FedRAN: Federated Mobile Edge Computing with Differential Privacy

Aashish Gottipati, Alex Stewart, Jiawen Song, Qianlang Chen
University of Utah

Introduction

Problem Setting

- Increased access to powerful compute
  - Apple A14: 6 Core 3.1 GHz processor + Neural Engine
- More users and devices entering the network with 5G
  - Cisco estimates 850 ZB of data at the edge by end of 2021
  - Global data centers are estimated at 20.6 ZB
- Moving towards data driven, software-defined networks
  - Adapt in real time to dynamic environments
  - Quality of Service, slicing, and mobility optimization
- Can we utilize edge compute and data to help realize a data driven network?

How AI and Machine Learning Can Make or Break Our Mobile Privacy


Dmytro Spilka — July 28, 2021

Problem Setting Continued

- Endpoint privacy is essential
    - European Union’s General Data Protection Regulation
- Transferring over the network does not make sense either
- Is there a way we can learn without explicitly transferring data?

FedRAN

- A differentially private FL system to enable a privacy preserving, large scale edge computing ecosystem
- I.e. tap into the vast amounts of edge compute and data without compromising privacy

Background

Federated Learning

- Distributed method for training a model
- I.I.D data is not required
  - Data gathered at end points used to train global model
- Model updates are transferred and aggregated
- Enables access to vast amounts of edge data without straining endpoints

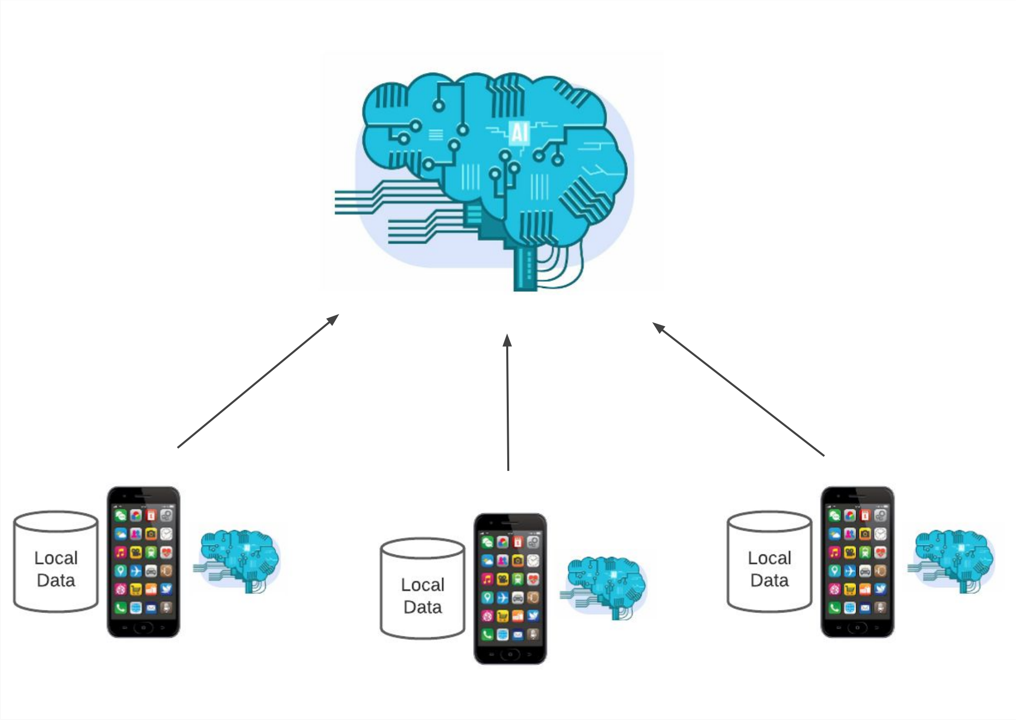

Figure 1: Generic Federated Learning Structure

Why Differential Privacy?

