Rob Romijnders
09-Dec-2024

Posters at NeurIPS that seem related to privacy, federated learning, and differential privacy.

https://openreview.net/pdf?id=6izXTVVzoI

Wednesday

Private Stochastic Convex Optimization with Heavy Tails: Near-Optimality from Simple
West Ballroom A-D #6310
Wed 11 Dec 11 a.m. PST — 2 p.m. PST (Bookmark)
https://nips.cc/virtual/2024/poster/93619

Log-concave sampling barrier, https://nips.cc/virtual/2024/poster/94777
East Exhibit Hall A-C #4203
[Abstract]
Wed 11 Dec 11 a.m. PST — 2 p.m. PST
https://openreview.net/pdf?id=XKrSB5a79F
Log-concave Sampling from a Convex Body with a Barrier: a Robust and Unified Dikin Walk

Differentially Private Set Representations
Sarvar Patel · Giuseppe Persiano · Joon Young Seo · Kevin Yeo
West Ballroom A-D #6209
Wed 11 Dec 11 a.m. PST — 2 p.m. PST (Bookmark)
https://nips.cc/virtual/2024/poster/95905

Private Algorithms for Stochastic Saddle Points and Variational Inequalities: Beyond Euclidean Geometry
Raef Bassily · Cristóbal Guzmán · Michael Menart
West Ballroom A-D #6208
Wed 11 Dec 11 a.m. PST — 2 p.m. PST (Bookmark)
https://nips.cc/virtual/2024/poster/96341

Unified Mechanism-Specific Amplification by Subsampling and Group Privacy Amplification
Jan Schuchardt · Mihail Stoian · Arthur Kosmala · Stephan Günnemann
West Ballroom A-D #6210
Wed 11 Dec 11 a.m. PST — 2 p.m. PST (Bookmark)

Exactly Minimax-Optimal Locally Differentially Private Sampling
West Ballroom A-D #6204
Wed 11 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)
https://nips.cc/virtual/2024/poster/96070

On Differentially Private U Statistics

Kamalika Chaudhuri · Po-Ling Loh · Shourya Pandey · Purnamrita Sarkar
West Ballroom A-D #6309
Wed 11 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)
https://nips.cc/virtual/2024/poster/92970

LLM Dataset Inference: Did you train on my dataset?
Pratyush Maini · Hengrui Jia · Nicolas Papernot · Adam Dziedzic
West Ballroom A-D #6205
Wed 11 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)
https://nips.cc/virtual/2024/poster/95944

Private Edge Density Estimation for Random Graphs: Optimal, Efficient and Robust
Hongjie Chen · Jingqiu Ding · Yiding Hua · David Steurer
West Ballroom A-D #6200
Wed 11 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)
https://nips.cc/virtual/2024/poster/96671

Prior-itizing Privacy: A Bayesian Approach to Setting the Privacy Budget in Differential Privacy
Zeki Kazan · Jerome Reiter
West Ballroom A-D #6209
Wed 11 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

Nearly Tight Black-Box Auditing of Differentially Private Machine Learning
Meenatchi Sundaram Muthu Selva Annamalai · Emiliano De Cristofaro
West Ballroom A-D #6208
Wed 11 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

A Huber Loss Minimization Approach to Mean Estimation under User-level Differential Privacy
Puning Zhao · Lifeng LAI · Li Shen · Qingming Li · Jiafei Wu · Zhe Liu
West Ballroom A-D #6207
Wed 11 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

Reimagining Mutual Information for Enhanced Defense against Data Leakage in Collaborative Inference
Lin Duan · Jingwei Sun · Jinyuan Jia · Yiran Chen · Maria Gorlatova
West Ballroom A-D #6210
Wed 11 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

Differential Privacy in Scalable General Kernel Learning via K-means Nystr{\"o}m Random Features
Bonwoo Lee · Jeongyoun Ahn · Cheolwoo Park
West Ballroom A-D #6206
Wed 11 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

Differentially Private Optimization with Sparse Gradients

Badih Ghazi · Cristóbal Guzmán · Pritish Kamath · Ravi Kumar · Pasin Manurangsi
West Ballroom A-D #6100
Wed 11 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

HEPrune: Fast Private Training of Deep Neural Networks With Encrypted Data Pruning
Yancheng Zhang · Mengxin Zheng · Yuzhang Shang · Xun Chen · Qian Lou
West Ballroom A-D #6310
Wed 11 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

Privacy without Noisy Gradients: Slicing Mechanism for Generative Model Training
Kristjan Greenewald · Yuancheng Yu · Hao Wang · Kai Xu
West Ballroom A-D #6101
Wed 11 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

