Novelty Assessment Report

Paper: Convergent Differential Privacy Analysis for General Federated Learning

PDF URL: https://openreview.net/pdf?id=7Zbe5ad3eX

Venue: ICLR 2026 Conference Submission

Year: 2026

Report Generated: 2026-01-07

Abstract

The powerful cooperation of federated learning (FL) and differential privacy (DP) provides a promising paradigm for the large-scale private clients. However, existing analyses in FL-DP mostly rely on the composition theorem and cannot tightly quantify the privacy leakage challenges, which is tight for a few communication rounds but yields an arbitrarily loose and divergent bound eventually. This also implies a counterintuitive judgment, suggesting that FL-DP may not provide adequate privacy support during long-term training under constant-level noisy perturbations, yielding discrepancy between the theoretical and experimental results. To further investigate the convergent privacy and reliability of the FL-DP framework, in this paper, we comprehensively evaluate the worst privacy of two classical methods under the non-convex and smooth objectives based on the F-DP analysis. With the aid of the shifted interpolation technique, we successfully prove that privacy in Noisy-FedAvg has a tight convergent bound. Moreover, with the regularization of the proxy term, privacy in Noisy-FedProx has a stable constant lower bound. Our analysis further demonstrates a solid theoretical foundation for the reliability of privacy in FL-DP. Meanwhile, our conclusions can also be losslessly converted to other classical DP analytical frameworks, e.g. (ϵ,δ)-DP and R$\'{e}$nyi-DP (RDP), to provide more fine-grained understandings for the FL-DP frameworks.

Disclaimer

This report is **AI-GENERATED** using Large Language Models and WisPaper (a scholar search engine). It analyzes academic papers' tasks and contributions against retrieved prior work. While this system identifies **POTENTIAL** overlaps and novel directions, **ITS COVERAGE IS NOT EXHAUSTIVE AND JUDGMENTS ARE APPROXIMATE**. These results are intended to assist human reviewers and **SHOULD NOT** be relied upon as a definitive verdict on novelty.

Note that some papers exist in multiple, slightly different versions (e.g., with different titles or URLs). The system may retrieve several versions of the same underlying work. The current automated pipeline does not reliably align or distinguish these cases, so human reviewers will need to disambiguate them manually.

If you have any questions, please contact: mingzhang23@m.fudan.edu.cn

Core Task Landscape

This paper addresses: **Convergent Differential Privacy Analysis for Federated Learning**

A total of **50 papers** were analyzed and organized into a taxonomy with **20 categories**.

Taxonomy Overview

The research landscape has been organized into the following main categories:

- **Privacy Analysis Frameworks and Theoretical Foundations**
- **Federated Learning Algorithm Design with Differential Privacy**
- **Communication and Computation Efficiency Enhancements**
- **Distributed Optimization with Differential Privacy**
- **Privacy-Preserving Collaborative Learning Systems**
- **Application-Specific Privacy-Preserving Learning**
- **Privacy-Utility Trade-offs and Incentive Mechanisms**
- **Communication-Efficient Privacy-Preserving Distributed Learning**
- **Trustworthy and Scalable Collaborative Learning Frameworks**

Complete Taxonomy Tree

- Convergent Differential Privacy Analysis for Federated Learning Survey Taxonomy
- Privacy Analysis Frameworks and Theoretical Foundations
    - Convergence and Privacy Trade-off Analysis ★ (5 papers)
    - [0] Convergent Differential Privacy Analysis for General Federated Learning (Anon et al., 2026) View paper
    - [1] Convergent Differential Privacy Analysis for General Federated Learning: the -DP Perspective (Y Sun, 2024) View paper
    - [8] Differentially private federated learning on non-iid data: Convergence analysis and adaptive optimization (Lin Chen, 2024) View paper
    - [15] Differentially private federated learning: Algorithm, analysis and optimization (Kang Wei, 2021) View paper
    - Privacy Amplification and Accounting Mechanisms (4 papers)
    - [4] Harmonizing Differential Privacy Mechanisms for Federated Learning: Boosting Accuracy and Convergence (Shuya Feng, 2024) View paper
    - [5] Universally Harmonizing Differential Privacy Mechanisms for Federated Learning: Boosting Accuracy and Convergence (Feng Shuya, 2024) View paper
    - [7] Mitigating Privacy-Utility Trade-off in Decentralized Federated Learning via -Differential Privacy (X Li, 2025) View paper
    - [14] Shuffled model of differential privacy in federated learning (Antonious M. Girgis, 2021) View paper
    - Clipping and Noise Injection Analysis (3 papers)
    - [19] Federated learning with sparsified model perturbation: Improving accuracy under client-level differential privacy (Rui Hu, 2023) View paper
    - [28] Understanding clipping for federated learning: Convergence and client-level differential privacy (Zhang Xin-wei, 2022) View paper
    - [36] A Differential Privacy Federated Learning Scheme Based on Adaptive Gaussian Noise (Sanxiu Jiao, 2023) View paper
- Federated Learning Algorithm Design with Differential Privacy
    - Centralized and Hierarchical FL with DP (4 papers)
    - [2] Client-based differential privacy federated learning (Zengwang Jin, 2023) View paper
    - [17] Utility-Enhanced Personalized Privacy Preservation in Hierarchical Federated Learning (Jianan Chen, 2025) View paper

