खंड २, अंक १, फरवरी –२०२६
ई–विज्ञानम
मासिक विज्ञान पत्रिका

Vol. 2, Issue 1, February-2026
e-vigyanam
Monthly Science Journal
सामान्य आलेख- प्रौद्योगिकी (General Article-Technology)

DOI: 10.66346/ev.v2i1.2026.2

क्वांटम कंप्यूटिंग और क्रिप्टोग्राफ़ी: एक क्वांटम-मैकेनिकल दृष्टिकोण

रजनी सिंह*
गणित एवं वैज्ञानिक संगणक विभाग, मदन मोहन मालवीय प्रौद्योगिकी विश्वविद्यालय, गोरखपुर, उ०प्र०, भारत-273010
लेखक से संवाद के लिए ईमेल*- 2024113011@mmmut.ac.in

आलेख प्राप्त: ०८ फरवरी २०२६; अंतिम संशोधित: १८ मार्च २०२६; स्वीकृत: २५ मार्च २०२६
प्रथम ऑनलाइन प्रकाशित: २६ अप्रैल २०२६

सारांश

सुपरपोज़ीशन, एंटैंगलमेंट तथा मापन जैसे क्वांटम यांत्रिकी के सिद्धांतों पर आधारित क्वांटम कम्प्यूटिंग गणना की एक पूर्णतः नई और क्रांतिकारी पद्धति है। क्वांटम कम्प्यूटर सूचना के प्रसंस्करण के लिए द्विआधारी बिट्स के स्थान पर क्वांटम बिट्स अथवा क्यूबिट्स का उपयोग करते हैं, जिनके माध्यम से कुछ गणनाएँ पारंपरिक कम्प्यूटरों की तुलना में कई गुना अधिक तेज़ी से सम्पन्न की जा सकती हैं। यह लेख सर्वप्रथम क्वांटम की अवधारणा का परिचय देता है तथा यह स्पष्ट करता है कि क्वांटम गणना किस प्रकार की जाती है | इसके पश्चात क्वांटम कम्प्यूटिंग के विकास का एक संक्षिप्त कालानुक्रमिक इतिहास प्रस्तुत किया गया है, साथ ही इसके वर्तमान अनुप्रयोगों और भविष्य की संभावित प्रगतियों पर भी चर्चा की गई है। विशेष रूप से क्वांटम भौतिकी और क्रिप्टोग्राफी के बीच संबंध पर ध्यान केंद्रित किया गया है, जिसमें पारंपरिक क्रिप्टोप्रणालियों के लिए क्वांटम एल्गोरिद्म द्वारा उत्पन्न खतरे तथा क्वांटम क्रिप्टोग्राफी द्वारा प्रदान की जाने वाली संभावनाओं को सम्मिलित किया गया है। संपूर्ण लेख में मानक संदर्भों का उल्लेख किया गया है तथा वैचारिक समझ को सुदृढ़ करने हेतु उपयुक्त शीर्षकों सहित चित्रों को सम्मिलित किया गया है।

सूचक शब्द: सुपरपोज़ीशन, एंटैंगलमेंट, मापन, क्रिप्टोग्राफी

खंड २, अंक १, फरवरी –२०२६
ई–विज्ञानम
मासिक विज्ञान पत्रिका

Vol. 2, Issue 1, February-2026
e-vigyanam
Monthly Science Journal
सामान्य आलेख- प्रौद्योगिकी (General Article-Technology)

DOI: 10.66346/ev.v2i1.2026.2

Quantum Computing and Cryptography: A Quantum-Mechanical Approach

Rajni Singh*
Department of Mathematics and Scientific Computing, Madan Mohan Malaviya University of Technology, Gorakhpur, Uttar Pradesh, India -273010
Corresponding Author Email*: 2024113011@mmmut.ac.in

Received On: 08 February 2026; Final Revision: 18 March 2026; Accepted On: 25 March 2026
Published Online First: 26 April 2026

ABSTRACT

Quantum computing is a revolutionary paradigm of computation based on the fundamental principles of quantum mechanics such as superposition, entanglement, and measurement. Unlike classical computers that process information using binary bits, quantum computers utilize quantum bits or qubits, which enable certain computations to be performed significantly faster than traditional computational methods. This paper first introduces the concept of quantum mechanics and explains how quantum computation is performed. It then presents a brief chronological overview of the development of quantum computing, along with a discussion of its current applications and potential future advancements. Particular emphasis is placed on the relationship between quantum physics and cryptography. The paper highlights the potential threats posed by quantum algorithms to classical cryptographic systems, as well as the promising opportunities offered by quantum cryptography for secure communication. Standard references are included throughout the article, and illustrative figures with appropriate headings are incorporated to enhance conceptual understanding.

Keywords: superposition; entanglement; measurement; cryptography

1.क्वांटम क्या है?

