论文收集（88篇）

- 深度学习（15篇）
  - SGD（5次）
    - ccs2016：Deep Learning with Differential Privacy
    - ijcai2019: Heterogeneous Gaussian Mechanism: Preserving Differential Privacy in Deep Learning with Provable Robustness
    - nips2020: Auditing Differentially Private Machine Learning: How Private is Private SGD?*
    - icml2018：Entropy-SGD optimizes the prior of a PAC-Bayes bound: Generalization properties of Entropy-SGD and data-dependent priors
    - icde2019：Collecting and Analyzing Multidimensional Data with Local Differential Privacy
  - DNN（3次）
    - icml2019: Scalable Differential Privacy with Certified Robustness in Adversarial Learning
    - kdd2019：Not Just Privacy: Improving Performance of Private Deep Learning in Mobile Cloud
    - aaai2019：Private Model Compression via Knowledge Distillation
  - GANs（2次）
    - nips2020: GS-WGAN: A Gradient-Sanitized Approach for Learning Differentially Private Generators
    - nips2019：Generalization in Generative Adversarial Networks: A Novel Perspective from Privacy Protection
  - 防御增强鲁棒性（1次）
    - S&P2019： Certified Robustness to Adversarial Examples with Differential Privacy
  - 针对深度学习特性改进差分隐私（1次）
    - S&P2019：Differentially Private Model Publishing for Deep Learning
  - 差分隐私+深度学习中的自动编码（1次）
    - aaai2016：Differential Privacy Preservation for Deep Auto-Encoders: An Application of Human Behavior Prediction
  - 差分隐私+推荐系统（2次）
    - aaai2018：Personalized Privacy-Preserving Social Recommendation
    - aaai2018：Privacy Preserving Point-of-interest Recommendation Using Decentralized Matrix Factorization
- 机器学习（50篇）
  - SGD（7次）
    - kdd2018：Concentrated Differentially Private Gradient Descent with Adaptive per-Iteration Privacy Budget
    - nips2018：cpSGD: Communication-efficient and differentially-private distributed SGD
    - nips2020：Privacy Amplification via Random Check-Ins
    - sigmod2016：Bolt-on Differential Privacy for Scalable Stochastic Gradient Descent-based Analytics
    - s&p2020：The Value of Collaboration in Convex Machine Learning with Differential Privacy
    - ijcai2017:Efficient Private ERM for Smooth Objectives
    - aaai2020：Differentially Private Learning with Small Public Data
  - 评价（1次）
    - USENIX Security2019：Evaluating Differentially Private Machine Learning in Practice
  - 在线学习（2次）
    - icml2017：The Price of Differential Privacy for Online Learning
    - nips2019：User-Specified Local Differential Privacy in Unconstrained Adaptive Online Learning
  - 差分隐私+松散线性回归（1次）
    - icml2019：On Sparse Linear Regression in the Local Differential Privacy Model
  - 差分隐私加贝叶斯（3次）
    - icml2020：Bayesian Differential Privacy for Machine Learning
    - aaai2016：On the Differential Privacy of Bayesian Inference
    - nips2017:Differentially Private Bayesian Learning on Distributed Data
  - 聚类（2次）
    - icde2016:Private Spatial Data Aggregation in the Local Setting
    - nips2020：Differentially Private Clustering: Tight Approximation Ratios
  - 贝叶斯网（2次）
    - icde2016:Differentially Private Multi-Party High-Dimensional Data Publishing
    - nips2018:Differentially Private Bayesian Inference for Exponential Families
  - 利用ml解决隐私配置问题（1次）
    - kdd2016:Convex Optimization for Linear Query Processing under Approximate Differential Privacy
  - 近端梯度下降（1次）
    - kdd2017:Privacy-Preserving Distributed Multi-Task Learning with Asynchronous Updates
  - 重新鉴定攻击（1次）
    - kdd2020:Re-identification Attack to Privacy-Preserving Data Analysis with Noisy Sample-Mean
  - ERM（经验风险最小化）（5次）
    - nips2017:Differentially Private Empirical Risk Minimization Revisited: Faster and More General
    - nips2018:Empirical Risk Minimization in Non-interactive Local Differential Privacy: Efficiency and High Dimensional Case
    - aaai2019:Differentially Private Empirical Risk Minimization with Smooth Non-Convex Loss Functions: A Non-Stationary View
    - aaai2020：Differentially Private Learning with Small Public Data
    - ijcai2017:Efficient Private ERM for Smooth Objectives
  - 变化点检测（1次）
    - nips2018:Differentially Private Change-Point Detection
  - k-means（1次）
    - nips2018:Differentially Private k-Means with Constant Multiplicative Error
  - Dp-learning算法设计（1次）
    - nips2018:Model-Agnostic Private learning
  - 利用ml对差分隐私进行改进（1次）
    - nips2018:Privacy Amplification by Subsampling: Tight Analyses via Couplings and Divergences
  - 基于满足差分隐私的某一方法并对其改进（1次）
    - nips2019：Differentially Private Bagging: Improved utility and cheaper privacy than subsample-and-aggregate
  - 新机制设计（1次）
    - nips2019：KNG: The K-Norm Gradient Mechanism
  - 贝叶斯+线性回归（1次）
    - nips2019：Differentially Private Bayesian Linear Regression
  - 马尔可夫网/马尔可夫随机场（2次）
    - icml2020:Privately Learning Markov Random Fields
    - nips2019：Differentially Private Markov Chain Monte Carlo
  - 联邦学习（2次）
    - nips2020：Inverting Gradients - How easy is it to break privacy in federated learning?