  - [26] Performance-Enhanced Federated Learning With Differential Privacy for Internet of Things (Xicong Shen, 2022) View paper
  - [33] Federated learning with differential privacy: Algorithms and performance analysis (Kang Wei, 2020) View paper
  - Decentralized and Peer-to-Peer FL with DP (4 papers)
  - [3] Dp-norm: Differential privacy primal-dual algorithm for decentralized federated learning (Takumi Fukami, 2024) View paper
  - [10] Privacy-Preserving and Reliable Decentralized Federated Learning (Yuan-Yuan Gao, 2023) View paper
  - [23] Noiseless Privacy-Preserving Decentralized Learning (Sayan Biswas, 2024) View paper
  - [37] Decentralized wireless federated learning with differential privacy (Shuzhen Chen, 2022) View paper
  - Personalized and Meta-Learning FL with DP (1 papers)
  - [6] Personalized federated learning with differential privacy and convergence guarantee (Kang Wei, 2023) View paper
  - Asynchronous FL with DP (4 papers)
  - [34] Asynchronous federated learning with differential privacy for edge intelligence (Li Yanan, 2019) View paper
  - [41] Privacy-Preserving Asynchronous Grouped Federated Learning for IoT (Tao Zhang, 2021) View paper
  - [45] Privacy-Preserving Verifiable Asynchronous Federated Learning (Yuan-Yuan Gao, 2021) View paper
  - [49] Multi-Stage Asynchronous Federated Learning With Adaptive Differential Privacy (Yanan Li, 2023) View paper
  - Vertical and Cross-Silo FL with DP (1 papers)
  - [11] Privacy-Preserving Asynchronous Vertical Federated Learning Algorithms for Multiparty Collaborative Learning (Bin Gu, 2021) View paper
- Communication and Computation Efficiency Enhancements
  - Quantization and Compression for DP-FL (2 papers)
  - [30] Privacy-preserving federated learning on lattice quantization (Ling-jie Zhang, 2023) View paper
  - [44] Layered Randomized Quantization for Communication-Efficient and Privacy-Preserving Distributed Learning (Guangfeng Yan, 2023) View paper
  - Adaptive and Accelerated Training Strategies (2 papers)
  - [24] A differential privacy federated learning framework for accelerating convergence (Yaling Zhang, 2022) View paper
  - [25] Adaptive Local Steps Federated Learning with Differential Privacy Driven by Convergence Analysis (Ling, 2023) View paper
- Distributed Optimization with Differential Privacy
  - Consensus and Constrained Optimization with DP (2 papers)
  - [22] Robust Constrained Consensus and Inequality-Constrained Distributed Optimization With Guaranteed Differential Privacy and Accurate Convergence (Yongqiang Wang, 2024) View paper
  - [29] Differentially Private Distributed Algorithms for Aggregative Games With Guaranteed Convergence (Yongqiang Wang, 2024) View paper
  - Online and Stochastic Optimization with DP (2 papers)
  - [13] Local Differential Privacy for Decentralized Online Stochastic Optimization With Guaranteed Optimality and Convergence Speed (Ziqin Chen, 2024) View paper
  - [16] Locally differentially private decentralized stochastic bilevel optimization with guaranteed convergence accuracy (Z Chen, 2024) View paper
  - ADMM-Based Distributed Learning with DP (2 papers)
  - [12] Privacy-preserving incremental ADMM for decentralized consensus optimization (Ye Yu, 2020) View paper
  - [48] DP-ADMM: ADMM-based distributed learning with differential privacy (Huang Zonghao, 2019) View paper
- Privacy-Preserving Collaborative Learning Systems
  - Secure Multiparty Computation and Encryption Integration (4 papers)
  - [18] A Scalable Approach for Privacy-Preserving Collaborative Machine Learning (Jinhyun So, 2022) View paper
  - [27] Privcoll: Practical privacy-preserving collaborative machine learning (Zhang Yan-jun, 2020) View paper
  - [31] PPCL: Privacy-preserving collaborative learning for mitigating indirect information leakage (Hongyang Yan, 2021) View paper
  - [46] Privacy-Preserving Federated Learning via System Immersion and Random Matrix Encryption (Haleh Hayati, 2022) View paper
  - Blockchain and Verification Mechanisms (1 papers)
  - [35] Privacy-Preserving Byzantine-Robust Federated Learning via Blockchain Systems (Yinbin Miao, 2022) View paper
  - Local Differential Privacy Frameworks (1 papers)
  - [32] LDP-Fed: Federated learning with local differential privacy (Truex Stacey, 2020) View paper
- Application-Specific Privacy-Preserving Learning
  - Wireless and Edge Intelligence (2 papers)
  - [38] Distributed privacy-preserving collaborative intrusion detection systems for VANETs (Tao Zhang, 2018) View paper
  - [47] Communication and Energy Efficient Wireless Federated Learning With Intrinsic Privacy (Zhenxiao Zhang, 2023) View paper
- Privacy-Utility Trade-offs and Incentive Mechanisms (2 papers)
  - [42] The value of collaboration in convex machine learning with differential privacy (Nan Wu, 2020) View paper
  - [50] Privacy preserving collaborative computing: Heterogeneous privacy guarantee and efficient incentive mechanism (Xin Wang, 2018) View paper
- Communication-Efficient Privacy-Preserving Distributed Learning (4 papers)
  - [20] Communication-efficient and privacy-aware distributed learning (Vinay Chakravarthi Gogineni, 2023) View paper
  - [21] Differentially Private and Communication Efficient Collaborative Learning (Bi, 2021) View paper
  - [39] LEASGD: an Efficient and Privacy-Preserving Decentralized Algorithm for Distributed Learning (Cheng, 2022) View paper
  - [40] Enforcing privacy in distributed learning with performance guarantees (Elsa Rizk, 2023) View paper
- Trustworthy and Scalable Collaborative Learning Frameworks (1 papers)
  - [43] Enabling trustworthy and scalable collaborative learning systems (Huancheng, 2025) View paper

