JIAHAO YU

ABOUT

Shanghai Jiaotong University(SJTU)
Major in ECE, Zhiyuan Honor Progarm
Advisor: Haojin Zhu, Liyao Xiang
GPA: overall 85.3/100; junior 87.7/100
Homepage
email:yujiahao@sjtu.edu.cn

RESEARCH INTERESTS

Machine Learning, Deep Learning
Privacy and Security
Federated Learning

PUBLICATION

MSTrojan: Backdoor Attacks in Federated Learning with First-Order Triggers(under revision for TMC)
Jiahao Yu, Jungang Yang, Liyao Xiang, Weiting Li, Quanshi Zhang

Privacy Threats in Robust Model Inversion Attack(under revision for PPAI21)
Jiahao Yu, Liyao Xiang, Quanshi Zhang, Baochun Li

Voiceprint Mimicry Attack Towards Speaker Verification System in Smart Home(INFOCOM20)
Lei Zhang, Yan Meng, **Jiahao Yu**, Chong Xiang, Brandon Folk, Haojin Zhu

Matrix Gaussian Mechanism for Differentially-Private Learning(under review for INFOCOM21)
Jungang Yang, **Jiahao Yu**, Ruidong Chen, Weiting Li, Liyao Xiang, Xinbing Wang, Baochun Li

EXPERIENCE

UIUC Summer research advised by Prof. Bo Li (Jul.2020-present)
Research Interest: Adversarial style transfer for NLP
Expected target: ACL21

MSRA Research Intern advised by Bin Zhu(Sep.2020-present)
Research Interest: Enhance adversarial robustness of malware detector
Expected target: one paper and relating patent

Ant Financial(Alibaba) Intern(Dec.2020-Mar.2021)(Expected)
Research Interest: Enhance performance of privacy-preserving federated learning

AWARDS

Zhiyuan Honor Rewards
1st place for Zhiyuan Scholar Program

PERSONAL SKILLS

Programming: C/C++,Python,Matlab,LaTeX,PowerShell
Software: Pytorch,Keras,Tensorflow,Echart