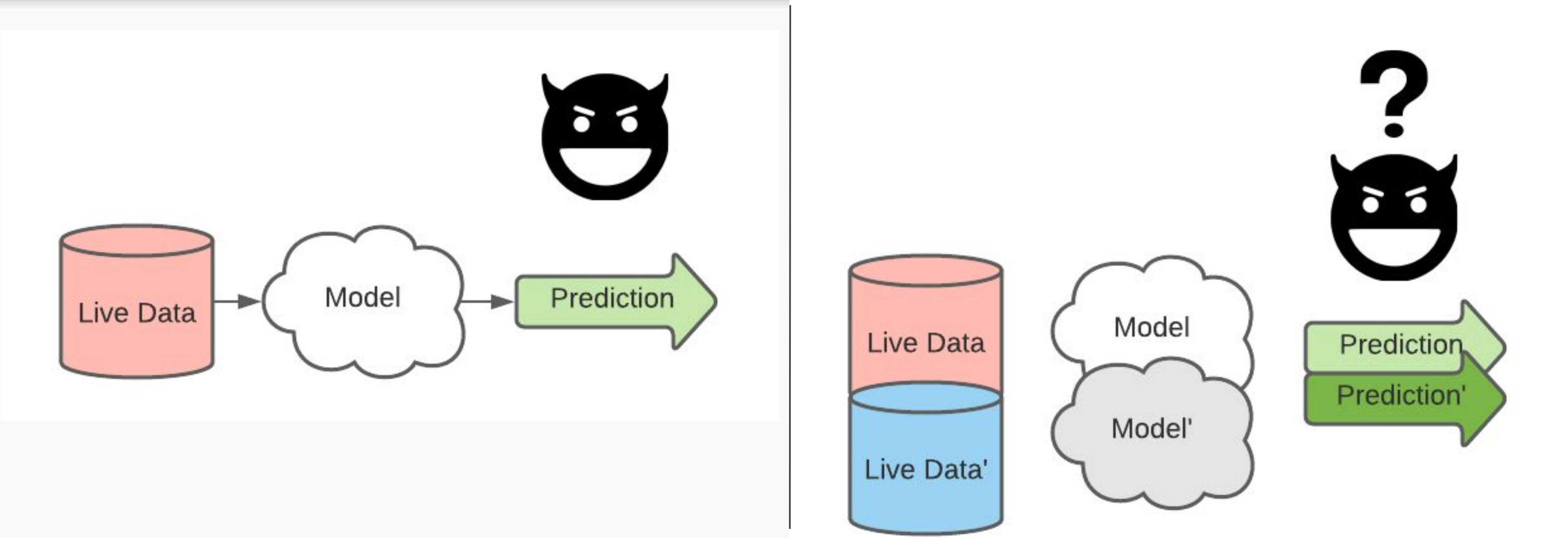

Figure 2: Adversarial Attacks within an FL environment

Differential Privacy

$$\forall X: P[M(x) \in E] \leq e^{\varepsilon} \cdot P[M(x`) \in X] + \delta$$

- "Probability that output distribution differs on single element from Database X"
- Preserves data security by obscuring gradient information with noise
  - Magnitude of noise is tempered via privacy budget ε
- Injected noise is sampled via privacy preserving statistical techniques
  - Laplacian, Exponential, and Gaussian mechanisms

FedRAN Overview

Implementation

- Generic federated learning architecture
- IBM's Federated Learning library to handle network interactions
- Configured FedRAN to run over srsLTE LTE Network
- Differentially private stochastic gradient descent with Tensorflow