Narrative

Core task: convergent differential privacy analysis for federated learning. The field organizes around several major branches that reflect distinct emphases in privacy-preserving distributed machine learning. Privacy Analysis Frameworks and Theoretical Foundations focuses on rigorous convergence and privacy trade-off analysis, examining how noise injection affects learning guarantees under various privacy models such as local, central, and shuffled differential privacy. Federated Learning Algorithm Design with Differential Privacy and Distributed Optimization with Differential Privacy develop concrete algorithmic strategies—ranging from gradient perturbation methods like DP-SGD to ADMM-based approaches—that balance model accuracy with formal privacy budgets. Communication and Computation Efficiency Enhancements and Communication-Efficient Privacy-Preserving Distributed Learning address the practical overhead of adding noise and transmitting updates, exploring quantization, sparsification, and adaptive local steps to reduce bandwidth costs. Meanwhile, Privacy-Preserving Collaborative Learning Systems and Trustworthy and Scalable Collaborative Learning Frameworks tackle system-level concerns including asynchronous aggregation, Byzantine robustness, and verifiable computation, while Application-Specific Privacy-Preserving Learning and Privacy-Utility Trade-offs and Incentive Mechanisms consider domain constraints and participant incentives in real-world deployments.

Within the theoretical foundations branch, a particularly active line of work investigates how different privacy definitions and noise mechanisms influence convergence rates under non-IID data and heterogeneous client participation. Convergent DP Federated[0] sits squarely in this cluster, analyzing the interplay between privacy guarantees and optimization convergence in federated settings. It shares thematic ground with Convergent fDP Perspective[9] and DP NonIID Convergence[8], which similarly examine convergence under differential privacy constraints and data heterogeneity, though each work may emphasize different noise calibration strategies or client sampling schemes. Nearby efforts such as DP Norm Primal Dual[3] and Harmonizing DP Mechanisms[4] explore alternative optimization frameworks and unified privacy accounting methods, highlighting ongoing questions about which algorithmic primitives best reconcile strong privacy with fast, stable learning. This landscape reveals a tension between tightening privacy bounds and maintaining practical convergence speeds, with Convergent DP Federated[0] contributing formal analysis that helps clarify these trade-offs in federated environments.

