C-DOT Quantum Hackathon 2023

CQuHACK 2023

Centre for Development of Telematics (C-DOT), a premier telecom R&D organization under the Department of Telecommunication, Govt. of India, welcomes experts from academia, industries, start-ups, and individual researchers in India to C-DOT Quantum Hackathon 2023 (CQuHACK2023). The objective of the Hackathon is to find vulnerabilities in the Quantum Security solutions developed by C-DOT and to address the same.

Quantum-Safe Solutions

C-DOT has developed the following two Quantum-safe key exchange mechanisms for secure communication:

1) Optical fibre-based Quantum Key Distribution (QKD)
2) Post-Quantum Cryptography (PQC) IP Encryptor

1) Quantum Key Distribution (QKD)

C-DOT has developed fibre-based Quantum Key Distribution (QKD) solution based on Differential Phase Reference (DPR) protocols. The QKD solution consists of two nodes, traditionally called Alice and Bob. Alice acts as a transmitter and Bob as a receiver. Alice and Bob are connected through a unidirectional quantum channel and an authenticated classical channel. The block diagram of the system is shown in Figure 1. The QKD modules are trusted nodes and only access (for eavesdropping) to these nodes can be through the fibres of the quantum channel and classical channel as shown through red pins. In the set-up shown in Figure 1, both the quantum channel and classical channel use separate dark fibres.

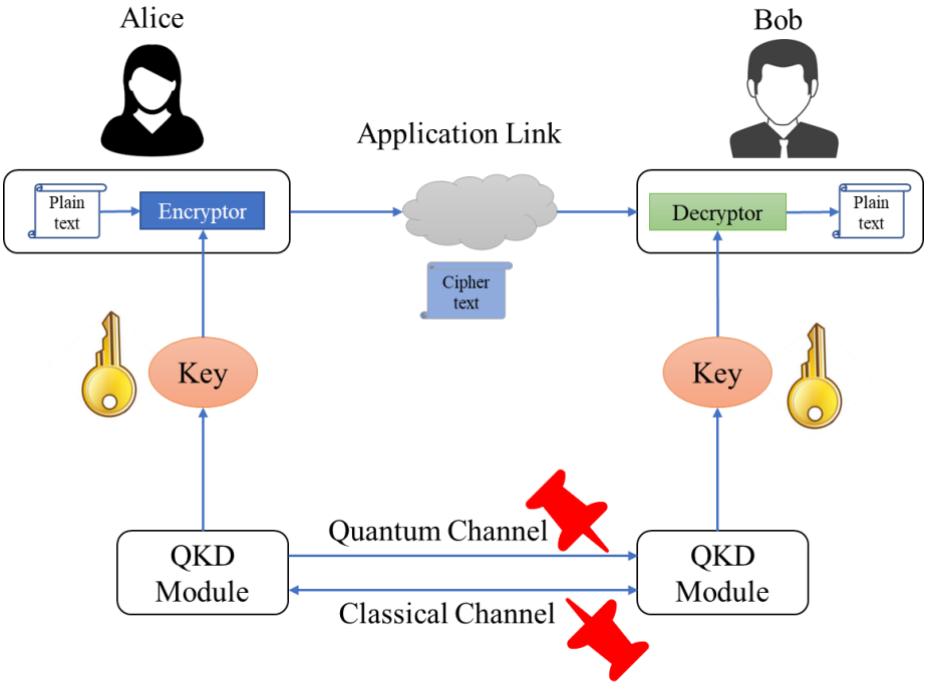

Figure 1: C-DOT QKD System

2) Post-Quantum Cryptography (PQC) IP Encryptor

C-DOT's indigenously developed PQC IP Encryptor is named as Compact Encryption Module (CEM), it is based on *Crystals-Kyber* scheme that is resistant to quantum computer-based attacks. Crystals-Kyber is one of the finalists of NIST's PQC standardization process, which got selected for standardzation. It relies on the hardness of Learning-With-Errors (LWE) problem defined over the module-lattices. The block diagram of Post-Quantum key exchange is depicted in Figure 2.

