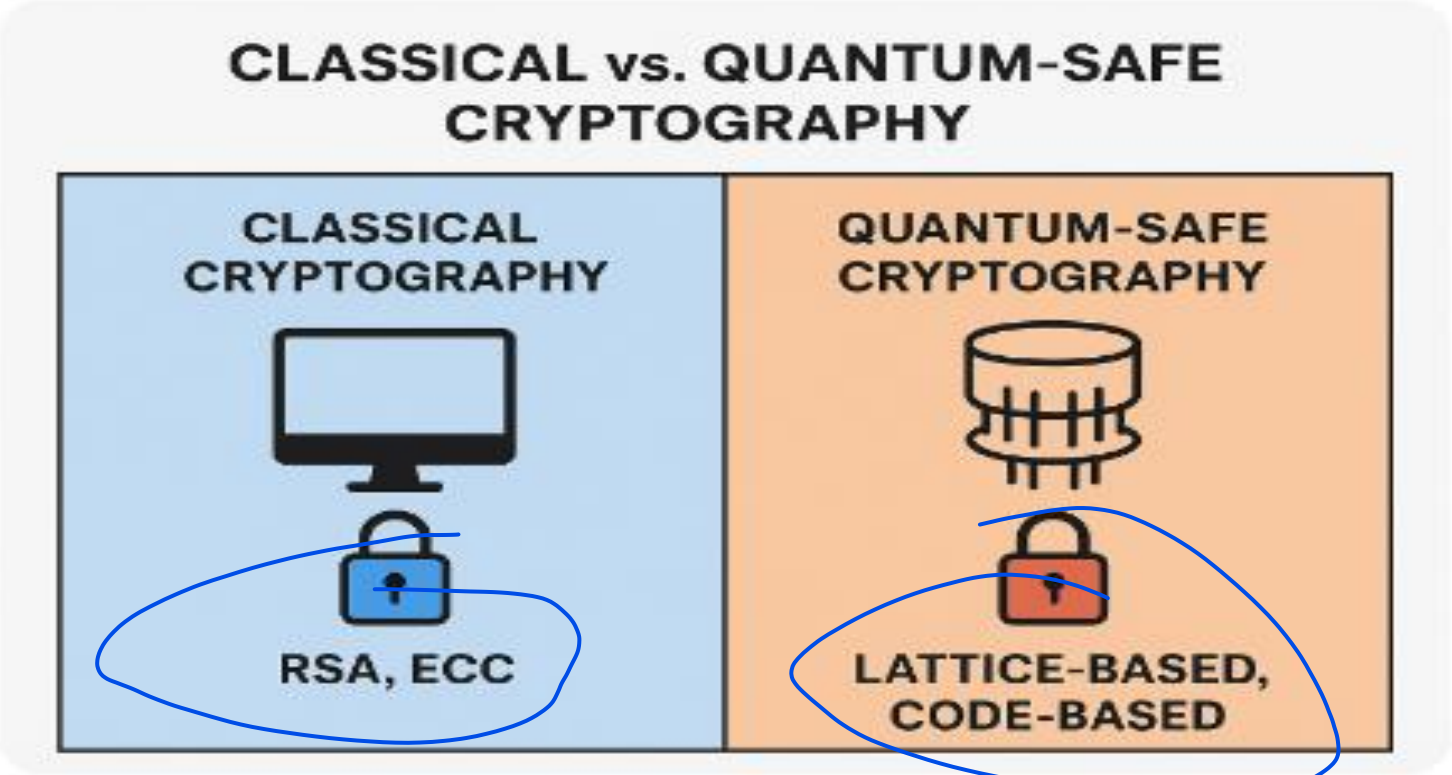
- Internet protocols such as **TLS/HTTPS**, **VPN**, **email encryption**, **blockchain**, and **software updates** rely on RSA/ECC.
- All these will become vulnerable in the post-quantum era.