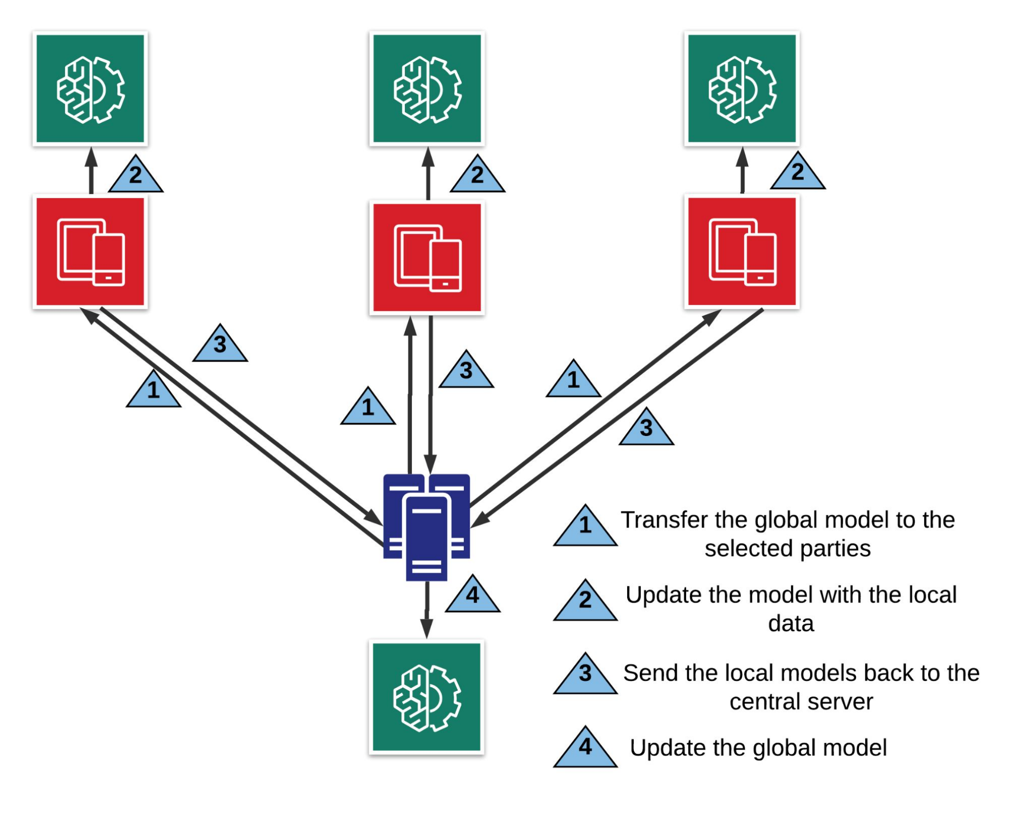

Figure 3: FedRAN Architecture

FedRAN Use Case: Smart Vehicles

- Traffic cone represents unknown foreign object to both cars
- Car 1 learns from Car 2's experience
- Similar framework employed at Tesla

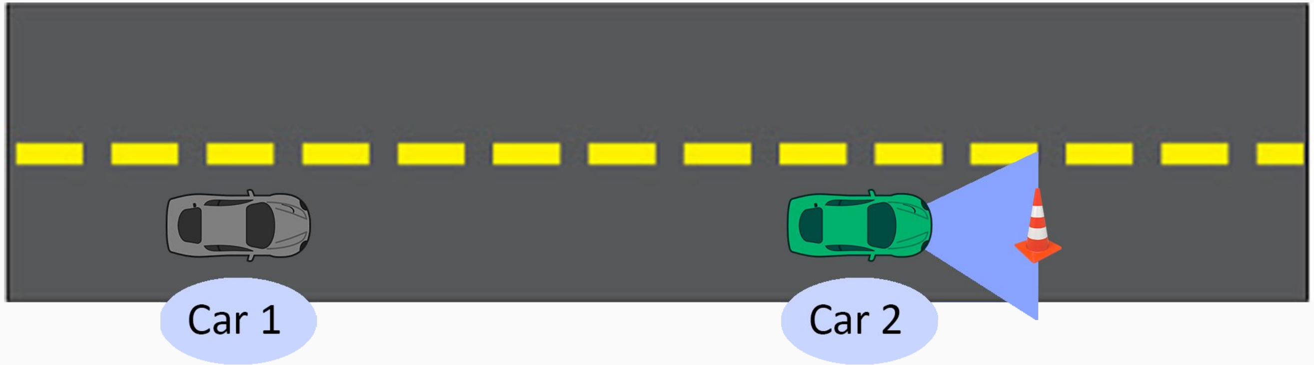

Figure 4: FedRAN Use Case

Evaluation

Evaluation Setup

- Powder Controlled RF Environment
- IBM Federated Learning Agents
- Latest srsLTE release
- Utilized MNIST handwritten digits dataset

