AdeptHEQ-FL: Adaptive Homomorphic Encryption for Federated Learning of Hybrid Classical-Quantum Models with Dynamic Layer Sparing

Md Abrar Jahin[1] Taufikur Rahman Fuad[2] M. F. Mridha[3] Nafiz Fahad[4] Md. Jakir Hossen[4]

[1]University of Southern California [2]Islamic University of Technology [3]American International University-Bangladesh [4]Multimedia University

INTRODUCTION

Federated Learning (FL) enables decentralized ML across clients without sharing raw data, vital for privacy-sensitive domains.

Key FL challenges

- Statistical heterogeneity (non-IID)
- Privacy leakage
- Communication overhead

Limitations of existing approaches

- **Quantum FL (QFL)**: Improved expressivity, lacks privacy/non-IID robustness [1]
- **Privacy-preserving techniques**: Protects data but reduces utility or incurs overhead
- **Compression** [2]: Efficient but ignores quantum or privacy synergy

AdeptHEQ-FL: A unified hybrid framework addressing all three concurrently.

Key Contributions

1. **Differential Privacy (DP)-Weighted Adaptive Aggregation** using client accuracies and **Homomorphic Encryption (HE)** to effectively address non-IID data
2. **Hybrid Classical-Quantum Architecture** for model expressivity in federated settings
3. **Efficient Dynamic Layer Sparing** reduces communication overhead
4. **Theoretical Convergence Analysis** guarantee under all components

Framework Overview

- **Client**: Trains CNN+PQC, adaptively freezes layers, encrypts final layer (CKKS)
- **Server**: Aggregates encrypted layers using DP-weighted accuracy, sends global model

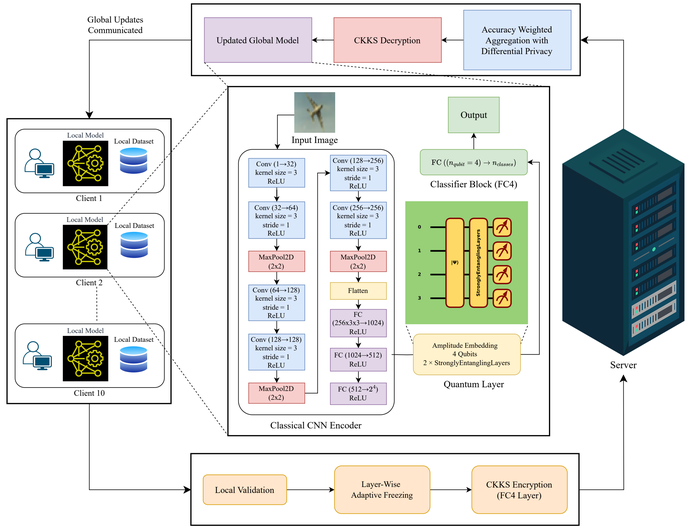

Figure 1. Overview of the AdeptHEQ-FL framework.

Model Architecture

Classical Component: Convolutional Neural Network (CNN)

- 3 conv blocks (conv → ReLU → maxpool)
- Extracts local features, flattened to $\mathbb{R}^{2n}$

Quantum Component: Parametric Quantum Circuit (PQC)

- 4 qubits, 2-layer Strongly Entangling
- **Amplitude Encoding**: $|\psi_x\rangle = \sum x_i |i\rangle$
- **Rotation + CNOT** gates, followed by **Pauli-Z** measurement
- Outputs: $f_{\text{PQC}}(x) \in \mathbb{R}^4$

Final Fully Connected Layer and Output

- Fully connected layer (FC4): $\mathbb{R}^4 \to \mathbb{R}^m$
- Overall: $f(x;\theta) = f_{\text{FC4}}(f_{\text{PQC}}(f_{\text{CNN}}(x)))$

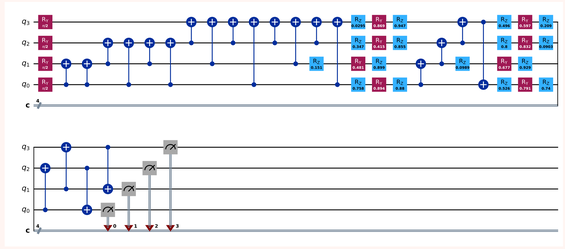

Figure 2. 4-qubit 2-layered PQC of AdeptHEQ-FL comprising amplitude embedding, two Strongly Entangling Layers (parameterized R_z, R_y, R_z rotations), CNOT-based entanglement, and projective measurements. The CNOT connectivity ensures full inter-qubit interaction within each layer.

