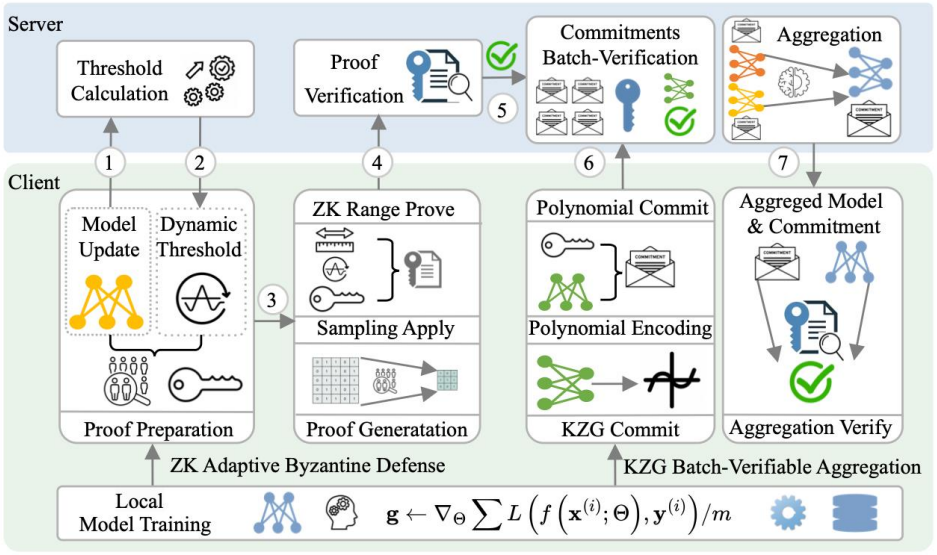
Batch-Verifiable Federated Learning Against Byzantine Threats: A Zero-Knowledge-Enabled Additive-Homomorphic Approach

Heyi ZHANG, Jun WU, Qianqian PAN, Li DING

Frontiers of Computer Science, DOI: 10.1007/s11704-026-51805-6

Problems & Ideas

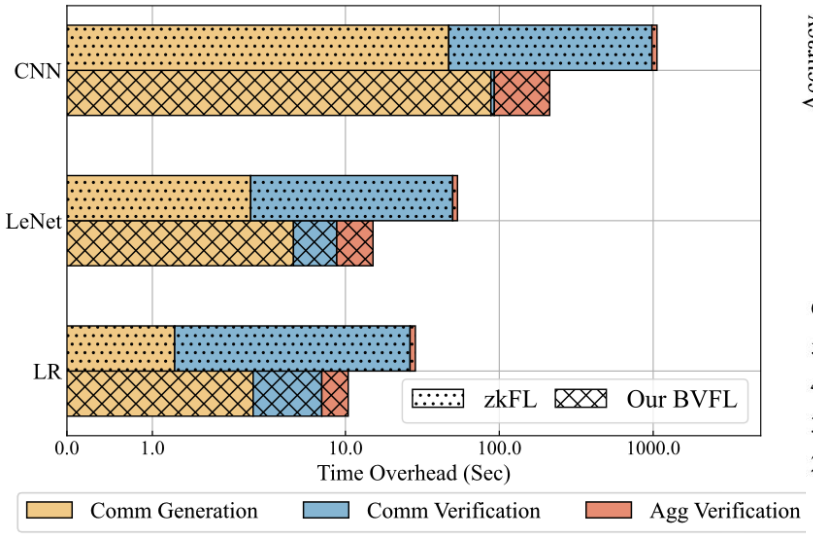
- Problems of conventional secure FL approaches:
  - **Limitations of Prior Works:** FL faces dual threats from Byzantine clients and malicious aggregators, while existing works often focus on single-side defense or rely on unrealistic assumptions.
  - **High Overhead:** Traditional element-wise verification incurs excessive computational costs for large-scale models.
- Ideas: A unified lightweight framework (BVFL) that integrates zero-knowledge adaptive defense for Byzantine robustness and KZG polynomial commitments for efficient batch-verifiable aggregation.



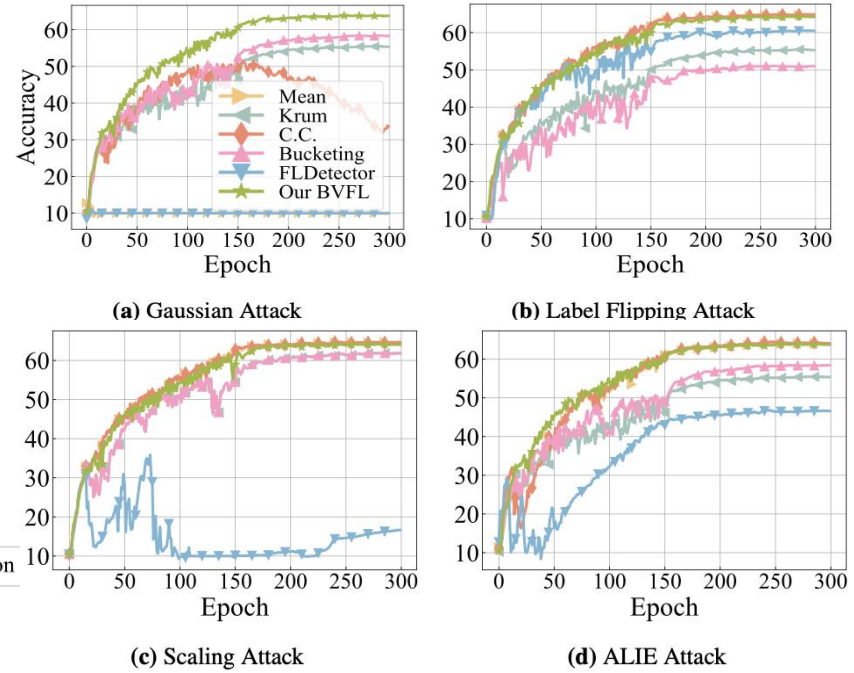
Overview of BVFL with random sampling for efficient robustness and verifiability.

Main Contributions

- Contributions:
  - **BVFL Framework:** A batch-verifiable framework achieving both client-side robustness and server-side verifiability.
  - **ZK-based Defense:** Adaptive thresholding with random sampling to mitigate Byzantine attacks without privacy leakage.
  - **PolyAgg Protocol:** Innovative KZG polynomial commitment enabling batch verification, up to **9x faster** than state-of-the-art methods.



Efficiency: Significant time overhead reduction compared to Pedersen-based zkFL across varying model sizes.



Robustness: Consistently highest accuracy against diverse attacks (e.g., Gaussian, Scaling) on CIFAR-10.