1143-91-561 **Tao Zhang*** (tz636@nyu.edu), 10.081B, 10th Floor, 2 Metrotech, Brooklyn, NY 11201, and **Quanyan Zhu**. *Mechanism Design of Differential Privacy of Machine Learning Algorithms over Networks.*

Differential privacy offers a strong guaranteed bound on the privacy leakage that a data owner (DO) may incur in machine learning processes. Improving the differential privacy of learning algorithms is often at odds with the performance of machine learning. DOs usually have natural privacy concerns while the machine learner (MLR) prefers guaranteed learning performances. Optimally addressing the tradeoff between privacy and performance is pivotal to establish a sustainable collaboration between DOs and MLR. To this end, we consider a problem of centralized machine learning algorithm using data collaboratively gathered from a group of DOs and propose a mechanism design approach to construct a framework of differentially private machine learning when the incentives of DOs and MLRs, respectively, to preserve privacy and improve performance are misaligned. First, each DO has a private valuation of the mechanism and reports her privacy budget to the MLR. After receiving all the reports, the MLR allocates a privacy budget to each DO. The MLR is the mechanism designer, who aims to maximize the utility of the learning outputs while providing acceptable privacy level for the DOs based on their valuation by choosing an optimal privacy budget allocation rule and an optimal pricing rule. (Received August 21, 2018)