Federated Learning Mechanisms

Accuracy-Weighted DP Aggregation

- Addresses the non-IID data by weighting client contributions
- Each client privatizes their validation accuracy $a_i^{(t)}$ using the Laplace mechanism: $\tilde{a}_i^{(t)} = \max(0, \min(1, a_i^{(t)} + \zeta)), \quad \zeta \sim \text{Lap}\left(\frac{\Delta_i}{\epsilon}\right)$
- Total privacy loss over $T = 20$ rounds is bounded by: $(\epsilon_{\text{total}}, \delta) = (10, 10^{-5})$
- Server computes aggregation weights $w_i^{(t)}$ via a numerically stable tempered softmax
- Global model is updated as: $\theta^{(t)} = \sum_i w_i^{(t)} \theta_i^{(t)}$

Layer-Wise Adaptive Freezing

- Layer score: $s_l^{(t)} = \|\theta_l^{(t)} - \theta_l^{(t-1)}\|_2$
- Exponential moving average: $\bar{s}_l^{(t)}$; Freeze if $\bar{s}_l^{(t)} < 0.001$
- **Quantum layers remain unfrozen** for adaptability and expressivity

HE (CKKS scheme)

- Only FC_4 encrypted
- Aggregation over encrypted vectors (multiplicative depth 3, $\approx$ 128-bit security)
- Polynomial modulus degree: 8192, scale: 2^{40}

Results

Experimental Setup

- FL: 10 clients, Dirichlet $\alpha = 0.1$, 20 rounds, 10 local epochs
- Optimizer: Adam (lr=1e-3), Batch: 32
- DP: $\epsilon = 1.0$/round, Aggregation: softmax $\tau = 0.5$

Key Findings

Table 1. Performance comparisons of different models across three datasets are shown. The table displays the average loss and accuracy in percentages for the models in our experiment across three different datasets. Each metric is reported as the mean ± standard deviation, calculated over five experimental runs. **Bold** values indicate the best performance in each dataset column.

Model	n_{qubits}	n_{layers}	CIFAR10		SVHN		FashionMNIST	
			Loss (↓)	Accuracy (%) (↑)	Loss (↓)	Accuracy (%) (↑)	Loss (↓)	Accuracy (%) (↑)
Standard-FedQNN	6	6	1.503 ± 0.039	63.60 ± 0.45	0.349 ± 0.002	93.22 ± 0.05	$\mathbf{0.313 \pm 0.003}$	91.96 ± 0.09
FHE-FedQNN	6	6	1.972 ± 0.042	57.89 ± 0.20	0.340 ± 0.006	92.94 ± 0.14	0.328 ± 0.003	91.78 ± 0.11
AdeptHEQ-FL	4	2	$\mathbf{1.306 \pm 0.015}$	$\mathbf{72.61 \pm 0.33}$	0.362 ± 0.004	$\mathbf{94.05 \pm 0.10}$	0.340 ± 0.003	$\mathbf{92.91 \pm 0.12}$
AdeptHEQ-FL	4	1	1.667 ± 0.009	67.22 ± 0.18	$\mathbf{0.331 \pm 0.003}$	93.71 ± 0.12	0.339 ± 0.007	92.76 ± 0.04
AdeptHEQ-FL	2	1	1.640 ± 0.009	62.62 ± 0.42	0.526 ± 0.006	93.58 ± 0.09	0.385 ± 0.004	92.46 ± 0.13

- **AdeptHEQ-FL (4-qubit 2-layer)** achieves highest accuracy across all datasets
- **Efficient & Resource Sensitivity**: Fewer qubits/layers reduce performance, esp. for complex data
- **Ablations** confirm benefits of adaptive aggregation and layer freezing

Conclusion & Future Work

Conclusion

AdeptHEQ-FL is a **privacy-preserving**, **communication-efficient**, and **expressive** hybrid FL framework. It tackles non-IID challenges using DP-weighted aggregation, leverages hybrid models, and reduces communication via adaptive freezing—all while maintaining convergence guarantees and high accuracy.

Limitations & Future Work

- HE currently on FC4 only → Extend to full model
- Simulations only → Validate on quantum hardware
- Assumes convexity in theory → Extend for non-convex settings
- Scale to larger, real-world datasets

Acknowledgment

This work was supported by Multimedia University (MMU), Malaysia.

References

[1] Nouhaila Innan, Muhammad Al-Zafar Khan, Alberto Marchisio, Muhammad Shafique, and Mohamed Bennai. FedQNN: Federated Learning using Quantum Neural Networks. In *International Joint Conference on Neural Networks, IJCNN 2024, Yokohama, Japan, June 30 - July 5, 2024*, pages 1–9. IEEE, 2024.

[2] Zhenyuan Guo, Lei Xu, and Liehuang Zhu. FedSIGN: A sign-based federated learning framework with privacy and robustness guarantees. *Comput. Secur.*, 135:103474, 2023.