क्वांटम शब्द की उत्पत्ति क्वांटम यांत्रिकी से हुई है और यह किसी भौतिक राशि की सबसे छोटी विसंयुक्त (Discrete) इकाई को दर्शाता है [1] । क्वांटम भौतिकी में ऊर्जा, कोणीय संवेग (Angular Momentum) तथा स्पिन जैसे भौतिक प्रेक्षणीय निरंतर रूप से परिवर्तित नहीं होते, बल्कि वे केवल कुछ निश्चित मान ही ग्रहण करते हैं, जिन्हें क्वांटा (Quanta) कहा जाता है। उदाहरणस्वरूप, किसी परमाणु के भीतर इलेक्ट्रॉन के ऊर्जा स्तर क्वांटीकृत होते हैं।

इस क्वांटीकरण के परिणामस्वरूप अनेक ऐसे गैर-पारंपरिक (Non-classical) घटनाक्रम उत्पन्न होते हैं, जिनमें प्रमुख रूप से निम्नलिखित शामिल हैं:

• सुपरपोज़ीशन (Superposition): एक क्वांटम तंत्र एक ही समय में एक से अधिक अवस्थाओं में अस्तित्व में रह सकता है।

• एंटैंगलमेंट (Entanglement): दो या अधिक क्वांटम तंत्रों के बीच ऐसा गहरा संबंध हो सकता है जिसे पारंपरिक भौतिकी द्वारा समझाया नहीं जा सकता।

•मापनपतन (MeasurementCollapse): जब किसी क्वांटम तंत्र का मापन किया जाता है, तो वह अनेक संभावित अवस्थाओं में से किसी एक निश्चित अवस्था में परिवर्तित हो जाता है।

ये सभी अवधारणाएँ क्वांटम कम्प्यूटिंग की भौतिक आधारशिला का निर्माण करती हैं [2]।

2.क्वांटम कम्प्यूटिंग कैसे की जाती है?

क्वांटम कम्प्यूटिंग में क्यूबिट्स (Qubits) को सूचना की मूल इकाई के रूप में उपयोग किया जाता है। एक क्यूबिट एक ही समय में दोनों अवस्थाओं के सुपरपोज़ीशन में अस्तित्व में रह सकता है, जबकि पारंपरिक बिट केवल 0 या 1 में से किसी एक अवस्था में ही हो सकता है। इसे गणितीय रूप से इस प्रकार व्यक्त किया जाता है:

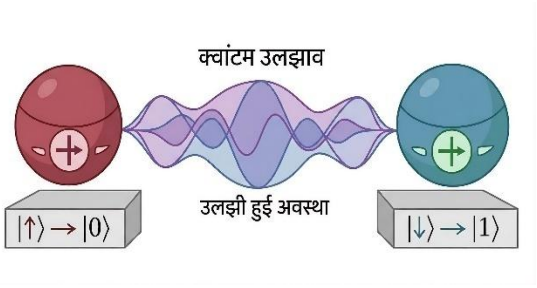
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

जहाँ α और β जटिल (Complex) प्रायिकता आयाम (Probability Amplitudes) होते हैं।

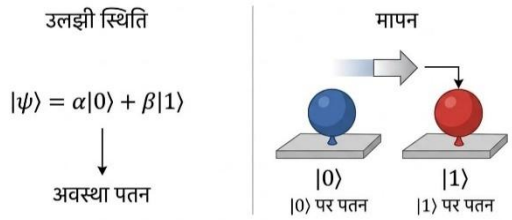
2.1. क्वांटम गणना के आवश्यक तत्त्व

- क्यूबिट का भौतिक क्रियान्वयन: क्यूबिट्स को साकार करने के लिए इलेक्ट्रॉन का स्पिन, फोटॉन का ध्रुवण (Polarization) अथवा सुपरकंडक्टिंग परिपथ जैसे भौतिक तंत्रों का उपयोग किया जाता है।
- क्वांटम गेट्स: क्वांटम गेट्स यूनिटरी संक्रियाएँ होती हैं जो क्यूबिट्स की अवस्था को परिवर्तित करती हैं, जैसे हैडमार्ड (Hadamard), पाउली (Pauli) तथा CNOT गेट।
- क्वांटम परिपथ (Quantum Circuits): गणनात्मक उद्देश्यों के लिए क्यूबिट्स पर लागू किए गए क्वांटम गेट्स के क्रम को क्वांटम परिपथ कहा जाता है।
- मापन (Measurement): मापन की प्रक्रिया में क्यूबिट्स की क्वांटम अवस्था पतित होकर शास्त्रीय सूचना (0 या 1) में परिवर्तित हो जाती है।

क्वांटम एल्गोरिद्म को निष्पादित करने की प्रक्रिया में पहले एक प्रारंभिक क्वांटम अवस्था तैयार की जाती है, उसके पश्चात क्यूबिट्स पर क्वांटम गेट्स की एक श्रृंखला लागू की जाती है, और अंत में अंतिम अवस्था का मापन कर परिणाम प्राप्त किया जाता है।



