सी-डॉट क्वांटम हैकाथॉन 2023

सीक्यूहैक 2023

सेंटर फॉर डेवलपमेंट ऑफ़ टेलीमैटिक्स (C-DOT), दूरसंचार विभाग, भारत सरकार के अधीन एक प्रमुख दूरसंचार अनुसंधान एवं विकास संगठन है। भारत सरकार, सी-डॉटक्वांटम हैकथॉन 2023 (सीक्यूहैक 2023) में भारत में शिक्षा जगत, उद्योगों, स्टार्ट-अप्स और व्यक्तिगत शोधकर्ताओं के विशेषज्ञों का स्वागत करती है। हैकथॉन का उद्देश्य सी-डॉट द्वारा विकसित क्वांटम सुरक्षा समाधानों में कमजोरियों का पता लगाना और उनका समाधान करना है।

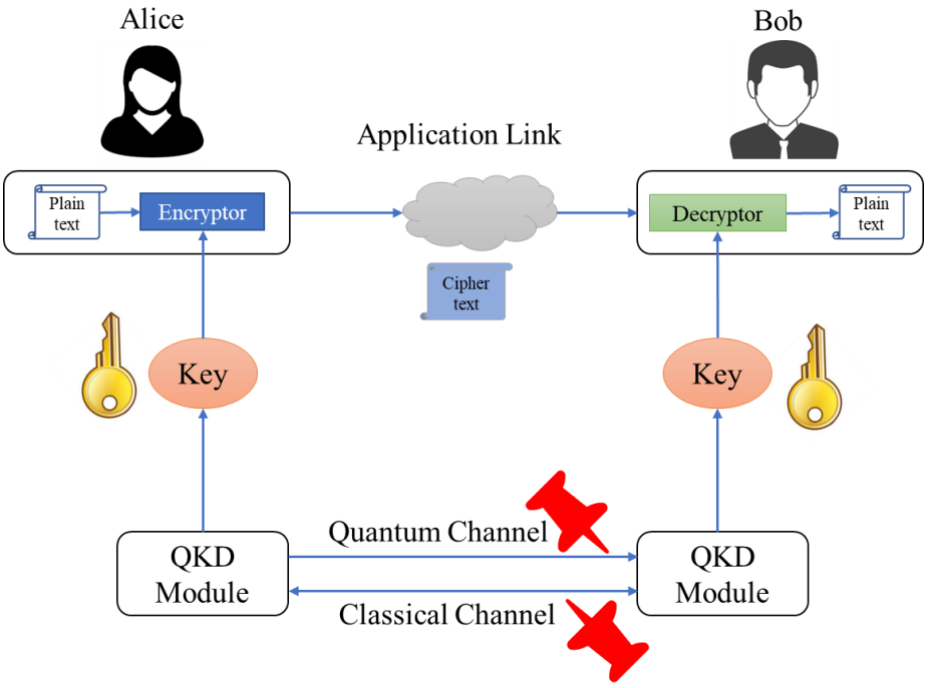
क्वांटम-सुरक्षित समाधान

सी-डॉट ने सुरक्षित संचार के लिए निम्नलिखित दो क्वांटम-सुरक्षित कुंजी विनिमय तंत्र विकसित किए हैं:

1) ऑप्टिकल फाइबर आधारित क्वांटम कुंजी वितरण (क्यूकेडी)
2) पोस्ट-क्वांटम क्रिप्टोग्राफी (पीक्यूसी) आईपी एनक्रिप्टर

1)क्वांटम कुंजी वितरण (क्यूकेडी)

