

Post Quantum Secure Aggregation for Federated Learning using Lattice based Cryptography

Rama Lakshmi Chunduri¹

¹University of California, San Diego

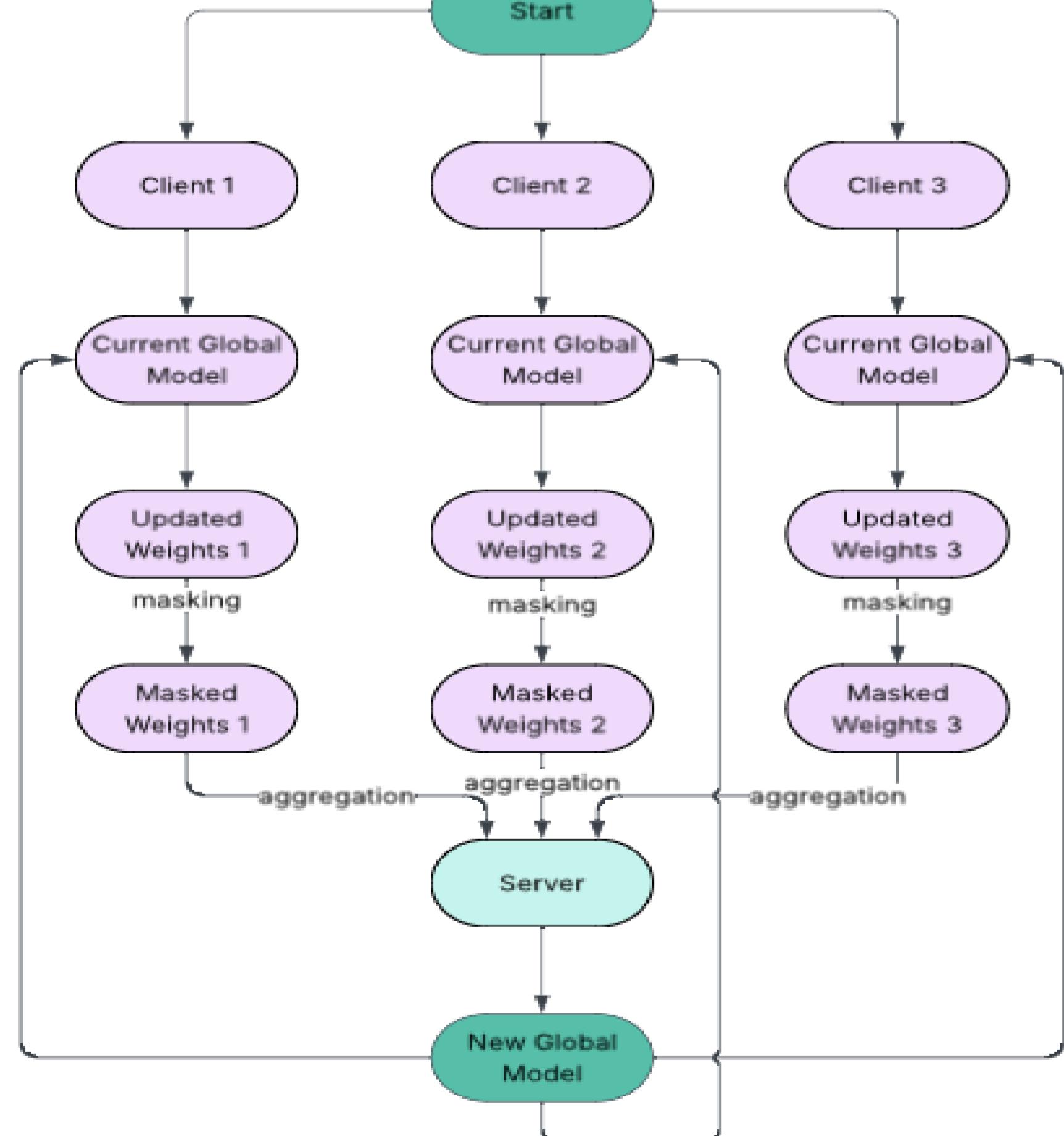
Introduction

Improving the machine learning models in smart devices we use on a daily basis is easier when you have a large dataset. While collecting datasets from users' devices plays a huge role in developing the machine learning model it also raises privacy concerns. This is where the federated machine learning model comes into play. Federated machine learning is a decentralized approach where a model is trained collaboratively using datasets from multiple devices without the data leaving their device. This process involves training the model on individual datasets on devices and then aggregating the results.