आकृति 1: स्थानिक रूप से पृथक क्यूबिट्स के बीच क्वांटम उलझाव :- इस आकृति में दो दूर-दूर स्थित क्यूबिट्स के बीच क्वांटम उलझाव दर्शाया गया है। उलझी हुई अवस्था में एक क्यूबिट का मापन दूसरे क्यूबिट की अवस्था को तुरंत निर्धारित कर देता है, चाहे उनके बीच कितनी भी दूरी क्यों न हो।



आकृति 2: क्वांटम सुपरपोज़िशन एवं मापन के दौरान अवस्था का पतन :- यह आकृति दर्शाती है कि एक क्यूबिट मापन से पहले सुपरपोज़िशन अवस्था $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ में रहता है। मापन करने पर क्वांटम अवस्था का पतन (State Collapse) होता है और क्यूबिट निश्चित रूप से $|0\rangle$ या $|1\rangle$ में परिवर्तित हो जाता है।

3.संक्षिप्त इतिहास और कालानुक्रमिक विकास

क्वांटम कम्प्यूटिंग के इतिहास में कई महत्वपूर्ण मोड़ (Turning Points) पहचाने जा सकते हैं:

- 1900 से 1930 के बीच : प्लैंक, आइंस्टीन, बोहर, हाइज़ेनबर्ग तथा श्रोडिंगर जैसे वैज्ञानिकों ने क्वांटम यांत्रिकी की आधारशिला रखी।
- 1981: रिचर्ड फाइनमैन ने क्वांटम तंत्रों की सहायता से भौतिक प्रक्रियाओं के अनुकरण (Simulation) का विचार प्रस्तुत किया।
- 1985: डेविड डॉयच ने सार्वभौमिक क्वांटम कम्प्यूटर (Universal Quantum computer) की अवधारणा को औपचारिक रूप दिया।
- 1994: पीटर शोर ने पूर्णांकों के गुणनखंडन के लिए शोर का एल्गोरिद्म प्रस्तुत किया, जिसने पारंपरिक एल्गोरिद्मों की तुलना में घातीय (Exponential) गति-वृद्धि को प्रदर्शित किया।[3]

- 1996: लोव ग्रोवर ने ग्रोवर का खोज एल्गोरिद्म प्रस्तावित किया, जो असंरचित खोज समस्याओं के लिए द्विघात (Quadratic) गति-वृद्धि प्रदान करता है।[4]

- 2000 के दशक से वर्तमानतक: सुपरकंडक्टिंग क्यूबिट्स, ट्रैप्ड आयन तथा फोटोनिक प्रणालियों पर आधारित लघु-स्तरीय क्वांटम प्रोसेसरों का प्रयोगात्मक रूप से साकार किया गया है।

4.क्वांटम कंप्यूटिंग और क्वांटम यांत्रिकी

क्वांटम यांत्रिकी का एक प्रत्यक्ष अनुप्रयोग क्वांटम कम्प्यूटिंग है। क्वांटम यांत्रिकी की गणितीय आधारशिला—जैसे हिल्बर्ट स्पेस, रैखिक संक्रियक (Linear Operators) तथा प्रायिकता आयाम (Probability Amplitudes)—क्वांटम गणना की नींव का निर्माण करती है। इंटरफेरेंस (हस्तक्षेप) और एंटैंगलमेंट (उलझाव) जैसी घटनाओं का जानबूझकर उपयोग किया जाता है ताकि सही गणनात्मक पथों को सुदृढ़ किया जा सके तथा त्रुटिपूर्ण पथों को न्यूनतम किया जा सके। इसके परिणामस्वरूप ऐसी गणनात्मक क्षमताएँ प्राप्त होती हैं जो पारंपरिक कम्प्यूटिंग में संभव नहीं हैं। [5]

5.क्वांटम कंप्यूटिंग और क्रिप्टोग्राफी

5.1. पारंपरिक क्रिप्टोग्राफी के लिए खतरा

कई पारंपरिक क्रिप्टोग्राफिक विधियों की सुरक्षा गणितीय समस्याओं की गणनात्मक कठिनाई पर आधारित होती है। उदाहरणस्वरूप:

- RSA और ECC (Elliptic Curve Cryptography) डिस्क्रीट लॉगरिद्म तथा पूर्णांक गुणनखंडन जैसी जटिल समस्याओं पर निर्भर करती हैं।

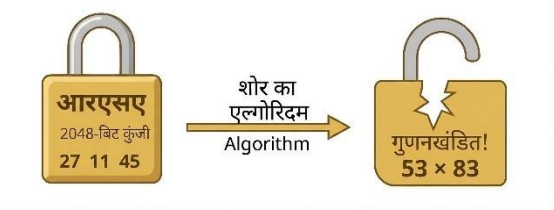
- वर्तमान पब्लिक-की क्रिप्टोसिस्टम्स के लिए शोर का एल्गोरिद्म एक गंभीर खतरा प्रस्तुत करता है, क्योंकि पर्याप्त रूप से शक्तिशाली क्वांटम कम्प्यूटर पर यह इन समस्याओं को प्रभावी ढंग से हल कर सकता है।