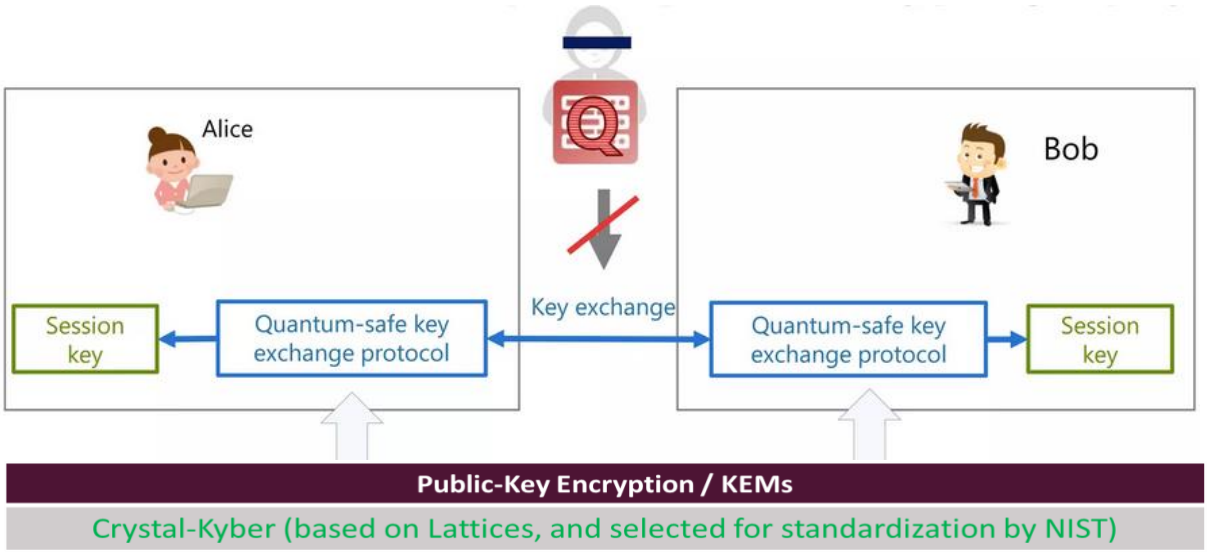
सी-डॉट ने डिफरेंशियल फेज रेफरेंस (डीपीआर) प्रोटोकॉल के आधार पर फाइबर आधारित क्वांटम की डिस्ट्रीब्यूशन (क्यूकेडी) समाधान विकसित किया है। क्यूकेडी समाधान में दो नोड होते हैं, जिन्हें परंपरागत रूप से ऐलिस और बॉब कहा जाता है। ऐलिस एक ट्रांसमीटर के रूप में और बॉब एक रिसीवर के रूप में कार्य करता है। ऐलिस और बॉब एक यूनिडायरेक्शनल क्वांटम चैनल और एक प्रमाणित शास्त्रीय चैनल के माध्यम से जुड़े हुए हैं। सिस्टम का ब्लॉक आरेख चित्र 1 में दिखाया गया है। क्यूकेडी मॉड्यूल विश्वसनीय नोड्स हैं और इन नोड्स तक केवल पहुंच (ईव्सड्रॉपिंग के लिए) क्वांटम चैनल और शास्त्रीय चैनल के फाइबर के माध्यम से हो सकती है जैसा कि लाल पिन के माध्यम से दिखाया गया है। चित्र 1 में दिखाए गए सेट-अप में, क्वांटम चैनल और क्लासिकल, चैनल दोनों अलग-अलग डार्क फाइबर का उपयोग करते हैं ।