Related Works in Same Category

The following **4 sibling papers** share the same taxonomy leaf node with the original paper:

1. Convergent Differential Privacy Analysis for General Federated Learning: the -DP Perspective

Authors: Y Sun, L Shen, D Tao | **Year/Venue**: 2024 | **URL**: View paper

Abstract

Federated learning (FL) is an efficient collaborative training paradigm extensively developed with a focus on local privacy, and differential privacy (DP) is a classical approach to capture â¦

⚠ Similarity Notice

These papers appear to be the same work or very closely related variants. Both titles are nearly identical ('Convergent Differential Privacy Analysis for General Federated Learning'), both address convergent differential privacy analysis for federated learning using f-DP framework with shifted interpolation techniques, and both analyze Noisy-FedAvg and Noisy-FedProx methods under non-convex smooth objectives. The abstracts, technical approaches, and main theoretical contributions (proving convergent privacy bounds) are essentially identical, suggesting these are likely the same paper or different versions of the same submission.

2. Differentially private federated learning on non-iid data: Convergence analysis and adaptive optimization

Authors: Lin Chen, Xiaofeng Ding, Zhifeng Bao, Pan Zhou, Hai Jin | **Year/Venue**: 2024 | **URL**: View paper

Abstract

Federated learning (FL) has attracted increasing attention in recent years due to its data privacy preservation and great applicability to large-scale user scenarios. However, when FL faces numerous clients, it is inevitable to emerge the non-independent and identically distributed (non-iid) data between clients, which brings an enormous challenge for model training and performance analysis like convergence. Besides, due to the non-iid data, the participating clients of FL tend to be extremely h...

Relationship Analysis

Both papers belong to the Convergence and Privacy Trade-off Analysis category, examining privacy-utility-convergence relationships in federated learning with differential privacy. They overlap in analyzing non-convex federated learning scenarios with differential privacy guarantees and addressing privacy budget accumulation over training rounds. However, the original paper focuses on f-DP analysis with shifted interpolation techniques to prove convergent privacy bounds for FedAvg and FedProx, while the candidate paper emphasizes truncated concentrated differential privacy for non-iid data with adaptive server-side optimization and uniform client sampling without replacement.

3. Convergent Differential Privacy Analysis for General Federated Learning: the f-DP Perspective

Authors: Sun Yan, Shen, Li, Yan Sun, Tao, et al. (8 authors total) | **Year/Venue**: 2024 | **URL**: View paper

Abstract

Federated learning (FL) is an efficient collaborative training paradigm extensively developed with a focus on local privacy, and differential privacy (DP) is a classical approach to capture and ensure the reliability of private security. Their powerful cooperation provides a promising paradigm for the large-scale private clients. As a predominant implementation, the noisy perturbation has been widely studied, being theoretically proven to offer significant protections. However, existing analyses...

⚠ Similarity Notice

These papers appear to be the same work or very closely related variants. Both titles are nearly identical ('Convergent Differential Privacy Analysis for General Federated Learning' vs. 'Convergent Differential Privacy Analysis for General Federated Learning: the f-DP Perspective'), and the abstracts describe essentially the same contributions: proving convergent privacy bounds for Noisy-FedAvg and Noisy-FedProx using f-DP analysis with shifted interpolation techniques under non-convex objectives. The core technical approach, main theorems, and results appear identical or extremely similar.

4. Differentially private federated learning: Algorithm, analysis and optimization

Authors: Kang Wei, Jun Li, Chuan Ma, Ming Ding, H. Poor, et al. (6 authors total) | **Year/Venue**: 2021 | **URL**: View paper

Abstract

â¦ a differential privacy â¦ , a better convergence performance leads to a lower protection level; (2) Increasing the number of N overall clients participating in FL can improve the convergence â¦

Relationship Analysis

Both papers belong to the Convergence and Privacy Trade-off Analysis category, examining privacy-utility-convergence relationships in federated learning with differential privacy. They overlap in analyzing how privacy guarantees evolve during FL training and the fundamental trade-offs between privacy budgets and convergence performance. The key difference is that the original paper focuses on proving convergent (non-divergent) privacy bounds using f-DP and shifted interpolation techniques for non-convex objectives, while the candidate paper appears to provide algorithmic frameworks and optimization strategies for DP-FL with emphasis on how client participation affects both convergence and privacy levels.

Contributions Analysis

Overall novelty summary. This paper develops convergent privacy bounds for Noisy-FedAvg and Noisy-FedProx under non-convex objectives using f-DP analysis and shifted interpolation techniques. It resides in the 'Convergence and Privacy Trade-off Analysis' leaf, which contains five papers total including the original work. This leaf sits within the broader 'Privacy Analysis Frameworks and Theoretical Foundations' branch, indicating a moderately populated research direction focused on formal privacy guarantees rather than algorithm design or system implementation. The sibling papers in this leaf similarly examine convergence-privacy trade-offs, suggesting this is an active but not overcrowded theoretical niche.

