पोस्ट-क्वांटम क्रिप्टोग्राफी

प्रिलिम्स के लिये:

पोस्ट-क्वांटम क्रिप्टोग्राफी, क्वांटम कंप्यूटिंग, रिविस्ट-शमीर-एडलमैन, ECC एलिप्टिक कर्व क्रिप्टोग्राफी, डिफी-हेलमैन, क्वांटम बिट्स

मेन्स के लिये :

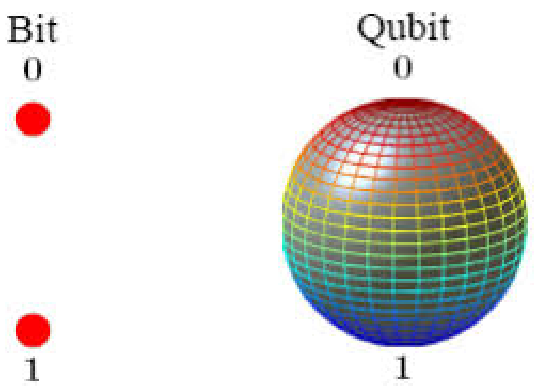
पोस्ट-क्वांटम क्रिप्टोग्राफी, संबंधित चुनौतियाँ और आगे की राह

चर्चा में क्यों?

कंप्यूटिंग ने बैंकिंग से लेकर युद्ध क्षेत्र तक मानव सभ्यता के विभिन्न पहलुओं को परिवर्तित कर दिया हैक्वांटम कंप्यूटिंग के उद्गम ने **भविष्य में कंप्यूटर सुरक्षा** पर इसके प्रभाव के बारे में चिंताएँ बढ़ा दी हैं।

क्वांटम कंप्यूटिंग:

- **परिचय:**
  - क्वांटम कंप्यूटिंग ***एक तेज़ी से उभरती हुई तकनीक है*** जो पारंपरिक कंप्यूटरों की तुलना में बहुत जटिल समस्याओं को हल करने हेतु **क्वांटम यांत्रिकी के नियमों का** उपयोग करती है।
  - क्वांटम यांत्रिकी **भौतिकी की उपशाखा है जो क्वांटम के व्यवहार का वर्णन करती है जैसे** - परमाणु, इलेक्ट्रॉन, फोटॉन और आणविक एवं उप-आणविक क्षेत्र।
  - यह अवसरों से परिपूर्ण नई तकनीक है जो हमें विभिन्न संभावनाएँ प्रदान करके **भविष्य में हमारी दुनिया को आकार देगी।**
  - यह वर्तमान के पारंपरिक कंप्यूटिंग प्रणालियों की तुलना में सूचना को मौलिक रूप से संसाधित करने का एक अलग तरीका है।
- **विशेषताएँ:**
  - जबकि वर्तमान में पारंपरिक कंप्यूटर **बाइनरी 0 और 1 स्थिति** के रूप में जानकारी संग्रहीत करते हैं, क्वांटम कंप्यूटर **क्वांटम बिट्स (क्यूबिट्स/Qubits)** का उपयोग करके गणना करने के लिये प्रकृति के मौलिक नियमों का उपयोग करते हैं।
  - एक बिट के विपरीत एक **क्यूबिट**, जिसे **0 या 1** होना चाहिये, राज्यों के संयोजन में हो सकता है जो तेज़ी से **बड़ी गणनाओं की अनुमति देता है तथा उन्हें जटिल समस्याओं को हल करने की क्षमता प्रदान करता है** जिसमें सबसे शक्तिशाली पारंपरिक सुपर कंप्यूटर भी सक्षम नहीं हैं।



- **महत्त्व:**
  - क्वांटम कंप्यूटर जानकारी में हेर-फेर करने के लिये **क्वांटम मैकेनिकल घटना (Quantum Mechanical Phenomenon)** का उपयोग कर सकते हैं और उनसे आणविक तथा रासायनिक अंत:क्रिया की प्रक्रियाओं **पर प्रकाश डालने,** जटिल समस्याओं का अनुकूल

समाधान करने तथा कृत्रिम बुद्धिमत्ता की क्षमता को बढ़ावा देने **की अपेक्षा** की जाती है।
  - ये नई वैज्ञानिक खोजों, जीवन रक्षक औषधियों एवं **आपूर्ति शृंखलाओं**, लॉजिस्टिक्स और वित्तीय डेटा के मॉडलिंग **में प्रगति** का मार्ग प्रशस्त कर सकते हैं।

क्वांटम कंप्यूटिंग की पोस्ट क्वांटम चिंताएँ:

- **वर्तमान सुरक्षा तकनीकों में कमज़ोरियाँ:**
  - वर्तमान सुरक्षा उपाय, जैसे कि **RSA (रिविस्ट-शमीर-एडलमैन/ Rivest- Shamir- Adleman), ECC (एलिप्टिक कर्व्स क्रिप्टोग्राफी/Elliptic Curves Cryptography)** और डिफी-हेलमैन की एक्सचेंज (Diffie-Hellman Key Exchange), "कठिन" गणितीय समस्याओं पर निर्भर करते हैं जिनका समाधान **शोर के क्वांटम एल्गोरिदम (Shor's Quantum Algorithm)** द्वारा किया जा सकता है।
    - वर्ष 1994 में **पीटर शोर** ने एक **क्वांटम एल्गोरिदम** विकसित किया जो (कुछ संशोधनों के साथ) इन सभी सुरक्षा उपायों का आसानी से समाधान कर सकता है।
  - क्वांटम कंप्यूटिंग में विकास के साथ ही मौजूदा सुरक्षा उपाय **कमज़ोर होते जाएंगे, जिससे वैकल्पिक तकनीकों की खोज की आवश्यकता** होगी।

