पोस्ट-क्वांटम क्रिप्टोग्राफी

प्रिलिम्स के लिये:

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

मेन्स के लिये :

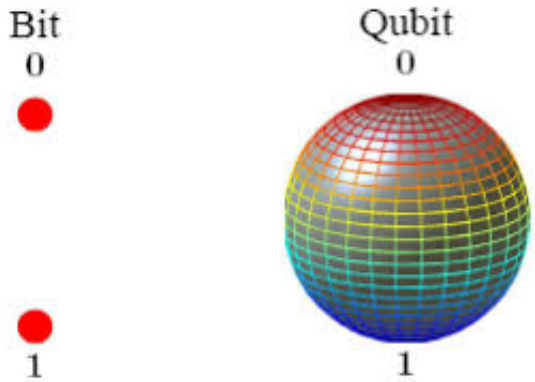
पोस्ट-क्वांटम क्रिप्टोग्राफी, संबंधित चुनौतियाँ और आगे की राह

चर्चा में क्यों?

कंप्यूटिंग ने बैंकिंग से लेकर युद्ध क्षेत्र तक मानव सभ्यता के विभिन्न पहलुओं को परिवर्तित कर दिया है। **क्वांटम 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 आणवकि तथा रासायनकि अंत:क्रयिा की प्रक्रयिाओं **पर प्रकाश डालने,** जटलि समस्याओं का अनुकूल समाधान करने तथा कृत्रमि बुद्धमित्ता की क्षमता को बढ़ावा देने **की अपेक्षा** की जाती है।
- ये नई वैज्ञानकि खोजों, जीवन रक्षक औषधयिों एवं **आपूर्त शृंखलाओं**, लॉजस्टिक्स और वत्तिीय डेटा के मॉडलगि **में प्रगत** का मार्ग प्रशस्त कर सकते हैं।

क्वांटम कंप्यूटगि की पोस्ट क्वांटम चतिाएँ:

- **वर्तमान सुरक्षा तकनीकों में कमज़ोरयिाँ:**
  - वर्तमान सुरक्षा उपाय, जैसे कि **RSA (रविस्ट-शमीर-एडलमैन/ Rivest- Shamir- Adleman), ECC (एलप्टिकि कर्व्स क्रप्टिोग्राफी/Elliptic Curves Cryptography)** और डफी-हेलमैन की एक्सचेंज (Diffie-Hellman Key Exchange), "कठनि" गणतिीय समस्याओं पर नर्भिर करते हैं जनिका समाधान **शोर के क्वांटम एल्गोरदिम (Shor's Quantum Algorithm)** द्वारा कयिा जा सकता है।
    - वर्ष 1994 में **पीटर शोर** ने एक **क्वांटम एल्गोरदिम** वकिसति कयिा जो (कुछ संशोधनों के साथ) इन सभी सुरक्षा उपायों का आसानी से समाधान कर सकता है।
  - क्वांटम कंप्यूटगि में वकिास के साथ ही मौजूदा सुरक्षा उपाय **कमज़ोर होते जाएंगे, जसिसे वैकल्पकि तकनीकों की खोज की आवश्यकता** होगी।

नोट:

- RSA **एक व्यापक रूप से उपयोग कयिा जाने वाला क्रप्टिोग्राफकि एल्गोरदिम है और आधुनकि कंप्यूटर** सुरक्षा के मूलभूत नर्मिाण खंडों में से एक है। **RSA** का उपयोग मुख्य रूप से सुरक्षति संचार तथा डेटा एन्क्रप्शिन के लयि कयिा जाता है, जो वभिन्नि अनुप्रयोगों में गोपनीयता एवं प्रमाणीकरण प्रदान करता है।
- **एलप्टिकि कर्व क्रप्टिोग्राफी (ECC)** एक आधुनकि और व्यापक रूप से उपयोग की जाने वाली क्रप्टिोग्राफकि तकनीक है जो वभिन्नि **कंप्यूटर सुरक्षा अनुप्रयोगों के लयि सुरक्षा तथा दक्षता** प्रदान करती है।
- **डफी-हेलमैन (DH)** एक कुंजी वनिमिय एल्गोरदिम है जसिका उपयोग एक असुरक्षति चैनल पर दो पक्षों के बीच एक **शेयर्ड सीक्रेट की** (**Shared Secret Key) स्थापति** करने के लयि कयिा जाता है। इसे वर्ष 1976 में **व्हटिफील्ड डफी (Whitfield Diffie)** और मार्टनि हेलमैन द्वारा पेश कयिा गया था तथा इसे आधुनकि **पब्लकि की** (**Public-Key)** क्रप्टिोग्राफी के मूलभूत नर्मिाण खंडों में से एक माना जाता है।