5.2.क्वांटम क्रिप्टोग्राफी

इसके अतिरिक्त, क्वांटम भौतिकी सुरक्षित संचार के लिए नई संभावनाएँ भी प्रदान करती है:

- क्वांटम कुंजी वितरण (Quantum Key Distribution – QKD) प्रणालियाँ, जैसे BB84, मापन से उत्पन्न विक्षोभ तथा नो-क्लोनिंग प्रमेय (No-Cloning Theorem) का उपयोग करके बिना शर्त सुरक्षा (Unconditional Security) सुनिश्चित करती हैं।

- किसी भी प्रकार की जासूसी (Eavesdropping) का प्रयास मापन में त्रुटियाँ उत्पन्न करता है, जिन्हें आसानी से पहचाना जा सकता है, जिससे सुरक्षित कुंजी विनिमय सुनिश्चित होता है।

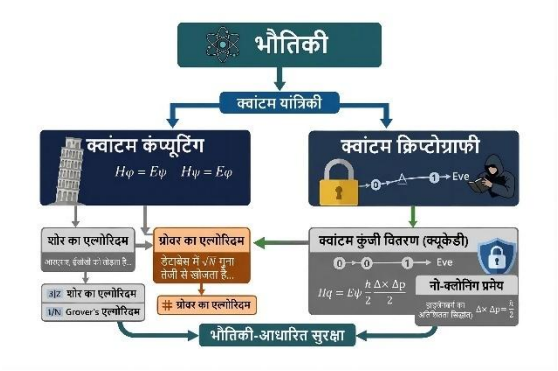


आकृति 3: RSA क्रिप्टोग्राफी पर शोर के एल्गोरिथ्म का प्रभाव :- यह आकृति दिखाती है कि कैसे शोर का क्वांटम एल्गोरिथ्म RSA जैसी पारंपरिक सार्वजनिक-कुंजी क्रिप्टोग्राफी को तोड़ सकता है। क्वांटम कंप्यूटर बड़ी संख्याओं का गुणनखंड कुशलता से निकाल सकता है, जिससे RSA की सुरक्षा कमजोर हो जाती है।

क्वांटम कंप्यूटिंग के तीव्र विकास के कारण पारंपरिक सार्वजनिक-कुंजी क्रिप्टोग्राफी प्रणालियाँ जैसे RSA और ECC भविष्य में असुरक्षित हो सकती हैं, क्योंकि शक्तिशाली क्वांटम कंप्यूटर Shor's Algorithm के माध्यम से बड़े पूर्णांकों के गुणनखंडन (factorization) तथा विविक्त लघुगणक (discrete logarithm) जैसी गणितीय समस्याओं को अपेक्षाकृत कम समय में हल कर सकते हैं। इस संभावित खतरे को देखते हुए शोधकर्ताओं ने पोस्ट-क्वांटम क्रिप्टोग्राफी (Post-Quantum Cryptography) का विकास प्रारंभ किया है। यह ऐसी क्रिप्टोग्राफिक तकनीकों का समूह है जो उन गणितीय समस्याओं पर आधारित होती हैं जिन्हें न केवल पारंपरिक कंप्यूटर बल्कि क्वांटम कंप्यूटर के लिए भी हल करना अत्यंत कठिन माना जाता है।

पोस्ट-क्वांटम क्रिप्टोग्राफी के प्रमुख वर्गों में लैटिस-आधारित क्रिप्टोग्राफी (Lattice-Based Cryptography), कोड-आधारित क्रिप्टोग्राफी (Code-Based Cryptography), हैश-आधारित क्रिप्टोग्राफी (Hash-Based Cryptography) तथा मल्टीवेरिएट बहुपद क्रिप्टोग्राफी (Multivariate Polynomial Cryptography) शामिल हैं। लैटिस-आधारित क्रिप्टोग्राफी उच्च आयामी वेक्टर स्पेस में स्थित बिंदुओं की ज्यामितीय संरचना पर आधारित होती है, जहाँ Shortest Vector Problem (SVP) तथा Learning With Errors (LWE) जैसी समस्याएँ अत्यंत कठिन मानी जाती हैं। इसी प्रकार कोड-आधारित क्रिप्टोग्राफी त्रुटि-सुधार कोड (error-correcting codes) पर आधारित होती है, जबकि हैश-आधारित क्रिप्टोग्राफी सुरक्षित क्रिप्टोग्राफिक हैश फ़ंक्शन का उपयोग करके डिजिटल हस्ताक्षर (digital signatures) प्रदान करती है।