Security is very crucial in these aggregation protocols as the gradients of the machine learning model on a device being leaked puts the original data at risk. Solutions such as fully homomorphic encryption (FHE) have been studied widely in federated learning as it allows for computations to be done on encrypted data. But as we know, most of these are based on RSA or ECC, they are computationally heavy, and vulnerable to quantum threats. In this paper we conduct a study experimentally on aggregation protocols that implement lattice based cryptography protocols and test their quantum security.

Methodology

We begin by implementing and validating a lattice-based additive encryption scheme on small toy weights to confirm the correctness and efficiency of masking and unmasking operations. We will then integrate this scheme into a federated learning pipeline and apply it to real-world datasets and models such as the MNIST dataset. We evaluate our protocol against existing aggregation approaches by measuring (i) aggregation runtime, (ii) communication cost, and (iii) model accuracy compared to plaintext training.



Security Goals and Threat Model

The aim of this project is to design an aggregation protocol that remains secure against quantum-capable adversaries. We consider three adversaries:

Server (Malicious) The central server is assumed to be a malicious adversary. It may attempt to learn information about individual client updates even when following the protocol honestly, or it may deviate from the protocol in an effort to manipulate or misuse client data.

Clients (Semi-honest) Clients are assumed to be semi-honest. They execute the protocol as specified in order to protect their own data, but they may attempt to infer more information about the aggregated model or other clients than intended.

Network (Eavesdropping) We assume the communication network is open and subject to passive eavesdropping. Thus, adversaries may intercept transmitted messages, motivating the use of post-quantum secure encryption to ensure confidentiality.

Security Goals. Our protocol aims to achieve:

- **Confidentiality:** Individual client updates must remain hidden from the server, other clients, and eavesdroppers.
- **Correctness:** The final aggregated model must accurately reflect the contributions of all participating clients.
- **Post-quantum security:** All guarantees should hold against adversaries equipped with quantum computing capabilities.