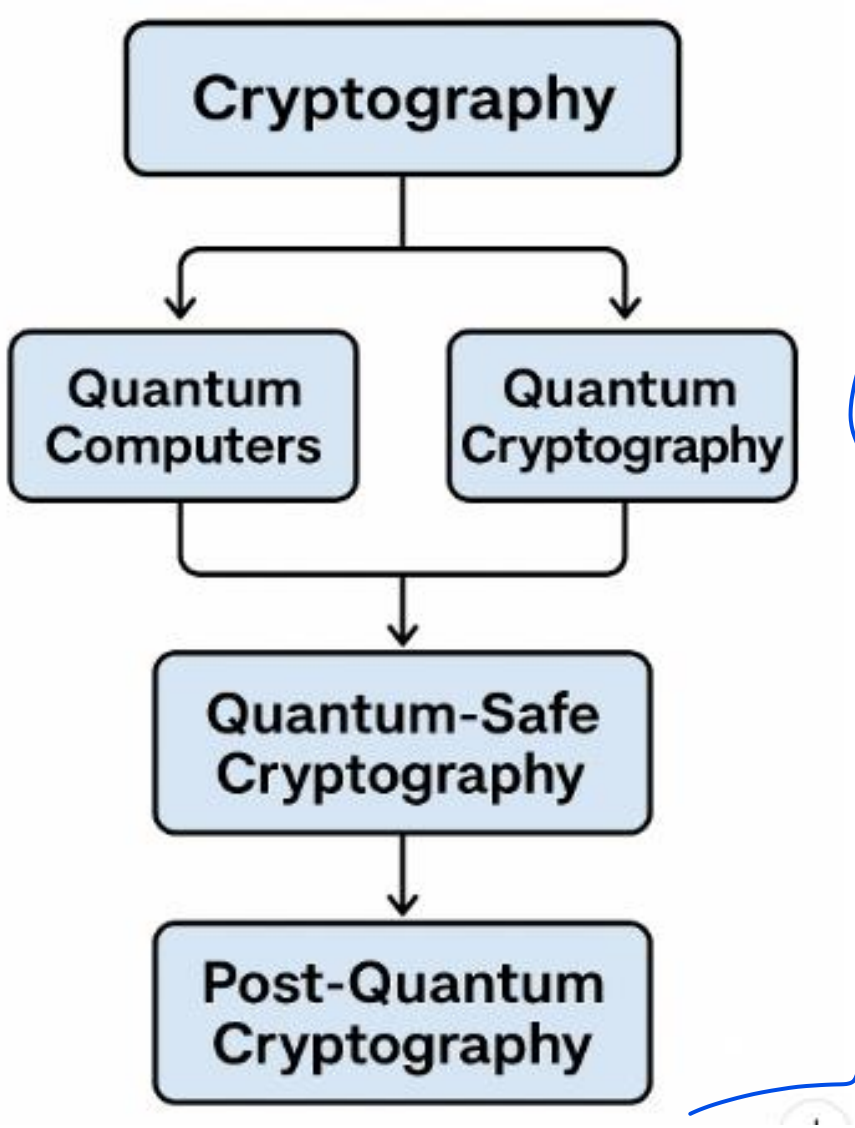
5.Early preparation for migration

- Transitioning the entire world's infrastructure to PQC will take many years.

Standardization (NIST PQC) is already in progress, so organizations must start planning.

CLASSICAL VERSUS QUANTUM SAFE CRYPTOGRAPHY




Cryptography
Quantum Computers
Quantum Cryptography
Quantum-Safe Cryptography
Post-Quantum Cryptography

CRYPTOGRAPHY

Cryptography is the science of securing communication.
All modern digital systems—banking, Aadhaar, emails, military communication, cloud services—depend on:

- **Symmetric cryptography** (AES, DES)
- **Asymmetric cryptography** (RSA, ECC)
- **Hash functions** (SHA-256, SHA-3)

Traditional cryptography assumes that attackers have **classical computers**.

