Enhancing Privacy and Efficiency in Decentralized Federated Learning via Hybrid Homomorphic Encryption, Differential Privacy, and Sketch-Based Compression

Nguyen Thanh Hoang*
*Faculty of Information Technology, Ho Chi Minh University of Technology
†AI Research Center, VNU-HCM
Corresponding author: hoang.nguyenthanh0201@hcmut.edu.vn

***Abstract*—Federated learning in decentralized settings faces two persistent challenges: update leakage and high communication costs under repeated peer-to-peer exchanges. We propose a hybrid protocol integrating additive homomorphic encryption (HE) for secure aggregation, client-side differential privacy (DP) with Rényi accounting, and linear sketch-based compression that reduces message dimension from $O(d)$ to $O(m)$ with $m \ll d$ while preserving aggregation linearity. We prove end-to-end (ϵ, δ)-DP via post-processing invariance of sketching and encryption, characterize multi-round privacy using RDP/subsampled-RDP, and quantify sketch-induced error with CountSketch/JL guarantees. A full methodology is provided for parameter selection, complexity analysis, and evaluation on MNIST, CIFAR-10, and FEMNIST over ring and Erdős–Rényi topologies, with baselines against FL+DP, FL+HE, FL+Sketch, and unsecured DFL. The framework delivers a balanced privacy–utility–efficiency trade-off appropriate for decentralized training.**

***Index Terms*—Decentralized Federated Learning, Homomorphic Encryption, Differential Privacy, Sketch, Privacy Preservation, Secure Aggregation**

I. Introduction

Federated learning (FL) enables collaborative training without centralizing raw data but remains vulnerable to information leakage through gradients or weights, especially acute in decentralized federated learning (DFL) where peer-to-peer exchanges replace a central server. Secure aggregation (SA) aims to reveal only sums, DP bounds per-user inference via noise, and linear sketching reduces communication while preserving additive structure; however, unified designs that are provable and efficient in DFL are limited.

Contributions. This paper introduces a hybrid DFL protocol combining: (i) threshold additive-HE secure aggregation tailored for P2P graphs; (ii) client-side DP with clipping and Gaussian mechanism under Rényi accounting (and subsampled-RDP when applicable); (iii) linear sketching (CountSketch or JL-style random projections) to compress updates while maintaining linear aggregability; (iv) end-to-end privacy proofs, error bounds, complexity analysis, parameter selection rules, and a complete experimental plan.

II. Related Work

A. Privacy in FL

Secure aggregation masks client updates to reveal only aggregates, forming a canonical primitive in FL systems. Differential privacy provides formal individual-level guarantees via randomized mechanisms (e.g., Gaussian) and composition analyses (moments accountant/RDP).

B. Decentralized Federated Learning

DFL removes the central server and relies on graph-based exchanges (e.g., ring, Erdős–Rényi) with synchronous or asynchronous protocols and gossip-style averaging; robustness and mixing rates influence convergence.

C. Communication Compression

Gradient sparsification, quantization, and sketching (CountSketch, random projections) reduce bandwidth; linear sketches preserve additive structure and admit unbiased/norm-preserving reconstruction with controlled error.

D. Gap Summary

A unified, provable framework marrying DP + HE + Sketch specifically for DFL—with concrete protocols, proofs, and implementable guidance—remains underexplored.

III. Proposed Methodology

A. System Model and Threat Model

Let $G = (V, E)$ be a connected P2P graph with $|V| = n$. Each node i holds local data D_i and parameters θ_i^t at round t, exchanging only with neighbors $N(i)$. The adversary is honest-but-curious, may collude across a subset of peers, observes ciphertext/plaintext messages on incident edges, and aims to infer per-user data; DP noise is applied client-side, top-L sketched coordinates are encrypted, and only aggregate sums are threshold-decrypted.