नोट:

- RSA **एक व्यापक रूप से उपयोग किया जाने वाला क्रिप्टोग्राफिक एल्गोरिदम है और आधुनिक कंप्यूटर** सुरक्षा के मूलभूत निर्माण खंडों में से एक है। **RSA** का उपयोग मुख्य रूप से सुरक्षित संचार तथा डेटा एन्क्रिप्शन के लिये किया जाता है, जो विभिन्न अनुप्रयोगों में गोपनीयता एवं प्रमाणीकरण प्रदान करता है।
- **एलिप्टिक कर्व क्रिप्टोग्राफी (ECC)** एक आधुनिक और व्यापक रूप से उपयोग की जाने वाली क्रिप्टोग्राफिक तकनीक है जो विभिन्न **कंप्यूटर सुरक्षा अनुप्रयोगों के लिये सुरक्षा तथा दक्षता** प्रदान करती है।
- **डिफी-हेलमैन (DH)** एक कुंजी विनिमय एल्गोरिदम है जिसका उपयोग एक असुरक्षित चैनल पर दो पक्षों के बीच एक **शेयर्ड सीक्रेट की** (**Shared Secret Key) स्थापित** करने के लिये किया जाता है। इसे वर्ष 1976 में **व्हिटफील्ड डिफी (Whitfield Diffie)** और मार्टिन हेलमैन द्वारा पेश किया गया था तथा इसे आधुनिक **पब्लिक की** (**Public-Key)** क्रिप्टोग्राफी के मूलभूत निर्माण खंडों में से एक माना जाता है।

- **मापनीयता और व्यावहारिकता:**
  - विशेष हार्डवेयर की आवश्यकता और सख्त पर्यावरणीय बाधाओं के कारण क्वांटम क्रिप्टोग्राफी सिस्टम को **बड़े नेटवर्क पर लागू करना एवं मापना चुनौतीपूर्ण** हो सकता है।
- **लंबी दूरी पर क्वांटम की (Key) वितरण:**
  - क्वांटम की डिस्ट्रीब्यूशन (Quantum Key Distribution) जैसी क्वांटम क्रिप्टोग्राफी प्रणालियों को **उस दूरी के संदर्भ में सीमाओं का सामना** करना पड़ता है जिस पर सिक्योरिटी की (Security keys) वितरित की जा सकती हैं। **क्वांटम क्रिप्टोग्राफी शोधकर्त्ताओं** के लिये इन Keys के वितरण की सीमा का विस्तार एक महत्त्वपूर्ण चुनौती है।
- **क्वांटम नेटवर्क अवसंरचना/बुनियादी ढाँचा:**
  - क्वांटम क्रिप्टोग्राफी के विकास के लिये एक मज़बूत क्वांटम नेटवर्क बुनियादी ढाँचे का निर्माण करना एक **जटिल कार्य** है।
  - इसमें क्वांटम सूचना के सुरक्षित प्रसारण को सुनिश्चित करने के लिये अन्य घटकों के बीच विश्वसनीय **क्वांटम रिपीटर्स, क्वांटम राउटर और क्वांटम मेमोरी** का विकास करना शामिल है।
- **हाइब्रिड विश्व में क्वांटम क्रिप्टोग्राफी:**
  - हाइब्रिड संचार परिदृश्य, **जिसमें क्वांटम और पारंपरिक संचार प्रणालियाँ सह-अस्तित्व में हैं,** पोस्ट-क्वांटम क्रिप्टोग्राफी अधिक प्रचलित होने के साथ ही विकसित होने लगेंगी।
  - इन प्रणालियों के बीच निर्बाध एकीकरण और सुरक्षित संचार सुनिश्चित करना एक चुनौती है।

आगे की राह

- पोस्ट-क्वांटम क्रिप्टोग्राफी में क्वांटम हमलों के प्रति कमज़ोरियों का मुकाबला करने के लिये **वैकल्पिक क्रिप्टोग्राफिक तकनीकों पर शोध** किया जाता है।
- संभावित रूप से भविष्य की क्वांटम खामियों का फायदा उठाने के लिये संदेशों को रिकॉर्ड करने वाले हमलावरों के कारण इस क्षेत्र का महत्त्व और अधिक बढ़ गया है।
- चूँकि व्यावहारिक और खतरनाक क्वांटम कंप्यूटर का विकास अभी दशकों दूर है, **क्वांटम भविष्य के लिये तैयार रहना अभी से ही आवश्यक है।** संवेदनशील डेटा और डिजिटल बुनियादी ढाँचे की सुरक्षा के लिये सरकारों, संगठनों तथा व्यक्तियों को पहले से ही क्वांटम हमलों के खिलाफ सुरक्षित प्रौद्योगिकियों के विकास पर कार्य करना चाहिये।
- पोस्ट-क्वांटम क्रिप्टोग्राफी के क्षेत्र में तेज़ी से विकास हो रहा है, जिसके लिये क्वांटम हमलों का सामना करने में सक्षम **ठोस सुरक्षा उपायों को विकसित करने के लिये निरंतर अनुसंधान और सहयोगात्मक प्रयासों की आवश्यकता है** । क्वांटम युग में डेटा को सुरक्षित रखने तथा डिजिटल बुनियादी ढाँचे की अखंडता को बनाए रखने हेतु **क्वांटम-सुरक्षित प्रौद्योगिकियों के लिये एक सक्रिय एवं सावधानी पूर्वक नियोजित संक्रमण काफी महत्त्वपूर्ण** होगा।

स्रोत: द हिंदू

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/post-quantum-cryptography