

पोस्ट-क्वांटम एन्क्रिप्शन क्रिप्टोग्राफी

स्रोत: हदुस्तान टाइम्स

वर्चुअल प्राइवेट नेटवर्क (VPN) कंपनियों **पोस्ट-क्वांटम क्रिप्टोग्राफी (PQC)** के कार्यान्वयन के माध्यम से **क्वांटम कंप्यूटिंग** द्वारा उत्पन्न **संभावित खतरों** के अनुकूल बन रही हैं।

- **क्वांटम कंप्यूटिंग** अत्यंत तीव्र गति से गणना करने की अपनी क्षमता के कारण **वर्तमान एन्क्रिप्शन विधियों के लिये कई खतरे** उत्पन्न करती है।
 - **असममति एन्क्रिप्शन का सरलीकरण:** क्वांटम कंप्यूटर जटिल गणितीय समस्याओं जैसे **बड़ी संख्याओं का गुणनखंडन** और असतत लघुगणक को हल कर सकते हैं।
 - इससे **रिविस्ट-शमीर-एडलमैन (RSA)** और **एलिप्टिकल कर्व क्रिप्टोग्राफी (ECC)** जैसी एन्क्रिप्शन विधियों पर असर पड़ सकता है, जिनका व्यापक रूप से सुरक्षा संचार के लिये उपयोग किया जाता है।
 - **स्टोर नाउ, डिक्रिप्ट लेटर (SNDL) अटैक:** साइबर अपराधी **एन्क्रिप्टेड डेटा को तुरंत संग्रहीत कर सकते हैं** और बाद में जब क्वांटम कंप्यूटर पर्याप्त शक्तिशाली हो जाते हैं, तो **उसे डिक्रिप्ट कर सकते हैं**, जिससे संवेदनशील जानकारी खतरे में पड़ सकती है।
 - **उद्योग-व्यापी डेटा सुरक्षा जोखिम:** यदि क्वांटम कंप्यूटर एन्क्रिप्शन मानकों का उल्लंघन करते हैं, तो **वित्त, स्वास्थ्य सेवा और सरकारी संचार** जैसे क्षेत्रों को डेटा उल्लंघन और वित्तीय नुकसान का खतरा हो सकता है।

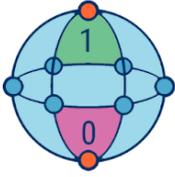
पोस्ट-क्वांटम एन्क्रिप्शन/क्रिप्टोग्राफी (PQC):

- **PQC** उन क्रिप्टोग्राफिक विधियों को संदर्भित करता है जो **क्वांटम कंप्यूटरों** द्वारा आसानी से हल किये जा सकने वाले **गणितीय समस्याओं पर निर्भर नहीं** होते हैं।
- इसे **क्वांटम-रेजिस्टेंस**, **क्वांटम-सेफ** या **क्वांटम-प्रूफ क्रिप्टोग्राफी** के रूप में भी जाना जाता है।
- इन विधियों को **क्लासिकल और क्वांटम कंप्यूटिंग सिस्टम** दोनों के **हमलों के खिलाफ सुरक्षित रहने** के लिये डिज़ाइन किया गया है।
- **VPN** तकनीक **डेटा को एन्क्रिप्ट** करती है और **उपयोगकर्ता के IP एड्रेस** को गुप्त रखती है, ताकि **डेटा की गोपनीयता और सुरक्षा** के लिये **उपकरणों के बीच सुरक्षा संचार सुनिश्चित** किया जा सके।

Quantum Computing

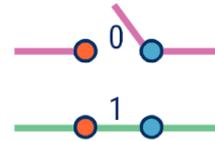
Vs.

Classical Computing



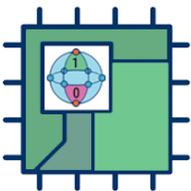
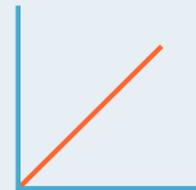
Calculates with qubits, which can represent 0 and 1 at the same time

Calculates with transistors, which can represent either 0 or 1



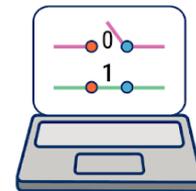
Power increases exponentially in proportion to the number of qubits

Power increases in a 1:1 relationship with the number of transistors



Quantum computers have high error rates and need to be kept ultracold

Classical computers have low error rates and can operate at room temp



Well suited for tasks like optimization problems, data analysis, and simulations

Most everyday processing is best handled by classical computers