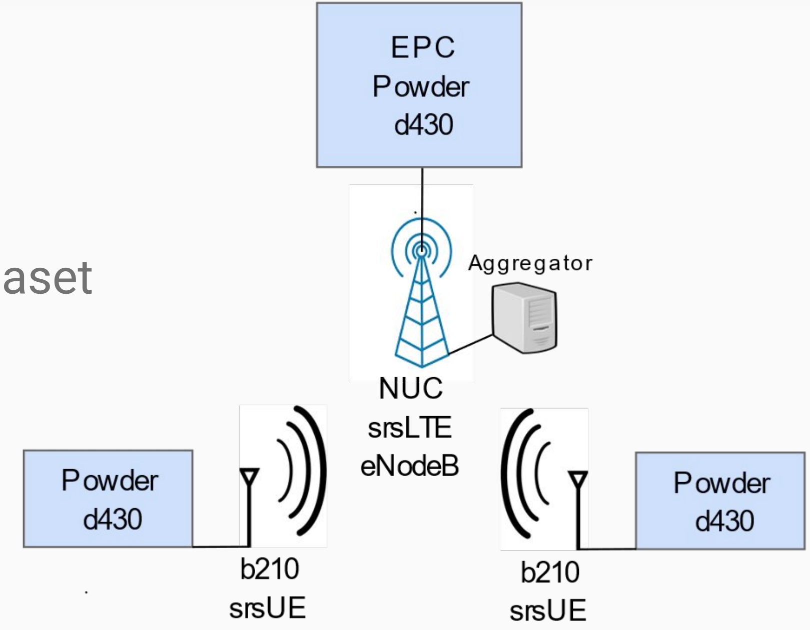

Figure 5: Network Topology

Training Procedure

- CNN implemented in TensorFlow 2.0
    - Kernel size 3 x 3, ReLU activation function, 2 x 2 max pooling, p = 0.5 dropout
- Categorical Cross Entropy Objective Function
- Stochastic Gradient Descent with and without Differential Privacy
- Set global termination classification accuracy to 90%
- Required all clients to participate in each communication round

Local vs. Distributed Model Evaluation Procedure

- Modified client training data by removing entire classes
  - E.g. on client 1, remove 1, 2, 3 and on client 2, remove 4, 5, 6
  - Emulate situation where client only has partial view of underlying distribution
- Train CNN locally and distributively for 60, 180, and 300 epochs
- Record final classification accuracy and CCE loss for each setting

