AMRITA VISHWA VIDYAPEETHAM

24AIM112- Mathematics for intelligent system 2
24AIM111 - Introduction to data structure and algorithms

Quantum encryption scheme based on taylor series and Fourier transform

Team members:
M Devadharshini CB.AI.U4AIM24126
B Amirthavarshini CB.AI.U4AIM24154
S Nithin CB.AI.U4AIM24133
G harisudharsan CB.AI.U4AIM24113

INTRODUCTION

- Data which include the privacy of the individual needs to be secured.
- different ways of encrypting the data one such method is homomorphic encryption
- allows the computation on the encrypted data different scheme has been developed to encrypt and decrypt
- our proposal of the scheme is based on QFT and taylor series based on encryption scheme

HOMOMORPHIC ENCRYPTION

- It enables computation on encrypted data without decryption.
- Supports privacy-preserving machine learning.

Types:

1. Partially Homomorphic Encryption (PHE)
2. Somewhat Homomorphic Encryption (SHE)
3. Fully Homomorphic Encryption (FHE)

- Our project aims to develop a quantum homomorphic encryption scheme

Development of Quantum Homomorphic Encryption Scheme

- It lets us process data while it's still encrypted, so privacy is never lost
- Our idea combines math and quantum computing:
- Taylor Series creates a secret signal that acts like a lock
- Quantum gates are used to safely hide and later unlock the data
- Quantum Fourier Transform (QFT) changes the data's form so no one can understand it without the key
- Convert data to quantum form using Ry gate
- Add secret signal using Rx gate
- Apply QFT and Rz gate for encryption

QUANTUM FOURIER TRANSFORM

- Quantum version of Discrete Fourier Transform (DFT).
- Efficiently transforms quantum states into frequency domain.
- It is important in quantum cryptography and Shor’s Algorithm.
- Here we used in this scheme to change the data’s domain before encryption.

TAYLOR SERIES

- Approximates complex functions using a polynomial expansion.
- In our project, it is used to generate a signal known only to the private key holder.
- It acts as a secret mathematical layer during encryption.
- It helps to ensure uniqueness and reversibility of the encryption process.

Proposed Scheme

Proposed scheme
Encode the classical data to quantum state
Apply QFT
phase shift using Quantum Gates
addition of a secret signal
Measurement of the output by the probability of the states

Quantum Gates

- Quantum gates manipulate qubits (quantum bits), similar to logic gates in classical computers**.** is used to change the qubit’s state

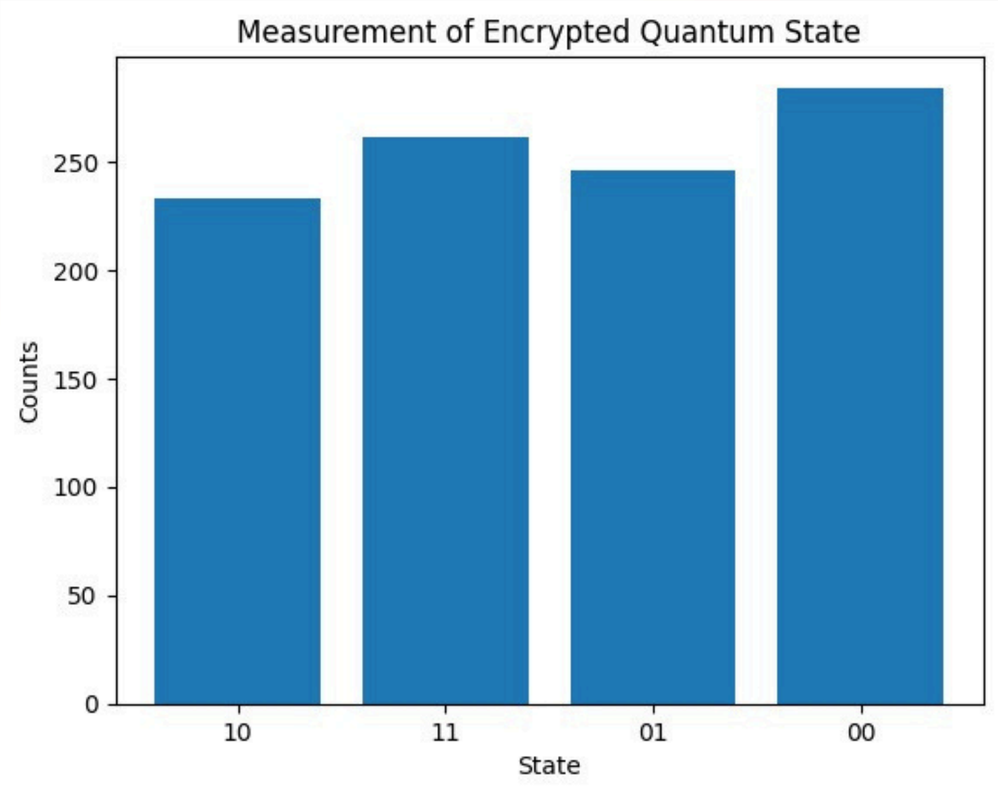
- They rotate or shift the state of a qubit, unlike classical gates which only flip between 0 and 1. quantum gates can work on superposition (both 0 and 1 at the same time)
  In our scheme:
  Ry gate encodes classical data into quantum form
  Rx gate adds a secret signal (from Taylor Series)
  Rz gate applies public key encryption (phase shift)
  These gates make the encryption secure and reversible.