चित्र 1: सी-डॉट क्यूकेडी सिस्टम

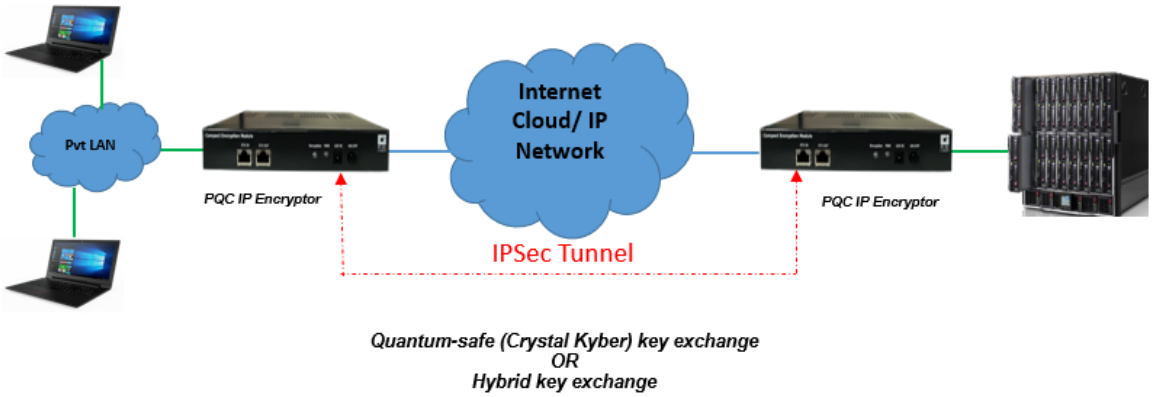
2) पोस्ट-क्वांटम क्रिप्टोग्राफी (पीक्यूसी) आईपी एनक्रिप्टर

सी-डॉट के स्वदेशी रूप से विकसित पीक्यूसी आईपी एनक्रिप्टर को कॉम्पैक्ट एनक्रिप्शन मॉड्यूल (सीईएम) नाम दिया गया है /*क्रिस्टल- काइबर योजना* पर आधारित है जो क्वांटम कंप्यूटर-आधारित हमलों के लिए प्रतिरोधी है। क्रिस्टल- किबर NIST की पीक्यूसी मानकीकरण प्रक्रिया के फाइनलिस्ट में से एक है, जिसे मानकीकरण के लिए चुना गया। यह मॉड्यूल-जाली पर परिभाषित लर्निंग-विथ-एरर्स (एलडब्ल्यूई) समस्या की कठोरता पर निर्भर करता है। पोस्ट-क्वांटम कुंजी विनिमय का ब्लॉक आरेख चित्र 2 में दर्शाया गया है।



चित्र 2: पोस्ट-क्वांटम कुंजी एनकैप्सुलेशन तंत्र (PQ-KEM)

कॉम्पैक्ट एन्क्रिप्शन मॉड्यूल (*सीईएम*) एईएस-256 एन्क्रिप्शन / डिक्रिप्शन का समर्थन करता है और क्वांटम हमलों के खिलाफ किसी भी दो भौगोलिक साइटों / महत्वपूर्ण बुनियादी ढांचे के उपकरणों की सुरक्षा के लिए इस्तेमाल किया जा सकता है। नीचे चित्र 3 क्लाइंट-सर्वर अनुप्रयोगों के लिए पीक्यूसी आईपी एन्क्रिप्टर समाधान के एक विशिष्ट परिनियोजन परिदृश्य को दर्शाता है।



चित्र 3: क्लाइंट-सर्वर अनुप्रयोगों के लिए कुंजी विनिमय और डेटा एनकैप्सुलेशन परिदृश्य

उद्देश्य

सीक्यूहैक 2023 का उद्देश्य कई विषयों के लोगों को अपने हार्डवेयर और/या सॉफ्टवेयर समाधानों का परीक्षण करने के लिए एक साथ आने के लिए आमंत्रित करना है-

1. वास्तविक समय के आधार पर क्यूकेडी सिस्टम द्वारा उत्पन्न की जा रही चाबियों के सेट से 256-बिट (या अधिक) कुंजी निकालने के लिए लाइव क्यूकेडी सिस्टम पर।
2. पीक्यूसी IP एन्क्रिप्टर के एक लाइव सत्र पर पीक्यूसी एन्क्रिप्टर द्वारा वास्तविक समय के आधार पर उत्पन्न की जा रही कुंजियों के सेट से 256-बिट (या अधिक) कुंजी निकालने के लिए।

कौन आवेदन कर सकता है?