    - aaai2020：Federated Latent Dirichlet Allocation: A Local Differential Privacy Based Framework
  - 差分隐私在机器学习理论下的探讨（1次）
    - s&p2017：Is Interaction Necessary for Distributed Private Learning?
  - 主成分分析（2次）
    - aaai2016：Wishart Mechanism for Differentially Private Principal Components Analysis
    - ijcai2019:Principal Component Analysis in the Local Differential Privacy Model
  - 高维数据分析（1次）
    - aaai2020:A Knowledge Transfer Framework for Differentially Private Sparse Learning
  - DP+ML理论研究（2次）
    - aaai2020：Differentially Private and Fair Classification via Calibrated Functional Mechanism
    - ijcai2019：Lower Bound of Locally Differentially Private Sparse Covariance Matrix Estimation
  - 成对学习问题（1次）
    - aaai2020:Pairwise Learning with Differential Privacy Guarantees
  - 梯度增强决策树（1次）
    - aaai2020:Privacy-Preserving Gradient Boosting Decision Trees
  - 防御攻击（1次）
    - ijcai2019:Data Poisoning against Differentially-Private Learners: Attacks and Defenses
  - LDA（潜在迪利克雷分配）（2次）
    - aaai2020：Federated Latent Dirichlet Allocation: A Local Differential Privacy Based Framework
    - ijcai2019:On Privacy Protection of Latent Dirichlet Allocation Model Training
  - 松散学习方法（1次）
    - ijcai2019：Differentially Private Iterative Gradient Hard Thresholding for Sparse Learning
  - 优化（算法、长尾数据随机凸优化、隐私非凸优化）（4次）
    - icml2020：On Differentially Private Stochastic Convex Optimization with Heavy-tailed Data
    - icml2020：Oracle Efficient Private Non-Convex Optimization
    - nips2019：Private Stochastic Convex Optimization with Optimal Rates
    - ijcai2019:Privacy-preserving Stacking with Application to Cross-organizational Diabetes Prediction
- 分布式（17篇）
  - SGD（4次）
    - nips2018：cpSGD: Communication-efficient and differentially-private distributed SGD
    - nips2020：Privacy Amplification via Random Check-Ins
    - sigmod2016：Bolt-on Differential Privacy for Scalable Stochastic Gradient Descent-based Analytics
    - s&p2020：The Value of Collaboration in Convex Machine Learning with Differential Privacy
  - GANs（1次）
    - nips2020：GS-WGAN: A Gradient-Sanitized Approach for Learning Differentially Private Generators
  - 乘法交替方向（1次）
    - icml2018：Improving the Privacy and Accuracy of ADMM-Based Distributed Algorithms
  - shuffled-model（1次）
    - icml2020：Private Counting from Anonymous Messages: Near-Optimal Accuracy with Vanishing Communication Overhead
  - 聚类（1次）
    - icde2016：Private Spatial Data Aggregation in the Local Setting
  - 近端梯度下降（1次）
    - kdd2017：Privacy-Preserving Distributed Multi-Task Learning with Asynchronous Updates
  - DNN（2次）
    - kdd2019：Not Just Privacy: Improving Performance of Private Deep Learning in Mobile Cloud
    - aaai2019:Private Model Compression via Knowledge Distillation
  - 贝叶斯（1次）
    - nips2017：Differentially Private Bayesian Learning on Distributed Data
  - k-means（1次）
    - nips2018：Differentially Private k-Means with Constant Multiplicative Error
  - 联邦学习（2次）
    - nips2020：Inverting Gradients - How easy is it to break privacy in federated learning?
