Reference (Adversarial Robustness)

1. Shafah, Huang, Najibi, Suciu, Studer, Dumitras, Goldstein. Poison frogs! targeted clean-label poisoning attacks on neural networks. In *NIPS*, 2018.
2. Bhagoji, Chakraborty, Mittal, & Calo. Analyzing federated learning through an adversarial lens. In *ICML*, 2019.
3. Koh, Steinhardt, & Liang. Stronger data poisoning attacks break data sanitization defenses. *arXiv*, 2018.
4. Fang, Cao, Jia, & Gong. Local model poisoning attacks to Byzantine-robust federated learning. *arXiv*, 2019.
5. Blanchard, Guerraoui, & Stainer. Machine learning with adversaries: Byzantine tolerant gradient descent. In *NIPS*, 2017.
6. Chen, Su, & Xu. Distributed statistical machine learning in adversarial settings: Byzantine gradient descent. *In Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 2017.
7. Yin, Chen, Ramchandran, Bartlett. Byzantine-robust distributed learning: Towards optimal statistical rates. In *ICML*, 2018.