Sample-Efficient Private Learning of Mixtures of Gaussians
Hassan Ashtiani · Mahbod Majid · Shyam Narayanan
West Ballroom A-D #6202
Wed 11 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

Thursday

Langevin unlearning, https://nips.cc/virtual/2024/poster/96754
West Ballroom A-D #6102 [Abstract]
Thu 12 Dec 11 a.m. PST — 2 p.m. PST
https://arxiv.org/pdf/2401.10371

Reconstruction Attacks on Machine Unlearning: Simple Models are Vulnerable
West Ballroom A-D #6204
Thu 12 Dec 11 a.m. PST — 2 p.m. PST (Bookmark)
https://nips.cc/virtual/2024/poster/94032

Efficient and Private Marginal Reconstruction with Local Non-Negativity
West Ballroom A-D #6205
Thu 12 Dec 11 a.m. PST — 2 p.m. PST (Bookmark)
https://nips.cc/virtual/2024/poster/93838

Noise-Aware Differentially Private Regression via Meta-Learning
Ossi Räisä · Stratis Markou · Matthew Ashman · Wessel Bruinsma · Marlon Tobaben · Antti Honkela · Richard Turner

West Ballroom A-D #6101
Thu 12 Dec 11 a.m. PST — 2 p.m. PST (Bookmark)

PrivacyLens: Evaluating Privacy Norm Awareness of Language Models in Action
Yijia Shao · Tianshi Li · Weiyan Shi · Yanchen Liu · Diyi Yang
West Ballroom A-D #6103
Thu 12 Dec 11 a.m. PST — 2 p.m. PST (Bookmark)

Continual Counting with Gradual Privacy Expiration
Joel Daniel Andersson · Monika Henzinger · Rasmus Pagh · Teresa Anna Steiner · Jalaj Upadhyay
West Ballroom A-D #6203
[Abstract]
Thu 12 Dec 11 a.m. PST — 2 p.m. PST
https://nips.cc/virtual/2024/poster/94923

Instance-Optimal Private Density Estimation in the Wasserstein Distance
Vitaly Feldman · Audra McMillan · Satchit Sivakumar · Kunal Talwar
West Ballroom A-D #6100
Thu 12 Dec 11 a.m. PST — 2 p.m. PST (Bookmark)
https://nips.cc/virtual/2024/poster/96229

Attack-Aware Noise Calibration for Differential Privacy
Bogdan Kulynych · Juan Gomez · Georgios Kaissis · Flavio Calmon · Carmela Troncoso
West Ballroom A-D #6303
Thu 12 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)
https://nips.cc/virtual/2024/poster/94073

SPEAR: Exact Gradient Inversion of Batches in Federated Learning
Dimitar I. Dimitrov · Maximilian Baader · Mark Müller · Martin Vechev
West Ballroom A-D #6301
Thu 12 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

Faster Differentially Private Top-k
Selection: A Joint Exponential Mechanism with Pruning
Hao WU · Hanwen Zhang
West Ballroom A-D #6305
Thu 12 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

Public-data Assisted Private Stochastic Optimization: Power and Limitations
Enayat Ullah · Michael Menart · Raef Bassily · Cristóbal Guzmán · Raman Arora
West Ballroom A-D #6302
Thu 12 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

Scalable DP-SGD: Shuffling vs. Poisson Subsampling

Lynn Chua · Badih Ghazi · Pritish Kamath · Ravi Kumar · Pasin Manurangsi · Amer Sinha · Chiyuan Zhang
West Ballroom A-D #6309
Thu 12 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

Revisiting Differentially Private ReLU Regression
Meng Ding · Mingxi Lei · Liyang Zhu · Shaowei Wang · Di Wang · Jinhui Xu
West Ballroom A-D #6310
Thu 12 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

Certified Machine Unlearning via Noisy Stochastic Gradient Descent
Eli Chien · Haoyu Wang · Ziang Chen · Pan Li
West Ballroom A-D #6304
Thu 12 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

On the Computational Complexity of Private High-dimensional Model Selection
Saptarshi Roy · Zehua Wang · Ambuj Tewari
West Ballroom A-D #6306
Thu 12 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

Friday

DOPPLER: Differentially Private Optimizers with Low-pass Filter for Privacy Noise Reduction
https://nips.cc/virtual/2024/poster/93453
West Ballroom A-D #6102
[Abstract]
Fri 13 Dec 11 a.m. PST — 2 p.m. PST