    - aaai2020:Federated Latent Dirichlet Allocation: A Local Differential Privacy Based Framework
  - 推荐系统（1次）
    - aaai2018：Privacy Preserving Point-of-interest Recommendation Using Decentralized Matrix Factorization
  - 联邦学习+LDA(1次)
    - aaai2020:Federated Latent Dirichlet Allocation: A Local Differential Privacy Based Framework
  - 针对某一方面的DP设计（1次）
    - ijcai2020：Differential Privacy for Stackelberg Games
  - 成对学习问题（1次）
    - aaai2020：Pairwise Learning with Differential Privacy Guarantees
- 中心化（17篇）
  - SGD（4次）
    - ccs2016：Deep Learning with Differential Privacy
    - ijcai2019：Heterogeneous Gaussian Mechanism: Preserving Differential Privacy in Deep Learning with Provable Robustness
    - kdd2018：Concentrated Differentially Private Gradient Descent with Adaptive per-Iteration Privacy Budget
    - nips2020：Auditing Differentially Private Machine Learning: How Private is Private SGD?*
  - DNN（1次）
    - icml2019：Scalable Differential Privacy with Certified Robustness in Adversarial Learning
  - GANs（1次）
    - nips2020：GS-WGAN: A Gradient-Sanitized Approach for Learning Differentially Private Generators
  - 防御增强鲁棒性（1次）
    - s&p2019：Certified Robustness to Adversarial Examples with Differential Privacy
  - 针对深度学习改进差分隐私（1次）
    - s&p2019：Differentially Private Model Publishing for Deep Learning
  - k-means（1次）
    - nips2018：Differentially Private k-Means with Constant Multiplicative Error
  - ERM（1次）
    - nips2018：Empirical Risk Minimization in Non-interactive Local Differential Privacy: Efficiency and High Dimensional Case
  - DP-learning算法设计（1次）
    - nips2018：Model-Agnostic Private Learning
  - 利用某一方法对差分隐私进行改进（2次）
    - nips2018：Privacy Amplification by Subsampling: Tight Analyses via Couplings and Divergences
    - nips2019：Differentially Private Bagging: Improved utility and cheaper privacy than subsample-and-aggregate
  - DP机制（1次）
    - nips2019：KNG: The K-Norm Gradient Mechanism
  - 在线学习（1次）
    - nips2019：User-Specified Local Differential Privacy in Unconstrained Adaptive Online Learning
  - 深度学习中的自动化编码（1次）
    - aaai2016：Differential Privacy Preservation for Deep Auto-Encoders: An Application of Human Behavior Prediction
  - 推荐系统（1次）
    - aaai2018：Personalized Privacy-Preserving Social Recommendation
- 数据发布（6篇）
  - 张量分解（1次）
    - nips2016：Online and Differentially-Private Tensor Decomposition
  - 无向图（1次）
    - icml2017：Differentially Private Learning of Undirected Graphical Models Using Collective Graphical Models
  - 差分隐私+贝叶斯网（1次）
    - icde2016：Differentially Private Multi-Party High-Dimensional Data Publishing
  - DNN（1次）
    - kdd2019：Not Just Privacy: Improving Performance of Private Deep Learning in Mobile Cloud
  - 关键基础设施网络数据发布（1次）
    - ijcai2019：Privacy-Preserving Obfuscation of Critical Infrastructure Networks
  - 若干个集合并集（1次）
    - icml2020：Differentially Private Set Union
- 其他方面
  - 对抗性分类（1次）
    - ndss2020：Adversarial Classification Under Differential Privacy
  - 敏感度（1次）
    - icml2017：Pain-Free Random Differential Privacy with Sensitivity Sampling
  - 指数机制（1次）
    - icml2019：Benefits and Pitfalls of the Exponential Mechanism with Applications to Hilbert Spaces and Functional PCA
  - 平面对变形（1次）
    - icml2019：Differentially Private Learning of Geometric Concepts
  - 泊松子采样（1次）
    - icml2019：Poisson Subsampled Renyi Differential Privacy
  - 频谱算法（1次）
    - icml2020：An end-to-end Differentially Private Latent Dirichlet Allocation Using a Spectral Algorithm
  - 理论研究（3次）
    - icml2020：Sharp Composition Bounds for Gaussian Difffferential Privacy via Edgeworth Expansion
    - ccs2018：Tight on Budget? Tight Bounds for r-Fold Approximate Differential Privacy
    - aaai2017：Cleaning the Null Space: A Privacy Mechanism for Predictors
  - 矩阵层面对差分隐私改进（1次）
    - ccs2019：MVG Mechanism: Differential Privacy under Matrix-Valued Query
  - 根据ERM选择DP等级（1次）
    - nips2017：Accuracy First: Selecting a Differential Privacy Level for Accuracy-Constrained ERM
  - Renyi差分隐私（1次）
    - nips2017：Rényi Differential Privacy Mechanisms for Posterior Sampling
  - 假设选择（1次）
    - nips2019：Private Hypothesis Selection
  - 实例最优算法（1次）
    - nips2020：Instance-optimality in differential privacy via approximate inverse sensitivity mechanisms
  - 梯度扰动的证明与研究（1次）
    - ijcai2020：Gradient Perturbation is Underrated for Differentially Private Convex Optimization