हाल के वर्षों में कई अंतरराष्ट्रीय मानकीकरण संस्थाएँ, विशेष रूप से NIST (National Institute of Standards and Technology), पोस्ट-क्वांटम एल्गोरिद्म के मानकीकरण पर कार्य कर रही हैं। NIST द्वारा प्रस्तावित कुछ महत्वपूर्ण एल्गोरिद्म जैसे CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, और SPHINCS+ को भविष्य की सुरक्षित संचार प्रणालियों के लिए संभावित मानक के रूप में चुना गया है। इन एल्गोरिद्म का उद्देश्य यह सुनिश्चित करना है कि भविष्य में भी डिजिटल संचार, डेटा गोपनीयता और साइबर सुरक्षा को क्वांटम कंप्यूटरों के संभावित खतरे से सुरक्षित रखा जा सके।

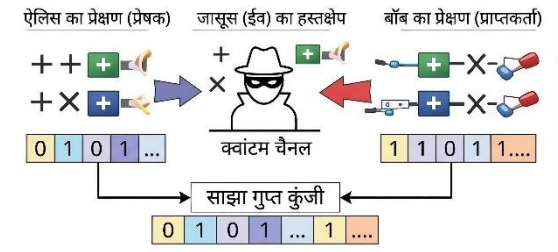


आकृति 4: क्वांटम यांत्रिकी से उत्पन्न क्वांटम कंप्यूटिंग तथा क्वांटम क्रिप्टोग्राफी की भौतिकी-आधारित सुरक्षा प्रणाली

6.भौतिकी-आधारित सुरक्षा की गारंटी:-

क्वांटम क्रिप्टोग्राफी की सुरक्षा अंततः मापन के दौरान क्वांटम प्रणालियों के भौतिक व्यवहार द्वारा सुनिश्चित होती है। जब कोई आक्रमणकारी क्वांटम संचार चैनल को देखने या मापने का प्रयास करता है, तो मापन की यह क्रिया क्वांटम अवस्थाओं को परिवर्तित कर देती है, जिसके परिणामस्वरूप साझा कुंजी में स्पष्ट त्रुटियाँ उत्पन्न होती हैं। इन त्रुटि दरों की निगरानी करके वैध उपयोगकर्ता गुप्त रूप से की जा रही जासूसी का पता लगा सकते हैं और समझौता की गई कुंजियों को त्याग सकते हैं।

इस प्रकार, क्वांटम क्रिप्टोग्राफी की सुरक्षा संगणनात्मक सीमाओं से संबंधित मान्यताओं पर नहीं, बल्कि प्राकृतिक भौतिक नियमों पर आधारित होती है, जिससे यह भविष्य की तकनीकी प्रगति के प्रति कहीं अधिक प्रतिरोधी बन जाती है।



आकृति 5: BB84 क्वांटम कुंजी वितरण (Quantum Key Distribution) प्रोटोकॉल :- यह आकृति BB84 प्रोटोकॉल को दर्शाती है, जिसमें प्रेषक (एलिस) और प्राप्तकर्ता (बॉब) फोटॉनों के क्वांटम अवस्थाओं का उपयोग करके एक साझा गुप्त कुंजी स्थापित करते हैं। किसी भी अनधिकृत हस्तक्षेप (ईव्सड्रॉपर) की स्थिति में त्रुटियाँ उत्पन्न होती हैं, जिससे जासूसी का पता चल जाता है।

7.पोस्ट-क्वांटम क्रिप्टोग्राफी में क्वांटम भौतिकी की भूमिका

जहाँ क्वांटम क्रिप्टोग्राफी क्वांटम तकनीक का उपयोग करती है, वहीं पोस्ट-क्वांटम क्रिप्टोग्राफी ऐसी पारंपरिक (क्लासिकल) विधियाँ विकसित करती है जो क्वांटम हमलों के प्रति प्रतिरोधी होती हैं। फिर भी, इस संदर्भ में भी भौतिकी हमारी समझ में मदद करती है, विशेषकर निम्नलिखित पहलुओं में:

- संगणनात्मक सीमाएँ (Computational limitations)
- शोर और डीकोहेरेंस (Noise and decoherence)
- वृहद-स्तरीय क्वांटम कंप्यूटरों की भौतिक व्यावहारिकता (Physical feasibility of large-scale quantum computers)

इन भौतिक पहलुओं का अध्ययन यह निर्धारित करने में सहायक होता है कि क्वांटम-प्रतिरोधी प्रणालियाँ कितनी प्रभावी और व्यवहार में लागू करने योग्य हैं।

[6]

8.आधुनिक पोस्ट-क्वांटम क्रिप्टोग्राफी और हाल की प्रगति

क्वांटम संगणना में तीव्र प्रगति ने पारंपरिक सार्वजनिक-कुंजी क्रिप्टोग्राफी जैसे RSA और ECC की दीर्घकालिक सुरक्षा पर गंभीर प्रश्न उत्पन्न कर दिए हैं, क्योंकि शोर के एल्गोरिद्म जैसे क्वांटम एल्गोरिद्म बड़े पूर्णांकों के गुणनखंडन को बहुपद समय में हल करने में सक्षम हैं। इसी संदर्भ में पोस्ट-क्वांटम क्रिप्टोग्राफी (Post-Quantum Cryptography – PQC) का विकास हुआ है, जिसका उद्देश्य ऐसे क्रिप्टोग्राफिक तंत्र विकसित करना है जो शास्त्रीय तथा क्वांटम दोनों प्रकार के आक्रमणों के विरुद्ध सुरक्षित हों। आधुनिक PQC मुख्यतः उन गणितीय समस्याओं पर आधारित है जिन्हें क्वांटम कंप्यूटर द्वारा भी कुशलतापूर्वक हल करना कठिन माना जाता है। इनमें लैटिस-आधारित, कोड-आधारित, हैश-आधारित तथा बहुवेरीय बहुपद-आधारित प्रणालियाँ प्रमुख हैं।