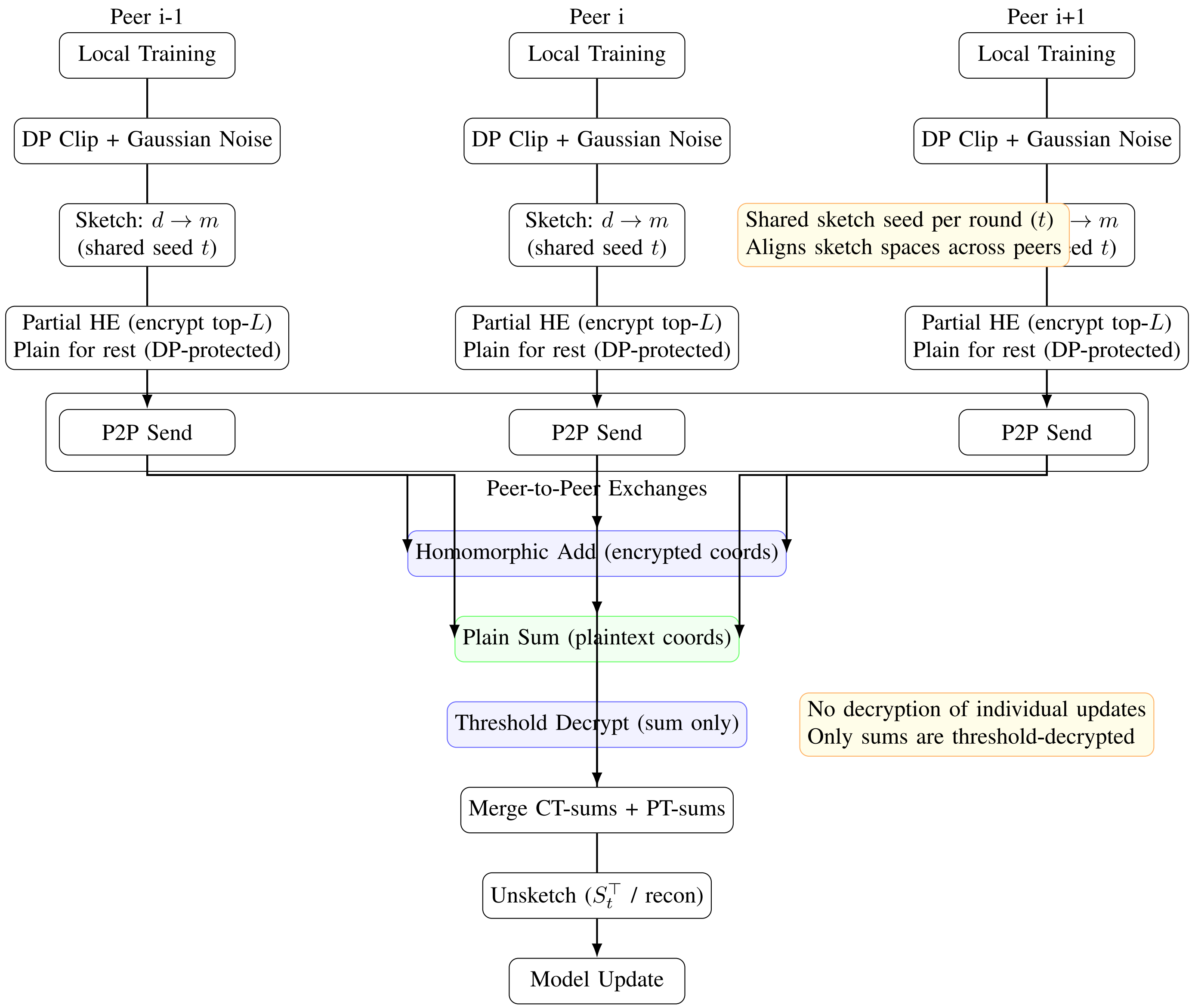

Fig. 1: DFL architecture with HE + DP + Sketch: per-peer pipeline, P2P exchange, parallel aggregation (CT vs. PT), threshold decryption of sums, unsketch, and model update; key parameters: d, $m \ll d$, $L \leq m$.

B. Protocol Overview

At each round t: (1) node i computes local update g_i^t; (2) clips to $\bar{g}_i^t$ and adds Gaussian noise to obtain $\tilde{g}_i^t$; (3) applies a linear sketch $S_t \in \mathbb{R}^{m \times d}$ (shared seed per round) to get $s_i^t = S_t \tilde{g}_i^t$; (4) partially encrypts top-L coordinates via additive HE, leaving the remainder plaintext but DP-protected; (5) exchanges with neighbors; (6) homomorphically adds encrypted parts and sums plaintext parts; (7) threshold-decrypts encrypted sums; (8) unsketches to estimate the aggregate; (9) updates θ_i^{t+1}.

C. DP Layer

Clipping enforces sensitivity: $\bar{g}_i^t = g_i^t / \max\{1, \|g_i^t\|_2 / C\}$. Gaussian mechanism: $\tilde{g}_i^t = \bar{g}_i^t + \eta_i^t$, $\eta_i^t \sim \mathcal{N}(0, \sigma^2 C^2 I_d)$. Multi-round privacy uses Rényi DP (RDP) with per-round $\epsilon_\alpha = \alpha/(2\sigma^2)$, additive over rounds, and conversion to (ϵ, δ)-DP by optimizing over α; subsampled-RDP applies if participation/minibatching is subsampled.

D. Sketch Layer

Use CountSketch (with K hash/sign tables) or JL-style random projections (Rademacher/Gaussian). For CountSketch, reconstructions are unbiased with mean-squared error scaling as $O(\|x\|_2^2/m)$; JL projections preserve norms/inner products within $1 \pm \varepsilon$ for $m = O(\varepsilon^{-2} \log n)$. Linearity allows aggregation in the compressed domain.

