






Upgrade Federated Learning with MPC-based Secure Aggregation

Advisor: **Karl W. Koch**

Motivation

Learning from data improves, nowadays, virtually all areas in our life: e.g., next-word predictions on virtual keyboards, (premature) tumor analysis on MRI images, or enhancing autonomous driving. Federated Learning (FL), introduced by Google in 2016, enables Machine Learning locally on participants' devices. A prominent example is the virtual-keyboard application Gboard, which learns/t on millions of people's device to improve the global ML model via FL. Though, "plain FL" is vulnerable to data-reconstruction attacks. Thus, techniques such as (MPC-based) Secure Aggregation (SecAgg), which reveals only the final sum of all participants, have been added to FL. In recent years, several flavors of SecAgg protocols have been created.


 Your Mission, *should you choose to accept it*, is to enter the realm of MPC-based SecAgg-enhanced FL and accomplish the project's goals


 Interested to get to know more info?
Please feel free to contact me 

Goals

 Get to know

 Secure Multi-Party Computation (MPC)

 Federated Learning (FL)

 Familiarize with MPC-based SecAgg protocols in FL

 Dig Deeper into ≥ 1 Protocol

 Implement & Evaluate the Protocol(s)

Literature

- > K. Bonawitz et al.
Practical Secure Aggregation for Privacy-Preserving Machine Learning
CCS 2017
<https://dl.acm.org/doi/10.1145/3133956.3133982>

Courses & Deliverables

- Introduction to Scientific Working**
Short report on background
Short presentation
- Bachelor Project**
Project code and documentation
- Bachelor's Thesis**
Project code
Thesis
Final presentation

Recommended if you're studying

- CS
- ICE
- SEM

Prerequisites

- > Basic crypto background
- > Motivation to dig into the realm of privacy-preserving computations

Advisor Contact

karl.koch@tugraz.at