लैटिस-आधारित क्रिप्टोग्राफी विशेष रूप से Learning With Errors (LWE) समस्या पर आधारित है, जिसे निम्न प्रकार व्यक्त किया जाता है:

$$As+e \equiv b(modq)$$

यहाँ A एक ज्ञात मैट्रिक्स है, s गुप्त वेक्टर, e एक छोटा त्रुटि वेक्टर तथा q मॉड्यूलस है। इस समीकरण से sss को ज्ञात करना गणनात्मक रूप से अत्यंत कठिन माना जाता है, यहाँ तक कि क्वांटम कंप्यूटर के लिए भी। इसी कारण LWE तथा Ring-LWE आधारित योजनाएँ वर्तमान में सर्वाधिक लोकप्रिय हैं। कोड-आधारित क्रिप्टोग्राफी त्रुटि-सुधार कोडों की कठिन डिकोडिंग समस्या पर आधारित है, जबकि हैश-आधारित डिजिटल हस्ताक्षर योजनाएँ हैश फलनों की टकराव-प्रतिरोधकता पर निर्भर करती हैं, जिसे सामान्य रूप से इस प्रकार व्यक्त किया जा सकता है:

$$H(m1||m2)$$

जहाँ H एक सुरक्षित हैश फलन है और || संयोजन (concatenation) को दर्शाता है। बहुवेरीय बहुपद-आधारित प्रणालियाँ सीमित क्षेत्र (finite field) पर परिभाषित अनेक बहुपद समीकरणों को हल करने की कठिनाई पर आधारित होती हैं।

हाल के वर्षों में पोस्ट-क्वांटम एल्गोरिद्मों के मानकीकरण की दिशा में महत्वपूर्ण प्रगति हुई है, विशेषकर NIST द्वारा संचालित चयन प्रक्रिया के माध्यम से, जिसमें लैटिस-आधारित की-एन्कैप्सुलेशन और हैश-आधारित हस्ताक्षर योजनाओं को प्राथमिकता दी गई है। वर्तमान अनुसंधान का मुख्य

केंद्र बिंदु कुंजी आकार को कम करना, संगणनात्मक दक्षता बढ़ाना, साइड-चैनल आक्रमणों से सुरक्षा सुनिश्चित करना तथा इन एल्गोरिद्यों को TLS, VPN और क्लाउड संचार अवसंरचना में एकीकृत करना है। इस प्रकार, पोस्ट-क्वांटम क्रिप्टोग्राफी को भविष्य के पूर्णतः त्रुटि-सहिष्णु क्वांटम कंप्यूटरों से उत्पन्न संभावित क्रिप्टोग्राफिक खतरों के विरुद्ध एक व्यावहारिक और निकट-भविष्य समाधान के रूप में देखा जा रहा है।

9.प्रायोगिक और तकनीकी चुनौतियाँ

व्यावहारिक क्वांटम कंप्यूटर और क्वांटम क्रिप्टोग्राफी प्रणालियाँ विकसित करने में महत्वपूर्ण भौतिक चुनौतियाँ सामने आती हैं, जैसे कि:

- पर्यावरणीय अंतःक्रियाओं के कारण डीकोहेरेंस (Decoherence)
- क्वांटम शोर और त्रुटि सुधार (Quantum Noise and Error Correction)
- लंबी दूरी पर उलझाव (Entanglement) को बनाए रखना

ये समस्याएँ सीधे क्वांटम अवस्थाओं की नाज़ुकता से उत्पन्न होती हैं और इन्हें पार करना क्वांटम प्रौद्योगिकी के विकास की सबसे बड़ी बाधाओं में से एक है।

आकृति 6: NISQ युग की क्वांटम संगणन संरचना:- यह आकृति NISQ (Noisy Intermediate-Scale Quantum) युग की क्वांटम कंप्यूटिंग संरचना को दर्शाती है। इसमें क्वांटम प्रोसेसर, त्रुटि सुधार तंत्र और पारंपरिक नियंत्रण प्रणाली शामिल हैं। वर्तमान क्वांटम प्रणालियाँ शोर और डिकोहेरेंस से प्रभावित होती हैं, जिससे पूर्ण त्रुटिरहित गणना अभी एक चुनौती बनी हुई है।

