Development of Continuous Variable Quantum Key Distribution (CV-QKD)

Introduction:

Public Key Infrastructure (PKI) is mostly used across the globe to secure the Internet and is based on mathematically complex algorithms. The security is based on the assumption that it is virtually impossible, even for the most advanced classical computer, to perform certain mathematical functions like prime factorisation of a very large integer in a reasonable time. However, with the rapid advancements in quantum computing and quantum algorithms, this assumption does not hold very strong. Quantum Key Distribution (QKD) is a method of key exchange that eliminates any probability of eavesdropping. Fundamental rules of quantum mechanics ensure that any case of eavesdropping changes the system irreversibly, and the attempts of eavesdropping get detected.

QKD protocols can be broadly classified into two categories-Discrete Variable (DV) QKD and Continuous Variable (CV) QKD. In the case of DV-QKD, exchanged quantum states are encoded into the polarisation, phase or time bin of the transmitted qubits and the secret key is established upon detection of the individual photons. BB84 protocol, named after Charles Bennett and Gilles Brassard, was the first DV-QKD protocol. Although very popular, the DV-QKD protocol has certain limitations. The major limitation is in the single-photon detectors. Avalanche diode-based single-photon detectors suffer from lower detection efficiency (~30%) and complex control circuitry. Superconducting Nanowire Single Photon Detectors (SNSPDs) are having higher efficiency, but they need cryogenic temperature (~mK) and they are bulky and costly.

After almost 15 years, the first CV-QKD protocol was introduced. There has been an ever-increasing interest in CV-QKD in the research community after the demonstration of continuous variable teleportation in 1998. CV-QKD has several advantages compared to DV-QKD:

- In CV-QKD, both homodyne as well as heterodyne detection are used. The repetition rate of the homodyne detection (≈ 1 GHz) is much higher compared to the avalanche photodiodes with single photon sensitivity (≈ MHz) used in DV-QKD. Homodyne detection offers the largest signal-detection bandwidth for a given balanced-detector bandwidth. Although optical complexity is more in homodyne detection compared to heterodyne detection.
  On the other hand, heterodyne detection has less system complexity as much of the signal processing is done in the electrical domain.
- Homodyne detection is way more efficient than single-photon avalanche detectors, achieving detection efficiencies higher than 90% whereas single-photon detectors currently reach 30%.
- The class of states generally used in continuous variable QKD, the so-called Gaussian states, is easier to generate.
- CV-QKD is deemed to be more resilient to noise when the quantum channel is multiplexed with the classical channel on the same fibre. This makes it an ideal candidate to easily upgrade existing optical networks with quantum security.

- CV-QKD are more cost-effective as the components used are more compatible with existing telecom technologies.

Project Description:

Any QKD protocol consists of two phases. First is the preparation, transmission, and measurement of the quantum states to generate the raw key bits followed by classical post-processing in which the QKD nodes (conventionally called Alice and Bob) perform sifting, error correction, and privacy amplification. Before starting any operation, Alice and Bob must authenticate each other's classical channel communication using a secure mechanism to avoid a man-in-the-middle attack by an eavesdropper, Eve.

Block Diagram:

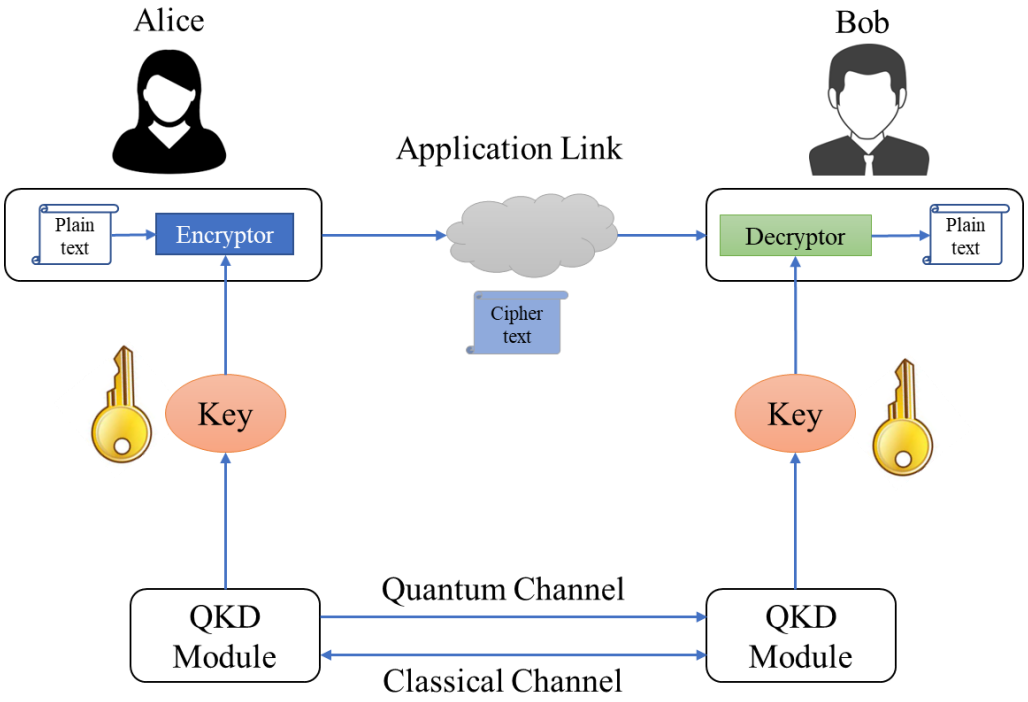

Fig. 1: Block Diagram of CV-QKD System

The project intends to develop QKD modules at Alice and Bob's end. Alice acts as a transmitter and Bob as a detector for the quantum states prepared by Alice. A detailed description of the system is given below.

CV-QKD System Description:

Nodes	• Alice - Transmitter • Bob - Detector
Protocols	• Coherent state CV-QKD • Gaussian modulation • Homodyne/heterodyne detection
Security	• Theoretical security proof of the used protocol • Finite size effects • Security parameter (ε)

Classical Post-processing[1]	• Sifting • Error correction[2] • Privacy amplification[2]
System Configuration Parameters	• Error correction code rate • Privacy amplification compression ratio
System Performance Metric	• Error rate • Supported channel loss (dB) • Secure key rate
System Interfaces	• 1 x 1000BASE-T for management traffic • 1 x SMF28 optical fibre from Alice to Bob (Quantum channel) • SMF28 optical fibre pair between Alice and Bob (Classical channel)
User Interfaces	• Graphical User Interface (GUI) for system configuration and performance visualisation • USB/Ethernet (10/100/10BASE-T) for key delivery as per ETSI standard
Dimension of the System	19” rack-mountable
Power	Single-phase 230 V AC @ 50 Hz

Note:

1. Suitable algorithms should be chosen for each of the post-processing steps.
2. Code rate for error correction algorithms and compression factor in privacy amplification should be configurable to adjust to different loss budget.
3. The final specifications need to be finalized in consultation with C-DOT
4. The collaborating partner(s) should have suitable theoretical and practical experience, appropriately skilled resources and facilities for undertaking development of such solution.
5. The collaborating partner(s) need to share the details of major components used in the design of the solution.
6. The collaborating partner(s) need to prepare a detailed test plan and ensure that the performance of the solution is thoroughly tested for various parameters. The detailed plan and timelines in which few tested unitss can be provided to C-DOT need to be provided in the proposal.
7. Complete details of the developed module need to be shared with C-DOT.