The taxonomy reveals neighboring leaves addressing 'Privacy Amplification and Accounting Mechanisms' (four papers) and 'Clipping and Noise Injection Analysis' (three papers), both within the same theoretical foundations branch. These adjacent directions explore complementary aspects: amplification techniques and moments accountant methods versus gradient clipping strategies. The paper's use of f-DP and shifted interpolation connects it to the amplification leaf's advanced accounting methods, while its focus on Noisy-FedAvg and Noisy-FedProx links it to the clipping leaf's noise perturbation strategies. The taxonomy's scope and exclude notes clarify that this work belongs in theoretical analysis rather than pure algorithm design, distinguishing it from the 'Federated Learning Algorithm Design with Differential Privacy' branch.

Among twenty-three candidates examined across three contributions, none were identified as clearly refuting the paper's claims. The first contribution (convergent privacy for Noisy-FedAvg) examined nine candidates with zero refutable matches; the second (Noisy-FedProx with constant lower bound) examined ten candidates with zero refutable matches; the third (f-DP framework with shifted interpolation) examined four candidates with zero refutable matches. This suggests that within the limited search scope, the specific combination of f-DP analysis, shifted interpolation, and convergent bounds for these two algorithms appears relatively unexplored. However, the search examined only top-K semantic matches and citations, not the entire literature.

Based on the limited analysis of twenty-three candidates, the work appears to occupy a distinct position within convergence-privacy trade-off research. The absence of refutable prior work among examined candidates suggests novelty in the specific technical approach, though the search scope does not cover all possible related work in privacy accounting or federated optimization. The taxonomy context indicates this contribution extends an active theoretical research direction rather than opening an entirely new area.

This paper presents **3 main contributions**, each analyzed against relevant prior work:

Contribution 1: Convergent privacy analysis for Noisy-FedAvg under non-convex objectives

Description: The authors prove that the privacy budget in Noisy-FedAvg does not diverge as the number of communication rounds increases, achieving a convergent privacy bound for non-convex and smooth objectives. This is the first such convergent privacy analysis for FL-DP methods under non-convex functions.

This contribution was assessed against **9 related papers** from the literature. Papers with potential prior art are analyzed in detail with textual evidence; others receive brief assessments.

1. Differentially private empirical risk minimization with non-convex loss functions

URL: View paper

Brief Assessment

NonConvex Loss ERM[63] focuses on centralized empirical risk minimization with non-convex loss functions using gradient Langevin dynamics, not federated learning with multiple clients performing local updates and communication rounds.

2. Differentially private federated learning on heterogeneous data

URL: View paper

Brief Assessment

Heterogeneous Data DP[62] focuses on privacy-utility trade-offs for federated learning with heterogeneous data using RDP analysis, but does not claim convergent privacy bounds that remain constant as communication rounds increase under non-convex objectives.

3. Convergent Differential Privacy Analysis for General Federated Learning: the -DP Perspective

URL: View paper

Brief Assessment

Convergent DP fDP[1] focuses on the same problem (convergent privacy for Noisy-FedAvg under non-convex objectives) and appears to be the same work or a closely related version, making refutation assessment not applicable in the traditional sense.

4. Personalized federated learning with differential privacy and convergence guarantee

URL: View paper

Brief Assessment

Personalized DP Convergence[6] focuses on personalized federated learning with meta-learning mechanisms and analyzes convergence under both convex and non-convex assumptions, but does not address the specific convergent privacy bound problem for standard Noisy-FedAvg that the original paper tackles using f-DP and shifted interpolation techniques.

5. Providing Differential Privacy for Federated Learning Over Wireless: A Cross-layer Framework

URL: View paper

Brief Assessment

Cross Layer Wireless[64] focuses on wireless physical layer design for over-the-air federated learning using channel noise and cooperative jamming for differential privacy, not on convergent privacy bounds for federated averaging algorithms under non-convex objectives.

6. It's our loss: No privacy amplification for hidden state DP-SGD with non-convex loss

URL: View paper

Brief Assessment

Hidden State NonConvex[66] focuses on showing that hidden state privacy amplification is impossible for general non-convex loss functions in DP-SGD, not on proving convergent privacy bounds for federated averaging methods. The candidate constructs a counter-example loss function to demonstrate tightness of existing DP-SGD analysis, which is a different technical contribution from analyzing privacy convergence in federated learning settings.

7. Concentrated differentially private federated learning with performance analysis

URL: View paper

Brief Assessment

Concentrated DP Performance[69] focuses on zero-concentrated differential privacy (zcdp) with convergence analysis for federated averaging, but does not claim to be the first convergent privacy analysis under non-convex objectives. The candidate's approach differs in using zcdp rather than f-dp analysis and does not explicitly address the divergence problem of privacy budgets that the original paper tackles.