इसके विपरीत, त्रुटि-सहिष्णु क्वांटम संगणना (Fault-Tolerant Quantum Computing) क्वांटम त्रुटि-सुधार तकनीकों पर आधारित होती है, जिनकी सहायता से अनेक भौतिक क्यूबिट्स को संयोजित कर एक तार्किक (Logical) क्यूबिट निर्मित किया जाता है। जहाँ NISQ युग की प्रणालियाँ संकर (Hybrid) एल्गोरिद्यों तथा प्रायोगिक प्रदर्शनों के लिए उपयोगी हैं, वहीं RSA जैसी पारंपरिक क्रिप्टोग्राफिक प्रणालियों को शोर के एल्गोरिद्य द्वारा तोड़ने जैसे बड़े पैमाने के क्रिप्टोग्राफिक आक्रमणों के लिए पूर्णतः त्रुटि-सहिष्णु संरचना आवश्यक है। यह अंतर वर्तमान क्वांटम हार्डवेयर और भविष्य की विस्तृत, मापनीय (Scalable) प्रणालियों के बीच विद्यमान तकनीकी अंतर को स्पष्ट रूप से दर्शाता है।

क्वांटम संगणना में किसी एक क्यूबिट की सामान्य अवस्था को गणितीय रूप से इस प्रकार व्यक्त किया जाता है $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$

जहाँ α और β जटिल (complex) प्रायिकता आयाम (probability amplitudes) हैं तथा $|\alpha|2+|\beta|2=1$

यह सामान्यीकरण (Normalization) शर्त को दर्शाता है।

क्वांटम कंप्यूटिंग में सूचना को संग्रहित और संसाधित करने के लिए क्वांटम बिट (qubit) का उपयोग किया जाता है, जो पारंपरिक बिट की तुलना में सुपरपोज़िशन और एंटैंगलमेंट जैसे क्वांटम गुणों के कारण अधिक शक्तिशाली होता है। वर्तमान में क्विबिट्स को कार्यान्वित करने के लिए कई भौतिक तकनीकों का उपयोग किया जा रहा है, जिनमें प्रमुख रूप से सुपरकंडक्टिंग सर्किट (Superconducting Circuits), ट्रैप्ड आयन (Trapped Ions) और फोटोनिक क्वांटम सिस्टम (Photonic Quantum Systems) शामिल हैं। प्रत्येक तकनीक के अपने विशिष्ट लाभ, सीमाएँ और अनुप्रयोग क्षेत्र हैं।

सुपरकंडक्टिंग क्विबिट्स माइक्रोवेव सर्किट और जोसेफसन जंक्शन (Josephson Junction) पर आधारित होते हैं और इन्हें अत्यंत निम्न तापमान (लगभग मिलीकैल्विन) पर संचालित किया जाता है। इनका मुख्य लाभ यह है कि क्वांटम गेट्स को बहुत तेज गति से संचालित किया जा सकता है, जिसके कारण कई आधुनिक क्वांटम कंप्यूटर, जैसे कि IBM और Google के क्वांटम प्रोसेसर, इसी तकनीक का उपयोग करते हैं। दूसरी ओर ट्रैप्ड आयन क्विबिट्स में आयनों को विद्युत-चुंबकीय क्षेत्र के माध्यम से एक वैक्यूम चैंबर में स्थिर रखा जाता है। इस तकनीक का सबसे बड़ा लाभ इसका उच्च कोहेरेंस समय (coherence time) और अत्यधिक सटीक क्वांटम गेट संचालन है, जिससे यह उच्च गुणवत्ता वाले क्वांटम गणनाओं के लिए उपयुक्त मानी जाती है।

इसके अतिरिक्त फोटोनिक क्वांटम सिस्टम में सूचना को प्रकाश कणों (photons) के ध्रुवीकरण (polarization) या फेज़ के माध्यम से एन्कोड किया जाता है। इस तकनीक का सबसे बड़ा लाभ यह है कि फोटॉन लंबी दूरी तक बिना अधिक क्षति के यात्रा कर सकते हैं, जिससे यह क्वांटम संचार और Quantum Key Distribution (QKD) के लिए अत्यंत उपयोगी सिद्ध होती है। हालांकि प्रत्येक तकनीक में कुछ चुनौतियाँ भी मौजूद हैं, जैसे कि स्केलेबिलिटी, त्रुटि-सुधार और स्थिरता। इसलिए वर्तमान शोध का मुख्य उद्देश्य ऐसी क्वांटम हार्डवेयर तकनीक विकसित करना है जो अधिक स्थिर, त्रुटि-प्रतिरोधी और बड़े पैमाने पर स्केलेबल हो, ताकि भविष्य में व्यावहारिक और शक्तिशाली क्वांटम कंप्यूटर बनाए जा सकें।