E. HE Layer

Adopt additive HE (Paillier) with threshold decryption; encrypt only top-L sketched coordinates (partial HE) while the rest remain plaintext but DP-protected. Homomorphic addition

Algorithm 1 Per-Node Decentralized HE+DP+Sketch (Round t)

```
Compute local update $g_i^t$
Clip and noise: $\tilde{g}_i^t = \mathrm{clip}(g_i^t; C) + \mathcal{N}(0, \sigma^2 C^2 I)$
Sample linear sketch $S_t$ (shared seed); $s_i^t = S_t \tilde{g}_i^t$
Partial HE: encrypt top-$L$ coords of $s_i^t$ (others plaintext)
Send $(s_i^t)$ to neighbors via P2P links
Aggregate: homomorphic-add encrypted coords; plain-sum plaintext coords
Threshold-decrypt encrypted sums (sums only)
Unsketch to estimate aggregate in $\mathbb{R}^d$
Update model: $\theta_i^{t+1} = \theta_i^t - \eta_t \hat{G}_i^t$
```

on ciphertext coordinates yields the encrypted sum; only sums are threshold-decrypted.

F. Decentralized Aggregation Protocol

IV. Theoretical Analysis

A. Differential Privacy Guarantees

Definition 1 (Differential Privacy)**.** *A randomized mechanism $\mathcal{M}$ is (ϵ, δ)-DP if for neighboring datasets D, D' and measurable sets S,*

$$\Pr[\mathcal{M}(D) \in S] \leq e^{\epsilon} \Pr[\mathcal{M}(D') \in S] + \delta.$$

Theorem 1 (Post-Processing and Rényi Composition)**.** *Let $\mathcal{M}$ be the Gaussian DP mechanism with clipping constant C and noise σ. Then any (randomized) mapping $\mathcal{A}$ (e.g., sketching, encryption, transport, threshold-decryption-of-sums) yields $\mathcal{A} \circ \mathcal{M}$ DP. Under RDP, Gaussian has per-round $\epsilon_\alpha = \alpha/(2\sigma^2)$; over T rounds they sum to $T\epsilon_\alpha$, which converts to (ϵ, δ)-DP by optimizing*

$$\epsilon = \min_{\alpha > 1} \left\{ \frac{T\alpha}{2\sigma^2} + \frac{\ln(1/\delta)}{\alpha - 1} \right\}.$$

Corollary (Subsampled-RDP). If per-round client participation is subsampled with rate γ, subsampled-RDP yields amplification that tightens cumulative privacy for fixed σ.

B. Cryptographic Security

Paillier provides additive homomorphism $E(m_1)E(m_2) = E(m_1 + m_2)$ with IND-CPA security under the decisional composite residuosity assumption; threshold decryption ensures only aggregates are revealed. Partial HE encrypts high-energy coordinates while plaintext coordinates remain protected by DP.

C. Sketch Error and Robustness

For CountSketch with K tables and suitable reconstruction,

$$\mathbb{E}\left[\|\hat{x} - x\|_2^2\right] \leq \frac{\kappa}{m} \|x\|_2^2,$$

for constant κ depending on sketch design; robust analyses show resilience to adaptive inputs. JL projections preserve norms/inner products up to $1 \pm \varepsilon$ for $m = O(\varepsilon^{-2} \log n)$.

D. Convergence with Noise and Sketch

Under smooth convex losses with bounded gradients, connected mixing, and diminishing stepsizes ($\sum_t \eta_t = \infty$, $\sum_t \eta_t^2 < \infty$), decentralized SGD converges to a neighborhood of an optimum whose radius scales with the net variance from DP noise $\sigma^2 C^2$ and sketch error $O(1/m)$, with topology-dependent constants due to mixing.

