上海交通大学自动化系
Department of Automation
Shanghai Jiao Tong University

系统控制与信息处理教育部重点实验室
Key Laboratory of System Control and Information Processing, Ministry of Education

学术报告会

时间：2024年8月1日 10:00
地点：电信群楼2-410会议室

Towards Differentially Private Deep Learning under Hidden State Assumption

Ass. Prof. Chen Liu
City University of Hong Kong

摘要:

Deep neural networks possess remarkable power, yet they also have the potential to compromise the privacy of sensitive training data. Differential privacy (DP), on the other hand, provides a robust mathematical framework for releasing statistical information about datasets while safeguarding the privacy of individual data subjects. However, within the realm of deep learning, it is challenging to enhance differential privacy due to the high-dimensionality and non-convex nature of the loss function.

In this talk, we present a novel approach called differentially private stochastic block coordinate descent (DP-SBCD) for training neural networks with provable guarantees of differential privacy under the hidden state assumption. Our methodology incorporates Lipschitz neural networks and decomposes the training process of the neural network into sub-problems, each corresponding to the training of a specific layer. By doing so, we extend the analysis of differential privacy under the hidden state assumption to encompass non-convex problems. Furthermore, in contrast to existing methods, we adopt a novel approach by utilizing calibrated noise sampled from adaptive distributions, yielding improved empirical trade-offs between utility and privacy.

简介:

Chen Liu is an Assistant Professor from the Department of Computer Science, City University of Hong Kong. He obtained his Ph.D. degree in 2022 from EPFL under the supervision of Prof. Sabine Süsstrunk and Dr. Mathieu Salzmann. His Ph.D. study was partially supported by Microsoft Research Scholarship as well. Previously, he obtained his master’ s and bachelor’ s degrees from EPFL and Tsinghua University, both in computer science. His research focuses on machine learning, optimization, adversarial robustness and differential privacy. More information is available on his website: liuchen1993.cn.