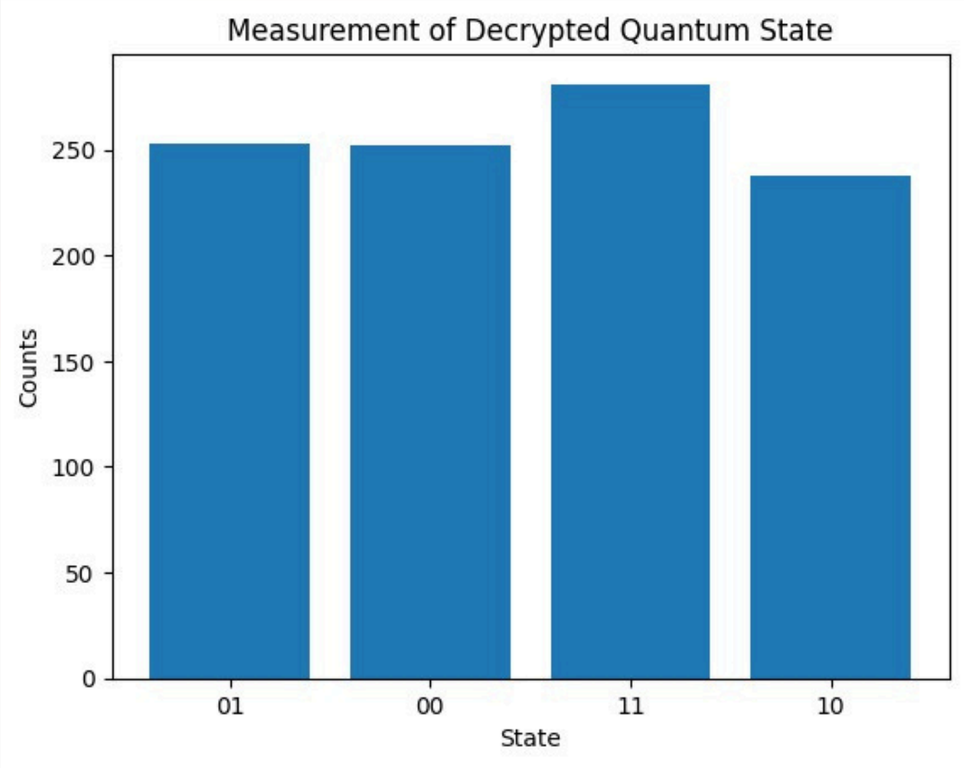
Applications

- Federated Learning - Machine learning approach where multiple devices collaboratively train and share the model without the exchange of the raw data.

- Privacy preserving Machine Learning(PPML) - This technique enables model training and inference while protecting sensitive data .

OUTPUT


Measurement of Encrypted Quantum State
Counts
0
50
100
150
200
250
10
11
01
00
State


Measurement of Decrypted Quantum State
Counts
0
50
100
150
200
250
01
00
11
10
State

RESULT

QUANTUM STATE	DECRYPTED RESULT	ENCRYPTED RESULT
00	277	246
01	251	255
10	236	246

CONCLUSION

- Our project presents a novel quantum encryption approach by integrating a key-based system with the mathematical strength of Taylor Series, Fourier Transform, and quantum mechanics.

- The proposed scheme lays a strong foundation for implementing quantum homomorphic encryption, enabling secure computation on encrypted quantum data and unlocking the full potential of homomorphic encryption in the quantum era

THANK YOU