- **मापनीयता और व्यावहारकिता:**
  - वशिष हार्डवेयर की आवश्यकता और सख्त पर्यावरणीय बाधाओं के कारण क्वांटम क्रप्टिोग्राफी सस्टिम को **बड़े नेटवर्क पर लागू करना एवं मापना चुनौतीपूर्ण** हो सकता है।
- **लंबी दूरी पर क्वांटम की (Key) वतिरण:**
  - क्वांटम की डस्ट्रिीब्यूशन (Quantum Key Distribution) जैसी क्वांटम क्रप्टिोग्राफी प्रणालयिों को **उस दूरी के संदर्भ में सीमाओं का सामना** करना पड़ता है जसि पर सक्योरटिी की (Security keys) वतिरति की जा सकती हैं। **क्वांटम क्रप्टिोग्राफी शोधकर्त्ताओं** के लयि इन Keys के वतिरण की सीमा का वस्तिार एक महत्त्वपूर्ण चुनौती है।
- **क्वांटम नेटवर्क अवसंरचना/बुनयिादी ढाँचा:**
  - क्वांटम क्रप्टिोग्राफी के वकिास के लयि एक मज़बूत क्वांटम नेटवर्क बुनयिादी ढाँचे का नर्मिाण करना एक **जटलि कार्य** है।
  - इसमें क्वांटम सूचना के सुरक्षति प्रसारण को सुनश्चिति करने के लयि अन्य घटकों के बीच वश्विसनीय **क्वांटम रपिीटर्स, क्वांटम राउटर और क्वांटम मेमोरी** का वकिास करना शामलि है।
- **हाइब्रडि वशि्व में क्वांटम क्रप्टिोग्राफी:**
  - हाइब्रडि संचार परदृिश्य, **जसिमें क्वांटम और पारंपरकि संचार प्रणालयिाँ सह-अस्तत्वि में हैं,** पोस्ट-क्वांटम क्रप्टिोग्राफी अधकि प्रचलति होने के साथ ही वकिसति होने लगेंगी।
  - इन प्रणालयिों के बीच नर्बिाध एकीकरण और सुरक्षति संचार सुनश्चिति करना एक चुनौती है।

आगे की राह

- पोस्ट-क्वांटम क्रप्टिोग्राफी में क्वांटम हमलों के प्रतकिमज़ोरयिों का मुकाबला करने के लयि **वैकल्पकि क्रप्टिोग्राफकि तकनीकों पर शोध** कयिा जाता है।
- संभावति रूप से भवष्यि की क्वांटम खामयिों का फायदा उठाने के लयि संदेशों को रकिॉर्ड करने वाले हमलावरों के कारण इस क्षेत्र का महत्त्व और अधकि बढ़ गया है।
- चूँकि व्यावहारकि और खतरनाक क्वांटम कंप्यूटर का वकिास अभी दशकों दूर है, **क्वांटम भवष्यि के लयि तैयार रहना अभी से ही आवश्यक है।** संवेदनशील डेटा और डजिटिल बुनयिादी ढाँचे की सुरक्षा के लयि सरकारों, संगठनों तथा व्यक्तयिों को पहले से ही क्वांटम हमलों के खलिाफ सुरक्षति प्रौद्योगकियिों के वकिास पर कार्य करना चाहयि।
- पोस्ट-क्वांटम क्रप्टिोग्राफी के क्षेत्र में तेज़ी से वकिास हो रहा है, जसिके लयि क्वांटम हमलों का सामना करने में सक्षम **ठोस सुरक्षा उपायों को वकिसति करने के लयि नरिंतर अनुसंधान और सहयोगात्मक प्रयासों की आवश्यकता है** । क्वांटम युग में डेटा को सुरक्षति रखने तथा डजिटिल बुनयिादी ढाँचे की अखंडता को बनाए रखने हेतु **क्वांटम-सुरक्षति प्रौद्योगकियिों के लयि एक सक्रयि एवं सावधानी पूर्वक नयिोजति संक्रमण काफी महत्त्वपूर्ण** होगा।

[स्रोत: द हिंदू](#)