Plots and Tables

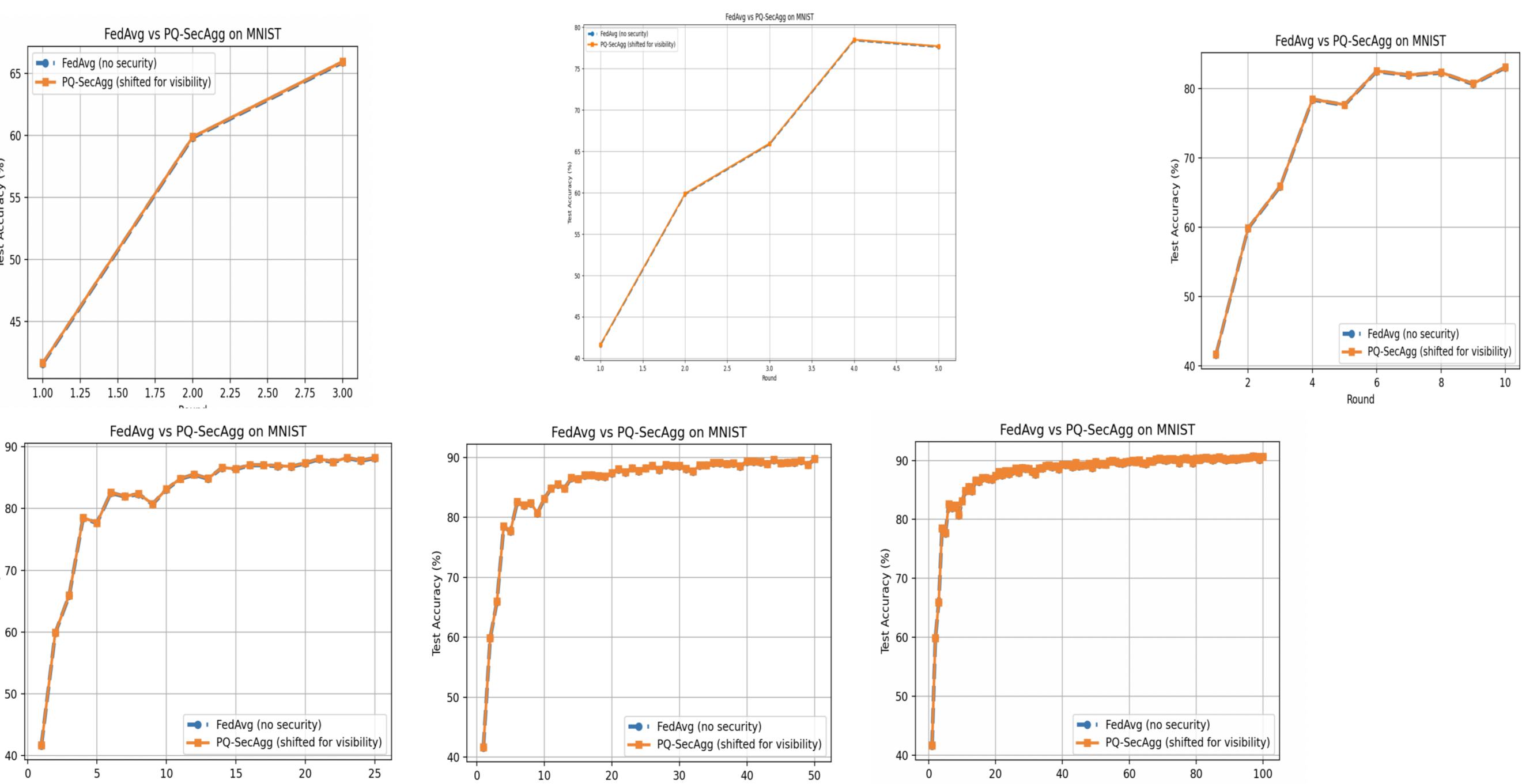


Table 1. Plaintext Aggregation vs. Post Quantum Secure Aggregation

Round No.	Plaintext Aggregation			PQ Secure Aggregation			
	Aggr. Time	Comm. Cost	Accuracy	Aggr. Time	Comm. Cost	Accuracy	Diff. in Norm
1	0.069953	418935	41.60%	0.001980	418935	41.6%	0.00000317
5	0.023126	418935	77.65%	0.001945	418935	77.65%	0.00000322
10	0.024403	418935	83.08%	0.001864	418935	83.08%	0.00000314
25	0.023847	418935	88.17%	0.001856	418935	88.17%	0.00000307
50	0.023452	418935	89.74%	0.001995	418935	89.74%	0.00000326
100	0.023429	418935	90.60%	0.001957	418935	90.60%	0.00000321

Results and Analysis

Results

Plaintext aggregation versus post quantum secure aggregation showed no difference in cost of communication and model accuracy although the aggregation times differ. As shown in the picture below both graphs of plaintext aggregation and post quantum secure aggregation turned out to be exactly the same for test accuracy vs. number of rounds. For the toy weights and for the MNIST dataset we see in the experiments that both of them have the exact same values for communication cost and model accuracy but different aggregation runtimes. It is also observed that the accuracy of the model increases with the number of rounds of training, but we don't train too many rounds to avoid overfitting. This can be observed in the recorded plots below. They represent the graphs for test accuracy plaintext aggregation versus post quantum secure aggregation for different values of number of rounds of training.

Analysis

The fact that the delta measurements for both plaintext aggregation and post quantum secure aggregation are exactly the same implies that the masks are cancelling each other and the server aggregates the same value in both cases. The difference in aggregation runtime is negligible even for a larger dataset such as the MNIST, meaning the cost of using post quantum secure aggregation is not much in terms of aggregation runtime.

Conclusions

We presented a secure aggregation protocol for federated learning that uses lattice-based cryptography to achieve post-quantum security. These experiments on MNIST demonstrated that this protocol maintains correctness of aggregation, and maintains its runtime very close to plaintext aggregation, and achieves accuracy comparable to both plaintext and ECC-based secure aggregation. Compared to ECC-SecAgg, our approach provides stronger long-term security guarantees against quantum adversaries, but at the cost of higher communication cost due to larger key sizes.

Secure Aggregation for Federated Learning was first introduced by Bonawitz et al. This paper explained a protocol based on elliptic curve cryptography which was used in Google's Gboard. Fully homomorphic encryption (FHE) can also be studied in the case of federated learning but since it is very computationally heavy secure aggregation can be preferred on large datasets. With the upcoming quantum threats RSA and ECC based protocols no longer guarantee security. In this situation lattice based cryptographic protocols are more promising and that is what this work contributes towards.

References

- [1] Bonawitz et al., "Practical Secure Aggregation for Federated Learning on User-Held Data," Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 1175–1191, 2017.
- [2] Kim Martineau and Cole Stryker, "What is Federated Learning," IBM Research Blog, 24-Aug-2022 , Available: <https://research.ibm.com/blog/what-is-federated-learning>. [Accessed: 10-Aug-2025].
- [3] National Institute of Standards and Technology, "NIST releases first 3 finalized post-quantum encryption standards," NIST News, 13-Aug-2024. [Online]. Available: <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>. [Accessed: 30-Aug-2025].
- [4] K. Burlachenko, A. Alrowithi, F. Albalawi and P. Richtárik, "Federated Learning is better with Non-Homomorphic Encryption," arXiv preprint arXiv:2312.02074, 2023. doi: 10.1145/3630048.3630182.