Results

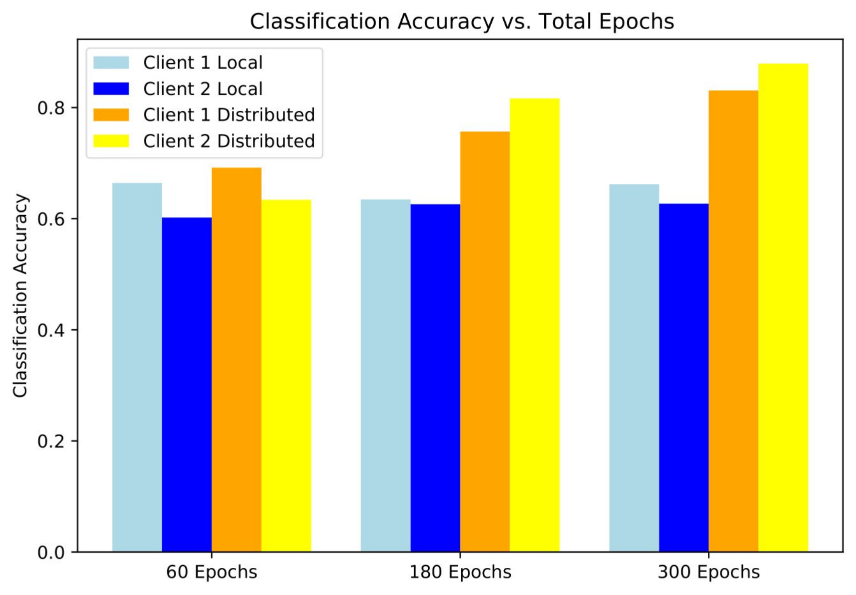

Figure 6: Local vs. Distributed Accuracy

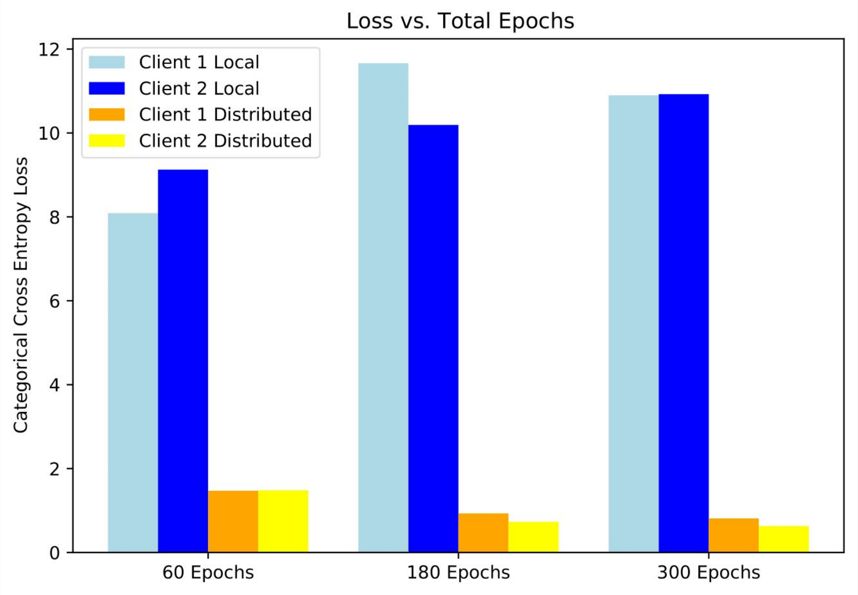

Figure 7: Local vs. Distributed Loss

Differential Privacy Evaluation Procedure

- Client had all image classes restored
- Trained CNN distributively for 60 epochs
- Utilized SGD DP variant with varying privacy budgets
- Recorded training accuracy across epochs for each privacy setting

