

* **Self-funding Project** (2020.01-now, host, ongoing)

A small experimental platform for Byzantine-robust federated learning and poisoning attacks.

* **NUAA Undergraduate Innovation Project** (2018.03-2018.12, main contributor, accomplished)

BlockVote: Implementing a PoW blockchain prototype to record voting logs and make statistics.

* **Outsourcing R&D task, Institute of Semiconductors, CAS** (2019.12-2020.03, host)

Android development task that implementing navigation and route planning algorithm.

Tel：+86 18652933335

Homepage: https://boriszhao.github.io

**Projects**

（\* marks the corresponding author, red color marks the supervisor.）

* **Bo Zhao**, Peng Sun\*, Tao Wang, Keyu Jiang, “FedInv: Byzantine-robust Federated Learning by Inversing Local Model Updates”, 36th AAAI Conference on Artificial Intelligence (**AAAI**), accepted with oral, 2022.
* **Bo Zhao**, Peng Sun, Liming Fang\*, Tao Wang, Keyu Jiang, “FedCom: A Byzantine-Robust Local Model Aggregation Rule Using Data Commitment for Federated Learning”, rejected by IEEE Symposium on Security and Privacy (**IEEE S&P**), under revision, 2021.
* **Bo Zhao**, Liming Fang\*, Hanyi Zhang, Chunpeng Ge, Weizhi Meng, Liang Liu, Chunhua Su, “Y-DWMS: A Digital Watermark Management System Based on Smart Contracts”, Sensors, accepted, 2019.
* Liming Fang, **Bo Zhao**, Yang Li, Zhe Liu\*, Chunpeng Ge, Weizhi Meng, “Countermeasure Based on Smart Contracts and AI against DoS/DDoS Attack in 5G Circumstances”, IEEE Network Magazine, accepted, 2020.

**Publications & Archives**

* Distributed Machine Learning / Federated Learning Security (ongoing)
* Blockchain and Computationally Intensive Smart Contracts

**Research Topics**

* 2016.09-2020.06

Nanjing University of Aeronautics and Astronautics

Information Security Undergraduate GPA：82/100

* 2020.09-

Nanjing University of Aeronautics and Astronautics

Cyberspace Security Master

**Education Background**

Date of Birth：1998.07

Mail：bozhao@nuaa.edu.cn

Bo Zhao

Resume