# Title: Quantum Cryptography using Quantum Neural Networks

## Introduction

As quantum computing advances, traditional cryptographic methods, like RSA and ECC, faces potential security threats, given that quantum algorithms can solve these methods much faster than classical computers. Quantum cryptography offers a promising solution by using principles of Quantum physics like superposition and entanglement to secure communication. Quantum Key Distribution (QKD) is a widely known method that enables two parties to share a secure key while detecting any eavesdropping attempts(property of Quantum physics i.e. no-cloning theorem ).

Quantum Neural Networks (QNNs), which leverage the power of quantum computing in neural network architectures, present a unique opportunity to enhance cryptographic processes. QNNs are designed to handle quantum data directly, enabling potentially more efficient and robust encryption, decryption, and key distribution protocols.

This project aims to develop a cryptographic protocol using QNNs to secure communication against both classical and quantum threats. By assessing the security and efficiency of QNN-based cryptography, this research will contribute to advancements in quantum-safe encryption, addressing the growing need for secure data transmission in the quantum era.

## Background

1. Quantum Cryptography: Explain how quantum cryptography leverages principles such as superposition and entanglement to enable secure communication. Key mechanisms like Quantum Key Distribution (QKD) can prevent eavesdropping, as any attempt to intercept keys alters their state, alerting the system to potential breaches.
2. Quantum Neural Networks: Discuss the foundations of QNNs, their unique properties for data processing, and how they differ from classical neural networks. QNNs can

potentially process information at a speed and efficiency that surpasses classical networks, making them suitable for optimizing cryptographic tasks.

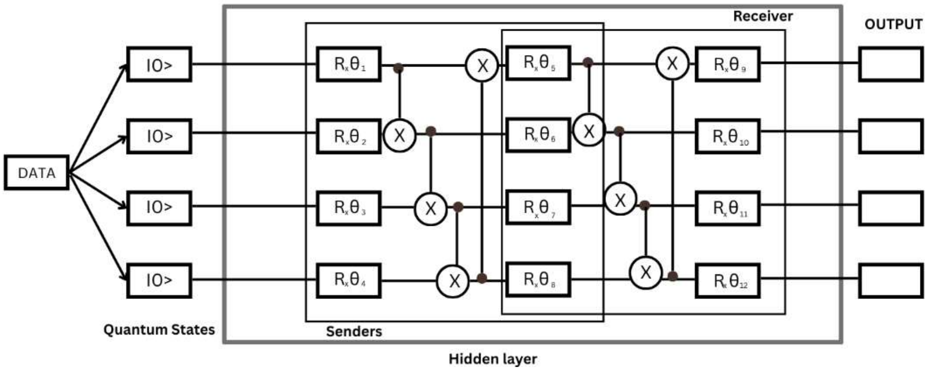
## Objectives

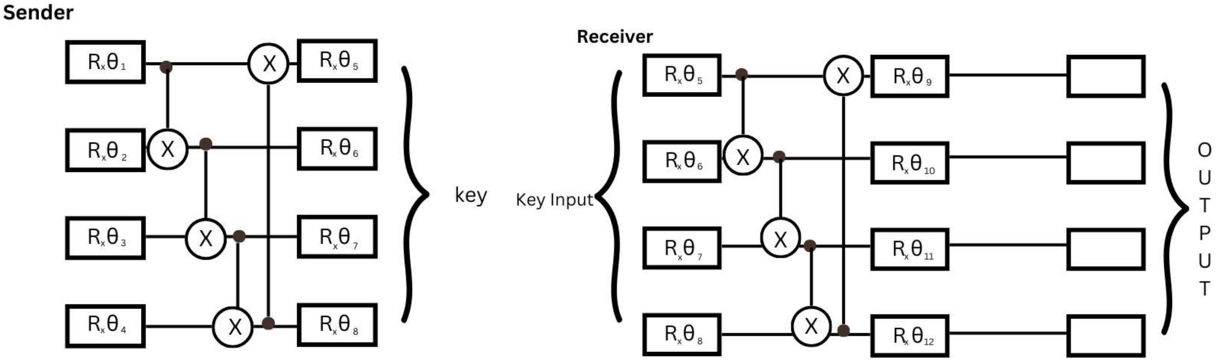
- Develop a QNN-based cryptographic model that can support secure, efficient encryption and decryption processes.
- Evaluate the robustness of QNN cryptographic protocols against common attacks (e.g., brute-force, quantum algorithm attacks).
- Analyze the computational efficiency and performance of QNN-based quantum cryptographic solutions in comparison to classical cryptography.

## Methodology

- Designing the Quantum Neural Network:
  - Architecture: Specify the QNN architecture tailored to cryptographic tasks, considering aspects like qubit arrangement, layers, and activation functions.
- Model Training:
  - Use quantum machine learning techniques to train the QNN, optimizing it for cryptographic efficiency and security.
- Cryptographic Protocol Development:
  - Design a secure QNN-based cryptographic protocol, which can include steps like key generation, encryption, and decryption.
  - Implement Quantum Key Distribution (QKD) to ensure secure transmission of keys.
- Tools and Simulations:
  - Utilize software tools like Qiskit or TensorFlow Quantum to simulate and implement QNN models.
  - Set up a testing environment for model evaluation on quantum or quantum-simulated hardware.
- Data Collection and Testing:

  - Define metrics for assessing security (e.g., resistance to quantum attacks), computational efficiency, and overall performance.
  - Test against various cryptographic attack scenarios to validate robustness.





## Expected Outcomes

- A fully developed QNN-based cryptographic model with verified efficiency and security.
- Insights into the practical application of QNNs in cryptography, with findings potentially contributing to advancements in quantum-secure communications.