A Practical Approach to Differential Private Learning
K.L. van der Veen

Abstract

Applying differential private learning to real-world data is currently unpractical. Differential privacy (DP) introduces extra hyper-parameters for which no thorough good practices exist, while manually tuning these hyper-parameters on private data results in low privacy guarantees. Furthermore, the exact guarantees provided by differential privacy for machine learning models are not well understood. Current approaches use undesirable post-hoc privacy attacks on models to assess privacy guarantees. To improve this situation, we introduce three tools to make DP machine learning more practical. First, two sanity checks for differential private learning are proposed. These sanity checks can be carried out in a centralized manner before training, do not involve training on the actual data and are easy to implement. Additionally, methods are proposed to reduce the effective number of tuneable privacy parameters by making use of an adaptive clipping bound. Lastly, existing methods regarding large batch training and differential private learning are combined. It is demonstrated that this combination improves model performance within a constant privacy budget.