CT Advanced Computing Center (CACC) Security Seminar Series 2022-2023

Speaker: Marten van Dijk
Date: Wednesday, February 8, 2023
Time: 1:00pm - 2:30pm
Location: ITE 401
Meeting Link : https://uconn-cmr.webex.com/uconn-cmr/j.php?MTID=mf5e70e87ecd7c0b61a5a799382f428ef
Meeting number (access code): 2620 057 2269
Meeting password: S2m536sFJab

Generalizing DP-SGD with Shuffling and Batching Clipping

Classical differential private DP-SGD implements individual clipping with random subsampling, which forces a mini-batch SGD approach. We provide a general differential private algorithmic framework that goes beyond DP-SGD and allows any possible first order optimizers (e.g., classical SGD and momentum based SGD approaches) in combination with batch clipping, which clips an aggregate of computed gradients rather than summing clipped gradients (as is done in individual clipping). The framework also admits sampling techniques beyond random subsampling such as shuffling. Our DP analysis follows the f-DP approach in a slightly stronger adversarial model and introduces a new proof technique which allows us to also analyze group privacy. In particular, for E epochs work and groups of size g, we show a simple closed form formula with sqrt{gE} DP dependency for batch clipping with shuffling. This is much better than the previously anticipated linear dependency in g.

Joint work with L. M. Nguyen, N. Nguyen, T. Nguyen, and P. H. Nguyen