QUANTUM COMPUTERS

Large-scale quantum computers can run **Shor's Algorithm**, which breaks:

- RSA (based on integer factorization)
- ECC (based on discrete logarithms)
- Diffie–Hellman key exchange

Therefore, future quantum machines threaten current cryptosystems.

QUANTUM CRYPTOGRAPHY

Quantum cryptography **uses quantum mechanics** to secure communication.

Quantum Key Distribution (QKD)

- Uses photons to transmit encryption keys
- Security guaranteed by the laws of quantum physics
- Any eavesdropping disturbs photons → detected immediately

- Quantum Cryptography is secure even against quantum computers. But it requires **special hardware**, optical fibers, and cannot work on all networks.

QUANTUM-SAFE CRYPTOGRAPHY

Quantum-safe cryptography refers to any cryptographic method that remains secure even if the attacker has a quantum computer.

- Quantum-safe includes two broad families:

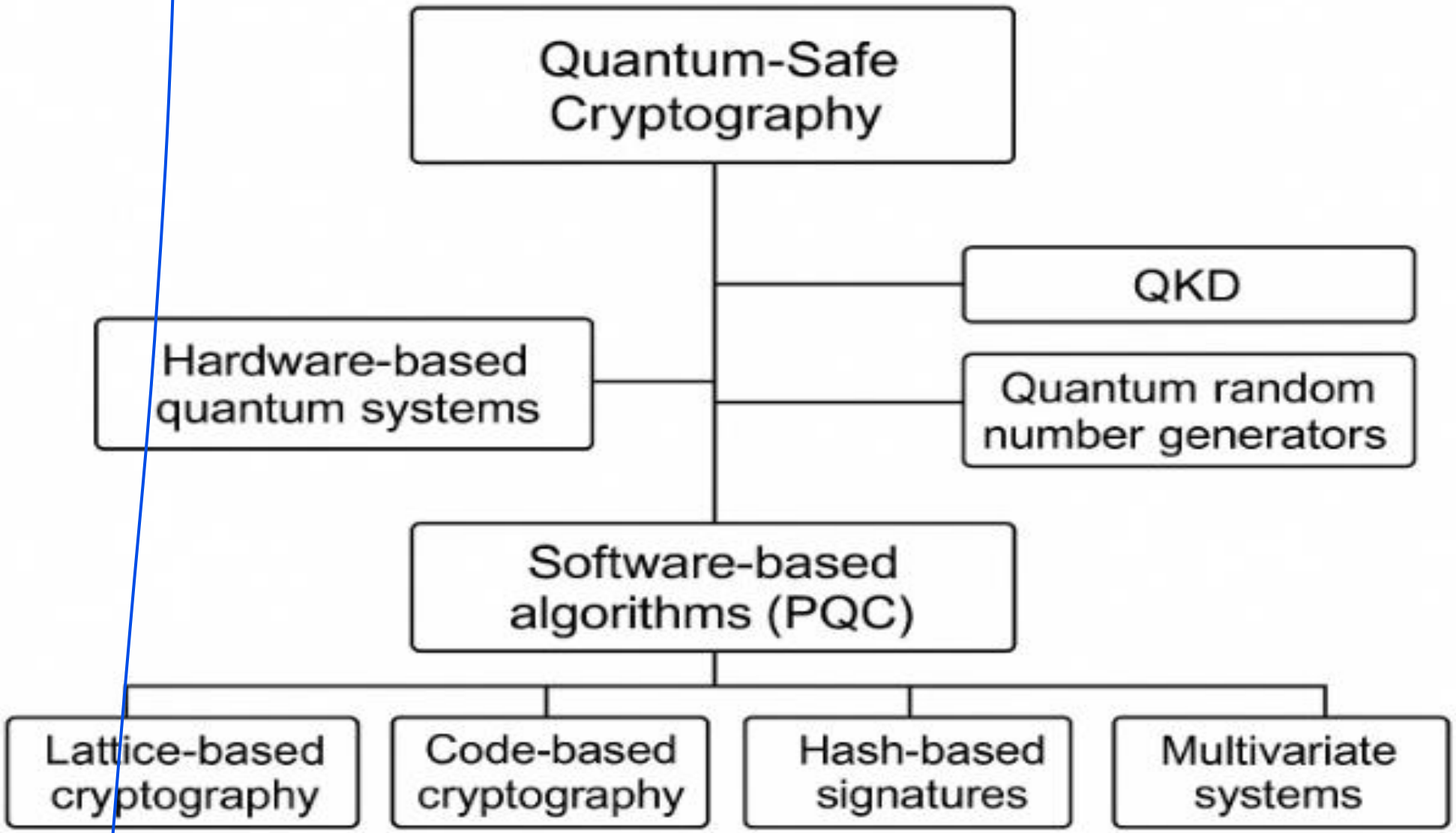
A. Hardware-based quantum systems

- QKD
- Quantum random number generators

B. Software-based algorithms (PQC)

- Lattice-based cryptography
- Code-based cryptography
- Hash-based signatures
- Multivariate systems

"quantum-safe" is an umbrella term that covers *both* quantum hardware solutions and algorithmic (classical but secure) solutions.


Quantum-Safe Cryptography
QKD
Hardware-based quantum systems
Quantum random number generators
Software-based algorithms (PQC)
Lattice-based cryptography
Code-based cryptography
Hash-based signatures
Multivariate systems

POST-QUANTUM CRYPTOGRAPHY

- Algorithms that run on **classical computers**, but are secure even against quantum attacks.
- PQC does **not** require quantum hardware
- Works in today's networks (TLS, SSL, VPNs, WiFi, IoT)
- Can be deployed immediately
- Selected and standardized by NIST

Examples (NIST PQC Standards):

- **CRYSTALS-Kyber** (KEM)
- **CRYSTALS-Dilithium** (signature)