8. Second-Order Convergence in Private Stochastic Non-Convex Optimization

URL: View paper

Brief Assessment

Second Order Convergence[65] focuses on finding second-order stationary points (SOSP) in differentially private stochastic non-convex optimization, not on federated learning privacy convergence bounds. The candidate addresses a fundamentally different problem setting without federated averaging.

9. Faster Convergence on Differential Privacy-Based Federated Learning

URL: View paper

Brief Assessment

Faster Convergence DP[68] focuses on improving convergence speed through modified local objective functions, not on proving convergent privacy bounds. The candidate does not address privacy budget convergence analysis under non-convex objectives.

Contribution 2: Convergent privacy analysis for Noisy-FedProx with constant lower bound

Description: The authors demonstrate that the proximal regularization term in Noisy-FedProx enables privacy to converge to a stable constant lower bound, showing that well-designed local regularization can achieve both optimization and privacy benefits in FL-DP.

This contribution was assessed against **10 related papers** from the literature. Papers with potential prior art are analyzed in detail with textual evidence; others receive brief assessments.

1. Federated Binary Matrix Factorization using Proximal Optimization

URL: View paper

Brief Assessment

Federated Binary Factorization[54] focuses on binary matrix factorization using proximal operators for aggregation, not on differential privacy analysis or privacy convergence bounds in federated learning frameworks.

2. Privacy-Preserving On-Screen Activity Recognition via One-Shot Federated Learning

URL: View paper

Brief Assessment

On Screen Activity[59] focuses on privacy-preserving on-screen activity recognition using one-shot federated learning, not on theoretical privacy analysis of FedProx with proximal regularization achieving stable privacy bounds.

3. Differentially private federated learning with local regularization and sparsification

URL: View paper

Brief Assessment

[Final Audit Failure] The model insisted on a refutation claim but failed to provide verifiable evidence after multiple retries. Marked as cannot_refute for safety. Please manually verify the candidate text.

4. Convergent Differential Privacy Analysis for General Federated Learning: the -DP Perspective

URL: View paper

Brief Assessment

Convergent DP fDP[1] analyzes Noisy-FedProx with proximal regularization achieving constant privacy bounds, addressing the same technical contribution. This appears to be the same work rather than prior art.

5. FedCC: Federated Cluster-Aware Contrastive Learning with Adaptive Differential Privacy under non-IID Settings

URL: View paper

Brief Assessment

FedCC Contrastive Learning[58] mentions proximal regularization and adaptive differential privacy but does not provide convergent privacy analysis or demonstrate stable constant lower bounds for privacy in federated learning with differential privacy.

6. A decentralized federated learning-based cancer survival prediction method with privacy protection

URL: View paper

Brief Assessment

Cancer Survival Prediction[57] focuses on applying federated learning to cancer survival prediction with privacy protection, not on theoretical privacy analysis of proximal regularization achieving stable privacy bounds in FL-DP frameworks.

7. Dynamic personalized federated learning with adaptive differential privacy

URL: View paper

Brief Assessment

Dynamic Personalized Adaptive[51] focuses on personalized federated learning with adaptive differential privacy mechanisms using Fisher information for dynamic personalization. It does not address proximal regularization achieving stable privacy lower bounds in federated learning with differential privacy, which is the core novelty claim of the original paper.

8. A Robust Pipeline for Differentially Private Federated Learning on Imbalanced Clinical Data using SMOTETomek and FedProx

URL: View paper

Brief Assessment

SMOTETomek FedProx Pipeline[55] focuses on addressing class imbalance in clinical data using SMOTETomek preprocessing and FedProx for non-IID data, not on theoretical privacy analysis or proving convergent privacy bounds for proximal regularization in FL-DP frameworks.

9. Federated Learning Models for Privacy-Preserving AI In Enterprise Decision Systems

URL: View paper

Brief Assessment

Enterprise Decision Systems[53] focuses on federated learning applications in enterprise contexts (healthcare, finance, retail) with emphasis on governance frameworks and sector-specific implementations, not on theoretical privacy convergence analysis or proximal regularization achieving stable privacy lower bounds in FL-DP.

10. Personalized federated learning for individual consumer load forecasting

URL: View paper

Brief Assessment

Consumer Load Forecasting[56] focuses on personalized federated learning for load forecasting with proximal regularization for optimization purposes, not on proving convergent privacy bounds or differential privacy analysis in federated learning frameworks.