PrivCirNet: Efficient Private Inference via Block Circulant Transformation
Tianshi Xu · Lemeng Wu · Runsheng Wang · Meng Li
West Ballroom A-D #6108
Fri 13 Dec 11 a.m. PST — 2 p.m. PST (Bookmark)

The Limits of Differential Privacy in Online Learning
Bo Li · Wei Wang · Peng Ye
West Ballroom A-D #6000
[Abstract]
Fri 13 Dec 4:30 p.m. PST — 7:30 p.m. PST
https://nips.cc/virtual/2024/poster/96120

PANORAMIA: Privacy Auditing of Machine Learning Models without Retraining

Mishaal Kazmi · Hadrien Lautraite · Alireza Akbari · Qiaoyue Tang · Mauricio Soroco · Tao Wang · Sébastien Gambs · Mathias Lécuyer
West Ballroom A-D #6009
[Abstract] [Project Page]
Fri 13 Dec 11 a.m. PST — 2 p.m. PST
https://nips.cc/virtual/2024/poster/96581

Private Attribute Inference from Images with Vision-Language Models
Batuhan Tömekçe · Mark Vero · Robin Staab · Martin Vechev
West Ballroom A-D #6008
Fri 13 Dec 11 a.m. PST — 2 p.m. PST (Bookmark)
https://nips.cc/virtual/2024/poster/96590

Dual Defense: Enhancing Privacy and Mitigating Poisoning Attacks in Federated Learning
Runhua Xu · Shiqi Gao · Chao Li · James Joshi · Jianxin Li
West Ballroom A-D #6012
Fri 13 Dec 11 a.m. PST — 2 p.m. PST (Bookmark)

On the Benefits of Public Representations for Private Transfer Learning under Distribution Shift
Pratiksha Thaker · Amrith Setlur · Steven Wu · Virginia Smith
West Ballroom A-D #6011
Fri 13 Dec 11 a.m. PST — 2 p.m. PST (Bookmark)

Differentially Private Equivalence Testing for Continuous Distributions and Applications
Or Sheffet · Daniel Omer
West Ballroom A-D #6103
Fri 13 Dec 11 a.m. PST — 2 p.m. PST (Bookmark)

Universal Exact Compression of Differentially Private Mechanisms
Yanxiao Liu · Wei-Ning Chen · Ayfer Ozgur · Cheuk Ting Li
West Ballroom A-D #6010
Fri 13 Dec 11 a.m. PST — 2 p.m. PST (Bookmark)

Private Geometric Median
Mahdi Haghifam · Thomas Steinke · Jonathan Ullman
West Ballroom A-D #6106
Fri 13 Dec 11 a.m. PST — 2 p.m. PST (Bookmark)

Instance-Specific Asymmetric Sensitivity in Differential Privacy
David Durfee
West Ballroom A-D #5902
Fri 13 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)
https://nips.cc/virtual/2024/poster/96679

Dimension-free Private Mean Estimation for Anisotropic Distributions
Yuval Dagan · Michael Jordan · Xuelin Yang · Lydia Zakynthinou · Nikita Zhivotovskiy
West Ballroom A-D #6005
Fri 13 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)
https://nips.cc/virtual/2024/poster/93891

Differentially Private Reinforcement Learning with Self-Play
Dan Qiao · Yu-Xiang Wang
West Ballroom A-D #6002
Fri 13 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)\

Faster Algorithms for User-Level Private Stochastic Convex Optimization
Andrew Lowy · Daogao Liu · Hilal Asi
West Ballroom A-D #6004
Fri 13 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

Auditing Privacy Mechanisms via Label Inference Attacks
Róbert Busa-Fekete · Travis Dick · Claudio Gentile · Andres Munoz Medina · Adam Smith · Marika Swanberg
West Ballroom A-D #5900
Fri 13 Dec 4:30 p.m. PST — 7:30 p.m. PST (Bookmark)

Unknown

SILENCE: Protecting privacy in offloaded speech understanding on resource-constrained devices
https://nips.cc/virtual/2024/poster/93343

Noisy Dual Mirror Descent: A Near Optimal Algorithm for Jointly-DP Convex Resource Allocation
Du Chen · Geoffrey A. Chua
https://nips.cc/virtual/2024/poster/96542

Locally Private and Robust Multi-Armed Bandits
Xingyu Zhou · Komo(Wei) ZHANG
https://nips.cc/virtual/2024/poster/96196

On Differentially Private Subspace Estimation in a Distribution-Free Setting
Eliad Tsfadia
[Abstract]