- **FALCON** (signature)
- **SPHINCS+** (hash-based signature)

NIST(**National Institute of Standards and Technology**)

- **NIST (National Institute of Standards and Technology)**

NIST is the **U.S. standards body** responsible for selecting and standardizing **Post-Quantum Cryptography (PQC)** algorithms.

Why NIST matters?

- Global Internet security infrastructure (TLS, HTTPS, VPNs, certificates) follows NIST standards.
- Governments, banks, cybersecurity agencies, and vendors adopt NIST-approved algorithms.

CATEGORY	ALGORITHM	TYPE
Key Encapsulation (KEM)	**CRYSTALS-Kyber**	Lattice-based
Digital Signatures	**CRYSTALS-Dilithium**	Lattice-based
	FALCON	Lattice-based
	SPHINCS+	Hash-based

LINK

- ://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards?utm_source=chatgpt.com

- https://quantum.cloud.ibm.com/learning/en/courses/quantum-safe-cryptography/quantum-safe-cryptography

QUICK REFERENCE -**UNIT 3**

TOPIC	SOURCE
Quantum Error Correction and Cryptography	PPT
Types of quantum errors and noise	PPT
Quantum Error-Correcting Codes: BIT FLIP PHASE FLIP	https://mgx.dev/app/0250a43e40f14e879c00756a7ebf7ff5 NOTES NOTES
Shor and Steane error-correcting codes	NOTES
Security advantages of quantum cryptography	PPT
Quantum key distribution BB84 protocol	https://quantum.cloud.ibm.com/learning/en/modules/computer-science/quantum-key-distribution https://mgx.dev/app/d04bb5547adc45808d69921a3a60878c

QUICK REFERENCE -**UNIT 4**

TOPIC	SOURCE
Von Neumann entropy	PPT & PROBLEMS
Fidelity and quantum mutual information.	PPT & PROBLEMS
Quantum Teleportation.	NOTES
No-cloning theorem Superdense coding.	NOTES
Real-world applications .	PPT https://www.geeksforgeeks.org/artificial-intelligence/application-of-quantum-computing/
Quantum-Safe and Post-Quantum Cryptograph	https://quantum.cloud.ibm.com/learning/en/courses/quantum-safe-cryptography PPT