10.भविष्य की संभावनाएँ

क्वांटम कंप्यूटिंग के तीव्र विकास से क्रिप्टोग्राफी और सुरक्षित संचार की दुनिया में मौलिक परिवर्तन आने की भविष्यवाणी की जा रही है। जैसे-जैसे वृहद-स्तरीय क्वांटम कंप्यूटर अधिक वास्तविक होते जा रहे हैं, संगणनात्मक कठिनता पर आधारित पारंपरिक एन्क्रिप्शन सिस्टम सुरक्षा खतरों का सामना करेंगे। इसी कारण, वैश्विक स्तर पर क्वांटम-सुरक्षित प्रौद्योगिकी की ओर रुझान बढ़ा है, जिसमें क्वांटम क्रिप्टोग्राफी और पोस्ट-क्वांटम क्रिप्टोग्राफिक विधियाँ शामिल हैं। ये दृष्टिकोण क्वांटम हमलावरों की उपस्थिति में दीर्घकालिक सुरक्षा सुनिश्चित करने के लिए विकसित किए गए हैं।

विशेष रूप से, क्वांटम क्रिप्टोग्राफी, और विशेषकर क्वांटम कुंजी वितरण (QKD), भविष्य की संचार संरचनाओं में महत्वपूर्ण भूमिका निभाने की संभावना रखती है। क्वांटम रिपीटर्स, सैटेलाइट-आधारित क्वांटम संचार, और एकीकृत फोटोनिक सिस्टम में चल रही शोध दूरियों, शोर और डीकोहेरेंस जैसी वर्तमान सीमाओं को पार करने का लक्ष्य रखती है। इसी समय, प्रायोगिक

क्वांटम भौतिकी में प्रगति, जैसे कि तेज़ कोहेरेंस समय और अधिक दोष-रोधी क्वांटम संरचनाएँ, क्वांटम संगणना की शक्ति और क्वांटम-सुरक्षित प्रोटोकॉल की प्रभावशीलता दोनों पर प्रभाव डालेगी।

दीर्घकाल में, क्वांटम भौतिकी, कंप्यूटर और एन्क्रिप्शन के संगम से सूचना सुरक्षा की अवधारणा पूरी तरह बदल जाएगी। सुरक्षा मॉडल केवल गणितीय मान्यताओं पर नहीं, बल्कि भौतिक नियमों पर आधारित होंगे, जो क्वांटम युग में भौतिकी-आधारित सुरक्षा की दिशा में एक मौलिक परिवर्तन को दर्शाता है।

11.निष्कर्ष

क्वांटम कंप्यूटिंग संगणना में एक मौलिक क्रांति का प्रतिनिधित्व करती है, जो क्वांटम भौतिकी के सिद्धांतों द्वारा प्रेरित है। इसका उद्भव उन पारंपरिक क्रिप्टोग्राफिक प्रणालियों के लिए गंभीर चुनौतियाँ प्रस्तुत करता है, जो संगणनात्मक कठिनता पर आधारित हैं। वहीं, क्वांटम भौतिकी सुरक्षा प्रदान करने के लिए क्वांटम एन्क्रिप्शन के रूप में शक्तिशाली समाधान भी प्रदान करती है, जो गणितीय जटिलता के बजाय प्राकृतिक सिद्धांतों पर आधारित है। क्वांटम कुंजी वितरण (Quantum Key Distribution – QKD) जैसे प्रोटोकॉल यह दर्शाते हैं कि अध्यारोपण (superposition), मापन-प्रेरित व्यवधान (measurement disturbance), और नो-क्लोनिंग प्रमेय (no-cloning theorem) जैसी भौतिक घटनाओं का उपयोग करके सुरक्षित संचार स्थापित किया जा सकता है।

भौतिकी, क्वांटम कंप्यूटिंग और क्रिप्टोग्राफी के बीच घनिष्ठ संबंध भौतिकी-आधारित सुरक्षा ढाँचों की ओर एक बदलाव का संकेत देता है। जैसे-जैसे क्वांटम तकनीकें विकसित होंगी, सुरक्षित संचार का भविष्य क्वांटम-प्रतिरोधी क्रिप्टोग्राफिक एल्गोरिदम को व्यावहारिक क्वांटम संचार प्रणालियों में एकीकृत करने पर निर्भर करेगा। अतः, क्वांटम क्रिप्टोग्राफी केवल तकनीकी सुधार नहीं है; यह एक प्रतिमान परिवर्तन है, जो क्वांटम युग में सूचना सुरक्षा की परिभाषा को पुनः निर्धारित करता है।

संदर्भ ग्रंथ सूची (Bibliography/References)

1. Deutsch, D. (1985). Quantum theory, the Church–Turing principle and the universal quantum computer. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 400(1818), 97-117. https://doi.org/10.1098/rspa.1985.0070
2. Feynman, R. P. (2018). Simulating physics with computers. In Feynman and computation (pp. 133-153). cRc Press.
3. Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). Ieee. https://doi.org/10.1109/SFCS.1994.365700
4. Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 212-219). https://dl.acm.org/doi/10.1145/237814.237866
5. Nielsen, M. A., & Chuang, I. L. (2010). Quantum computation and quantum information. Cambridge university press.
6. Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. Theoretical computer science, 560, 7-11. https://doi.org/10.1016/j.tcs.2014.05.025