Results

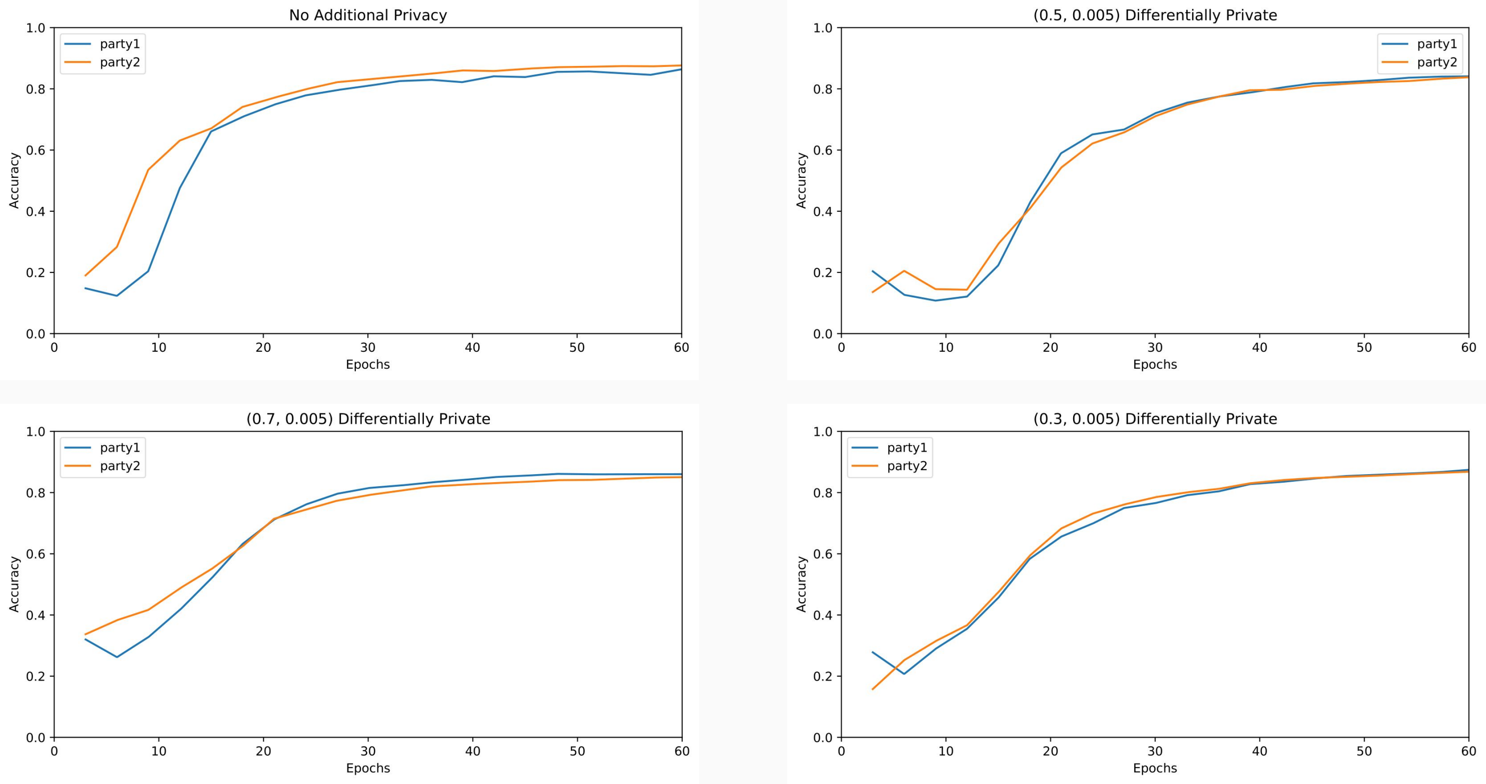

Figure 8: Training Accuracy with Varying Privacy Budgets

Summary

- Presented and validated a differentially private FL system at the mobile edge
- Enables a privacy preserving, large scale edge computing ecosystem
- Exploit advancements in compute to realize a data driven network
- Packaged FedRAN as a Powder profile to enable others to explore applications of FL in a real RF setting

References

- Aashish Gottipati, Alex Stewart, Jiawen Song, and Qianlang Chen. 2021. FedRAN Controlled RF Powder Profile. https://www.powderwireless.net/p/40deff44-9e62-11eb-b1eb-e4434b2381fc
- Cynthia Dwork, Aaron Roth, et al. 2014. The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science 9, 3-4 (2014), 211--407.
- H. Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Agüera y Arcas. 2017. Communication-Efficient Learning of Deep Networks from Decentralized Data. arXiv:1602.05629 [cs.LG]
- Heiko Ludwig, Nathalie Baracaldo, Gegi Thomas, Yi Zhou, Ali Anwar, Shashank Rajamoni, Yuya Ong, Jayaram Radhakrishnan, Ashish Verma, Mathieu Sinn, et al. 2020. IBM Federated Learning: an Enterprise Framework White Paper V0. 1. arXiv preprint arXiv:2007.10987 (2020).
- Ismael Gomez-Miguelez, Andres Garcia-Saavedra, Paul D Sutton, Pablo Serrano, Cristina Cano, and Doug J Leith. 2016. srsLTE: an open-source platform for LTE evolution and experimentation. In Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization. ACM, 25--32.
- Joe Breen, Andrew Buffmire, Jonathon Duerig, Kevin Dutt, Eric Eide, Mike Hibler, David Johnson, Sneha Kumar Kasera, Earl Lewis, Dustin Maas, Alex Orange, Neal Patwari, Daniel Reading, Robert Ricci, David Schurig, Leigh B. Stoller, Jacobus Van der Merwe, Kirk Webb, and Gary Wong. 2020. POWDER: Platform for Open Wireless Data-driven Experimental Research. In Proceedings of the 14th International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization (WiNTECH). https://doi.org/10.1145/3411276.3412204
- Martin Abadi, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. 2016. Deep Learning with Differential Privacy. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (Oct 2016). https://doi.org/10.1145/2976749.2978318

Thank you for your time. **Questions** are welcome!