Contribution 3: f-DP based worst privacy evaluation framework using shifted interpolation

Description: The authors develop a comprehensive framework for evaluating worst-case privacy in FL-DP methods by combining f-DP analysis with shifted interpolation techniques, providing information-theoretically lossless privacy bounds that can be converted to other DP frameworks.

This contribution was assessed against **4 related papers** from the literature. Papers with potential prior art are analyzed in detail with textual evidence; others receive brief assessments.

1. Convergent Differential Privacy Analysis for General Federated Learning: the -DP Perspective

URL: View paper

Brief Assessment

Convergent DP fDP[1] employs f-DP analysis with shifted interpolation techniques for federated learning privacy evaluation, matching the described methodology. This appears to be the same work.

2. DP-FedLoRA: Private Federated Fine-tuning via Low-Rank Adaptation of LLMs

URL: View paper

Brief Assessment

DP-FedLoRA[60] focuses on differentially private federated fine-tuning of large language models via low-rank adaptation, not on f-DP worst-case privacy evaluation frameworks or shifted interpolation techniques for federated learning.

3. Convergent Differential Privacy Analysis for General Federated Learning: the f-DP Perspective

URL: View paper

Brief Assessment

Convergent fDP Perspective[9] addresses federated learning with non-convex objectives using f-DP and shifted interpolation, while the original paper focuses on general reinforcement learning frameworks. The technical domains and problem settings differ fundamentally.

4. Adaptive Noise Calibration for Large-Scale Differentially Private Language Model Training

URL: View paper

Brief Assessment

Adaptive Noise Calibration[61] focuses on adaptive noise calibration for large-scale differentially private language model training, not on f-DP worst-case privacy evaluation using shifted interpolation for federated learning under non-convex objectives.

Appendix: Text Similarity Detection

Textual similarity detection checked 24 papers and found 6 similarity segment(s) across 2 paper(s).

The following **2 paper(s)** were detected to have high textual similarity with the original paper. These may represent different versions of the same work, duplicate submissions, or papers with substantial textual overlap. Readers are advised to verify these relationships independently.

1. Convergent Differential Privacy Analysis for General Federated Learning: the -DP Perspective

Detected in: Core Task (sibling), Contribution: contribution_1, Contribution: contribution_2, Contribution: contribution_3

⚠ **Note**: This paper shows substantial textual similarity with the original paper. It may be a different version, a duplicate submission, or contain significant overlapping content. Please review carefully to determine the nature of the relationship.

2. Convergent Differential Privacy Analysis for General Federated Learning: the f-DP Perspective

Detected in: Core Task (sibling), Contribution: contribution_3

⚠ **Note**: This paper shows substantial textual similarity with the original paper. It may be a different version, a duplicate submission, or contain significant overlapping content. Please review carefully to determine the nature of the relationship.

References

- [0] Convergent Differential Privacy Analysis for General Federated Learning View paper
- [1] Convergent Differential Privacy Analysis for General Federated Learning: the -DP Perspective View paper
- [2] Client-based differential privacy federated learning View paper
- [3] Dp-norm: Differential privacy primal-dual algorithm for decentralized federated learning View paper
- [4] Harmonizing Differential Privacy Mechanisms for Federated Learning: Boosting Accuracy and Convergence View paper
- [5] Universally Harmonizing Differential Privacy Mechanisms for Federated Learning: Boosting Accuracy and Convergence View paper
- [6] Personalized federated learning with differential privacy and convergence guarantee View paper
- [7] Mitigating Privacy-Utility Trade-off in Decentralized Federated Learning via -Differential Privacy View paper
- [8] Differentially private federated learning on non-iid data: Convergence analysis and adaptive optimization View paper
- [9] Convergent Differential Privacy Analysis for General Federated Learning: the f-DP Perspective View paper
- [10] Privacy-Preserving and Reliable Decentralized Federated Learning View paper
- [11] Privacy-Preserving Asynchronous Vertical Federated Learning Algorithms for Multiparty Collaborative Learning View paper
- [12] Privacy-preserving incremental ADMM for decentralized consensus optimization View paper
- [13] Local Differential Privacy for Decentralized Online Stochastic Optimization With Guaranteed Optimality and Convergence Speed View paper
- [14] Shuffled model of differential privacy in federated learning View paper
- [15] Differentially private federated learning: Algorithm, analysis and optimization View paper

