**Non-Linear Code-Based Cryptography**

Code based cryptography is a family of Post quantum cryptography (PQC) which are resilient to various attacks from quantum as well as classical computers. This family of PQC relies on well known hard problems in coding theory to derive their strength. There are two main algorithms - McEliece and Niederreiter systems- from which stems all other major schemes in this family.

There are several existing code based cryptosystems which effectively resists all known attacks. All of them are based on binary linear error correcting codes and their decoding hardness. The use of non-linear codes is yet to be explored. Hence, it is intended to focus on using Non-Linear code based PQC schemes.

The following non-linear code based schemes are to be developed

1. Incorporate Non Linear codes into McEliece Cryptosystem
2. Incorporate Non Linear codes into Niederreiter Cryptosystem

**Gate Level Implementation of Quantum Encryption Algorithm.**

The field of quantum cryptography is extensively growing in this current era. Its strength relies on the principles of laws of quantum physics. The two main areas of quantum cryptography are quantum key distribution (QKD) and quantum encryption algorithms. Using IBM Qiskit simulators written in Python, quantum computing algorithms were implemented at the gate level. We are working to develop a novel quantum encryption technique for quantum computers.

The following schemes are to be developed:

1. Implementation of Quantum Random Number generator (QRNG) using Quantum Fourier Transformation (QFT).
2. Implementation of Quantum Encryption Algorithm.
3. Implementation of Quantum Multi-Party communication system.