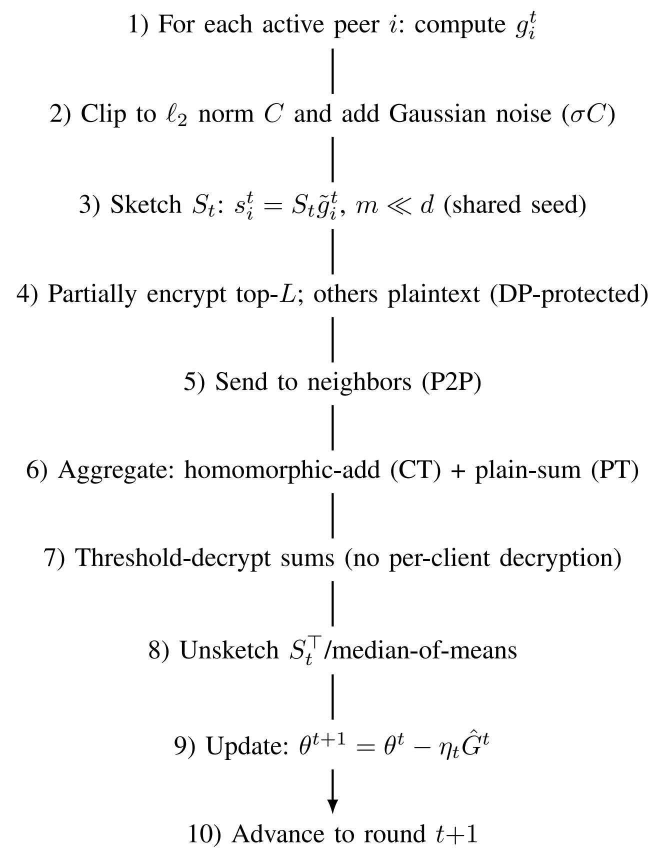

Fig. 2: Per-round protocol: DP $\to$ Sketch $\to$ Partial HE $\to$ P2P $\to$ secure aggregation $\to$ unsketch $\to$ update.

V. Experimental Evaluation

A. Setup

Datasets: MNIST, CIFAR-10, FEMNIST (LEAF). Models: small CNNs (MNIST/CIFAR-10) and MLP/CNN (FEMNIST). Partitions: non-IID via Dirichlet $\alpha = 0.5$. Topologies: ring and Erdős–Rényi with varying average degrees. Privacy: $\delta = 10^{-5}$, ϵ tracked by RDP/subsampled-RDP. Sketch sizes $m/d \in \{1\%, 2\%, 5\%\}$. Partial HE ratios $\rho = L/m \in [0.2, 0.5]$.

B. Baselines and Metrics

Baselines: FL+DP, FL+HE, FL+Sketch, unsecured DFL, and proposed HE+DP+Sketch DFL. Metrics: top-1 accuracy, bytes per round per client, runtime per round, and cumulative (ϵ, δ).

C. Comparison (Qualitative)

TABLE I: Qualitative comparison across methods.

Method	Privacy	Comm.	Compute	Utility
FL+DP	Formal DP	Mid	Low	Mid–High
FL+HE	Encrypted sum	High	High	High
FL+Sketch	None formal	Low	Low	Mid
DFL (ours)	DP+HE	Low–Mid	Mid	High

D. Expected Trends

Sketching at $m/d \in [1\%, 5\%]$ typically yields 8–20$\times$ communication reduction with $\leq 1\%$ accuracy loss at $\epsilon \in [2, 6]$; partial encryption amortizes HE cost by restricting ciphertext to top-L positions.

VI. Discussion

HE secures aggregation but is computationally heavy; linear sketching and partial HE reduce encrypted payload and cost. DP provides individual-level guarantees preserved via post-processing across sketching and encryption, enabling precise tuning of ϵ. Limitations include threshold-HE deployment, dynamic committees, and synchronization under churn; extensions include asynchronous DFL, Byzantine-robust decryption committees, and ledger-backed key audit.

VII. Conclusion

A hybrid DFL framework combining additive HE, client-side DP, and linear sketching achieves a practical privacy–utility–efficiency balance with formal guarantees, correctness in compressed aggregation, and favorable communication scaling; the analysis and design guidelines render the approach implementable across standard benchmarks and topologies.

References

[1] K. Bonawitz et al., “Practical Secure Aggregation for Privacy-Preserving Machine Learning,” in Proc. ACM CCS, 2017.

[2] P. Paillier, “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes,” EUROCRYPT, 1999.

[3] C. Dwork, “Differential Privacy: A Survey of Results,” in Proc. TAMC, 2008.

[4] I. Mironov, “Rényi Differential Privacy,” in Proc. IEEE CSF, 2017.

[5] Y.-X. Wang, B. Balle, S. Kasiviswanathan, “Subsampled Rényi Differential Privacy and Analytical Moments Accountant,” in Proc. AISTATS, 2019.

[6] M. Charikar, K. Chen, M. Farach-Colton, “Finding Frequent Items in Data Streams,” ICALP, 2002. (CountSketch)

[7] J. Cohen et al., “On the Robustness of CountSketch to Adaptive Inputs,” in Proc. ICML, PMLR, 2022.

[8] B. Ghojogh et al., “Johnson–Lindenstrauss Lemma, Linear and Nonlinear Random Projections,” arXiv:2108.04172, 2021.

[9] L. Yuan et al., “Decentralized Federated Learning: A Survey and Perspective,” arXiv:2306.01603 (v2), 2024.

[10] S. Caldas et al., “LEAF: A Benchmark for Federated Settings,” NeurIPS, 2019 (workshop).