- [16] Locally differentially private decentralized stochastic bilevel optimization with guaranteed convergence accuracy View paper
- [17] Utility-Enhanced Personalized Privacy Preservation in Hierarchical Federated Learning View paper
- [18] A Scalable Approach for Privacy-Preserving Collaborative Machine Learning View paper
- [19] Federated learning with sparsified model perturbation: Improving accuracy under client-level differential privacy View paper
- [20] Communication-efficient and privacy-aware distributed learning View paper
- [21] Differentially Private and Communication Efficient Collaborative Learning View paper
- [22] Robust Constrained Consensus and Inequality-Constrained Distributed Optimization With Guaranteed Differential Privacy and Accurate Convergence View paper
- [23] Noiseless Privacy-Preserving Decentralized Learning View paper
- [24] A differential privacy federated learning framework for accelerating convergence View paper
- [25] Adaptive Local Steps Federated Learning with Differential Privacy Driven by Convergence Analysis View paper
- [26] Performance-Enhanced Federated Learning With Differential Privacy for Internet of Things View paper
- [27] Privcoll: Practical privacy-preserving collaborative machine learning View paper
- [28] Understanding clipping for federated learning: Convergence and client-level differential privacy View paper
- [29] Differentially Private Distributed Algorithms for Aggregative Games With Guaranteed Convergence View paper
- [30] Privacy-preserving federated learning on lattice quantization View paper
- [31] PPCL: Privacy-preserving collaborative learning for mitigating indirect information leakage View paper
- [32] LDP-Fed: Federated learning with local differential privacy View paper
- [33] Federated learning with differential privacy: Algorithms and performance analysis View paper
- [34] Asynchronous federated learning with differential privacy for edge intelligence View paper
- [35] Privacy-Preserving Byzantine-Robust Federated Learning via Blockchain Systems View paper
- [36] A Differential Privacy Federated Learning Scheme Based on Adaptive Gaussian Noise View paper
- [37] Decentralized wireless federated learning with differential privacy View paper
- [38] Distributed privacy-preserving collaborative intrusion detection systems for VANETs View paper
- [39] LEASGD: an Efficient and Privacy-Preserving Decentralized Algorithm for Distributed Learning View paper
- [40] Enforcing privacy in distributed learning with performance guarantees View paper
- [41] Privacy-Preserving Asynchronous Grouped Federated Learning for IoT View paper
- [42] The value of collaboration in convex machine learning with differential privacy View paper
- [43] Enabling trustworthy and scalable collaborative learning systems View paper
- [44] Layered Randomized Quantization for Communication-Efficient and Privacy-Preserving Distributed Learning View paper
- [45] Privacy-Preserving Verifiable Asynchronous Federated Learning View paper
- [46] Privacy-Preserving Federated Learning via System Immersion and Random Matrix Encryption View paper
- [47] Communication and Energy Efficient Wireless Federated Learning With Intrinsic Privacy View paper
- [48] DP-ADMM: ADMM-based distributed learning with differential privacy View paper
- [49] Multi-Stage Asynchronous Federated Learning With Adaptive Differential Privacy View paper
- [50] Privacy preserving collaborative computing: Heterogeneous privacy guarantee and efficient incentive mechanism View paper
- [51] Dynamic personalized federated learning with adaptive differential privacy View paper
- [52] Differentially private federated learning with local regularization and sparsification View paper
- [53] Federated Learning Models for Privacy-Preserving AI In Enterprise Decision Systems View paper
- [54] Federated Binary Matrix Factorization using Proximal Optimization View paper
- [55] A Robust Pipeline for Differentially Private Federated Learning on Imbalanced Clinical Data using SMOTETomek and FedProx View paper
- [56] Personalized federated learning for individual consumer load forecasting View paper
- [57] A decentralized federated learning-based cancer survival prediction method with privacy protection View paper
- [58] FedCC: Federated Cluster-Aware Contrastive Learning with Adaptive Differential Privacy under non-IID Settings View paper
- [59] Privacy-Preserving On-Screen Activity Recognition via One-Shot Federated Learning View paper
- [60] DP-FedLoRA: Private Federated Fine-tuning via Low-Rank Adaptation of LLMs View paper
- [61] Adaptive Noise Calibration for Large-Scale Differentially Private Language Model Training View paper
- [62] Differentially private federated learning on heterogeneous data View paper
- [63] Differentially private empirical risk minimization with non-convex loss functions View paper
- [64] Providing Differential Privacy for Federated Learning Over Wireless: A Cross-layer Framework View paper
- [65] Second-Order Convergence in Private Stochastic Non-Convex Optimization View paper
- [66] It's our loss: No privacy amplification for hidden state DP-SGD with non-convex loss View paper
- [67] Differentially Private Federated Clustering Over Non-IID Data View paper
- [68] Faster Convergence on Differential Privacy-Based Federated Learning View paper
- [69] Concentrated differentially private federated learning with performance analysis View paper