सीक्यूहैक 2023 केवल भारतीय नागरिकों के लिए खुला है। इस हैकथॉन में शिक्षा जगत, उद्योगों, स्टार्ट-अप्स और संबंधित क्षेत्रों में विशेषज्ञता रखने वाले व्यक्तिगत शोधकर्ता भाग ले सकते हैं। प्रतिभागियों को अपने प्रासंगिक अनुभव, विस्तृत सीवी, और वैकल्पिक रूप से, सिस्टम (क्यूकेडी/पीक्यूसी/दोनों) को तोड़ने के लिए अपनी रणनीति की व्याख्या करते हुए एक संक्षिप्त लेख साझा करने की आवश्यकता है। प्रतिभागियों के चयन के संबंध में सी-डॉट का निर्णय अंतिम और बाध्यकारी होगा।

आवेदन कैसे करें?

आवेदक सहायक दस्तावेजों के साथ अपने आवेदन श्री रविंदर अंबरदार, प्रमुख-मार्केटिंग को ईमेल कर सकते हैं , सी-डॉट, दिल्ली (ईमेल: cquhack@cdot.in)। हैकाथॉन में प्रवेश नि:शुल्क है।

समय सारणी:

लाइव सिस्टम को पारस्परिक रूप से सहमत समय सारणी के अनुसार उपलब्ध कराया जाएगा। क्यूकेडी के मामले में केवल क्वांटम चैनल के साथ-साथ क्लासिकल चैनल फाइबर और पीक्यूसी के मामले में ईथरनेट लिंक तक पहुंच प्रदान की जाएगी। क्यूकेडी सिस्टम या पीक्यूसी आईपी एन्क्रिप्टरके लिए कोई भौतिक पहुँच प्रदान नहीं की जाएगी। कोई भी प्रयोग दिल्ली में सी-डॉट परिसर में करना होगा। समय-सीमा के विस्तार के लिए किसी भी अनुरोध की स्वीकृति सी-डॉट के पूर्ण विवेकाधिकार पर होगी।

अस्वीकरण:

क्यूकेडी सिस्टम या पीक्यूसी आईपी एनक्रिप्टर तक पहुंच केवल ऊपर दिखाए गए संबंधित एक्सेस पॉइंट्स के माध्यम से होगी (चित्र 1 और चित्र 3)। सिस्टम में किसी भौतिक पहुंच की अनुमति नहीं दी जाएगी। सिस्टम के आंतरिक हार्डवेयर और सॉफ्टवेयर विवरण भी गोपनीय रहेंगे। सिस्टम को हैक करने का प्रतिभागियों का दावा तभी मान्य होगा जब सिस्टम के प्रदर्शन या इसके संचालन के लिए किसी भी पता लगाने योग्य विसंगति को पेश किए बिना कुंजियों तक पहुँचा जा सकता है। प्रतिभागी कोई ऐसा प्रयोग भी नहीं कर सकते हैं जिससे सिस्टम के किसी हिस्से या पूरे सिस्टम को स्थायी नुकसान हो।

सिस्टम में सफल भेदन के मामले में, प्रतिभागियों को क्यूकेडी और पीक्यूसी सिस्टम प्रत्येक के लिए 10 लाख रुपये का पुरस्कार और पारस्परिक रूप से सहमत शर्तों पर क्वांटम सुरक्षा के क्षेत्र में सी-डॉट के साथ सहयोग करने का अवसर प्रदान किया जाएगा। सफल प्रतिभागियों को सिस्टम की कमियों को सी-डॉट के सामने प्रकट करना भी आवश्यक है ताकि उन्हें दूर किया जा सके। इस संबंध में विकसित कोई भी आईपीआर संबंधित प्रतिभागियों के साथ संयुक्त स्वामित्व में होगा। क्यूकेडी या पीक्यूसी सुरक्षा को भंग करने वाले समाधान तैयार करने के लिए वित्तपोषण की मांग की जाती है, तो प्रस्ताव सी-डॉट के सहयोगात्मक अनुसंधान कार्यक्रम (सीसीआरपी) नीति के अनुरूप प्रस्तुत किए जा सकते हैं।