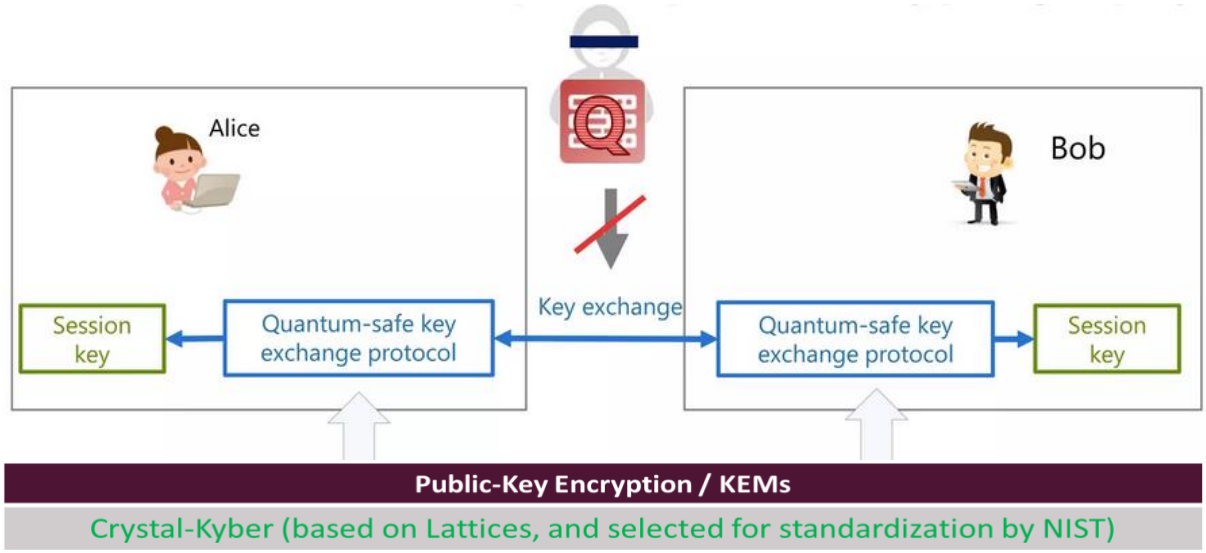

Figure 2: Post-Quantum Key Encapsulation Mechanism (PQ-KEM)

Compact Encryption Module (CEM) supports AES-256 encryption/decryption and can be used to protect any two geographical sites/devices of a critical infrastructure against quantum attacks. Figure 3 below depicts a typical deployment scenario of PQC IP Encryptor solution for client-server applications.

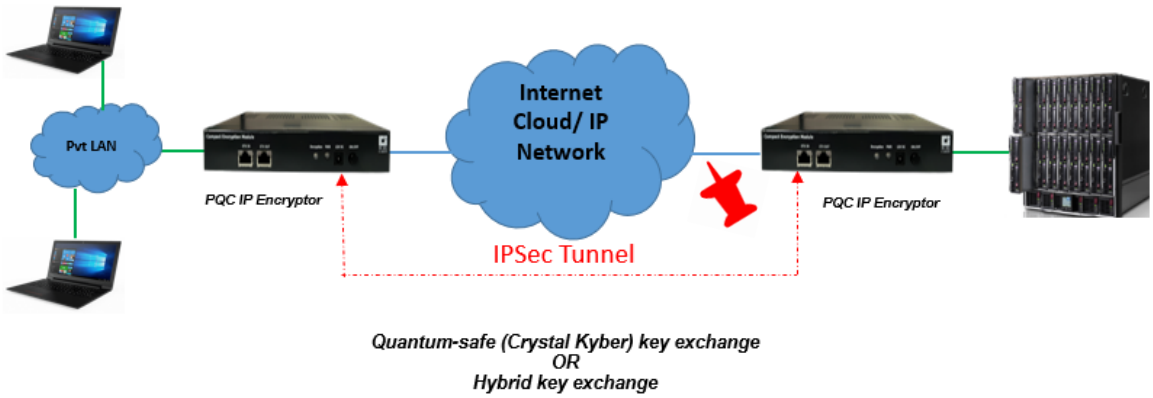

Figure 3: Key Exchange and Data Encapsulation Scenario for Client-Server applications

Aim

The aim of CQuHACK 2023 is to invite people from multiple disciplines to come together to test their hardware and/or software solutions-

1. on a live QKD system to extract a 256-bit (or more) key from the set of keys being generated by the QKD system on a real-time basis.
2. on a live session of PQC IP Encryptors to extract a 256-bit (or more) key from the set of keys being generated by the PQC Encryptors on a real-time basis.

Who can Apply?

CQuHACK 2023 is open only to Indian nationals. People from academia, industries, start-ups, and individual researchers who have expertise in the relevant areas can take part in this hackathon. The participants need to share their relevant experiences, detailed CVs, and optionally, a brief write-up explaining their strategy to break through the system (QKD/PQC/Both). The decision of C-DOT regarding the selection of the participants will be final and binding.

How to Apply?

Applicants can email their applications along with supporting documents to Mr. Ravinder Ambardar, Head-Marketing, C-DOT, Delhi (Email: cquhack@cdot.in). Entry to the hackathon is free-of-cost.

Timeline:

The live system will be made available for a mutually agreed timeline. Access will only be provided to the Quantum Channel as well as Classical Channel fibres in the case of QKD and to the Ethernet links in the case of PQC. No physical access will be provided to the QKD system or PQC IP Encryptor. Applicants specific requirements, if any, for the Hackathon can also be discussed with C-DOT. Any experiment will have to be performed in the C-DOT campus in Delhi. Approval of any request for an extension of the timeline will be at the sole discretion of C-DOT.

Disclaimer:

Access to the QKD system or PQC IP Encryptor will be through the respective access points shown above only (Figure 1 & Figure 3). No physical access will be allowed to the system. Internal hardware and software details of the system will also be confidential. The participants' claim of hacking the system will be valid only if the keys can be accessed without introducing any detectable anomaly to the system's performance or its operation. The participants also cannot perform any experiment that would result in permanent damage to any part of the system or the entire system.

In case of a successful hacking of the system, the participants will be provided with a prize of INR 10 Lakhs, each for the QKD and PQC systems and an opportunity to collaborate with C-DOT in the area of Quantum Security at mutually agreeable terms and conditions. The successful participants are also required to disclose the shortcomings of the system to C-DOT so that they can be addressed. Any IPR developed in this regard will be in joint ownership with the respective participants.

In case funding is sought for creating solutions that can break QKD or PQC security, proposals may be submitted in line with C-DOT's Collaborative Research Program (CCRP) Policy.