Yukun **Jiang**

Saarland University & CISPA Helmholtz Center for Information Security

📱 (+49) 152-3628-3737 | ✉ ashbringer0926@gmail.com | Saarbrücken, Germany

Education

CISPA Helmholtz Center for Information Security, Ph.D. in *Computer Science* *Jun. 2023 –*

CISPA Helmholtz Center for Information Security, Preparatory Ph.D. in *Computer Science* *Oct. 2022 – May 2023*

Sichuan University, B.E. in *Cyber Security* *Sep. 2018 – Jul. 2022*

Employment

CISPA Helmholtz Center for Information Security

Doctoral Researcher *Jun. 2023 –*

Research Assistant *Oct. 2022 – May 2023*

Tencent Cloud

Algorithm Engineer Intern *Feb. 2022 – Aug. 2022*

Publications

Yukun Jiang, Mingjie Li, Michael Backes, Yang Zhang: Adjacent Words, Divergent Intents: Jailbreaking Large Language Models via Task Concurrency. In Proceedings of The Thirty-Ninth Annual Conference on Neural Information Processing Systems (NeurIPS 2025).

Yukun Jiang, Zheng Li, Xinyue Shen, Yugeng Liu, Michael Backes, Yang Zhang: `ModSCAN`: Measuring Stereotypical Bias in Large Vision-Language Models from Vision and Language Modalities. In Proceedings of The 2024 Conference on Empirical Methods in Natural Language Processing (EMNLP 2024).

Yukun Jiang, Xinyue Shen, Rui Wen, Zeyang Sha, Junjie Chu, Yugeng Liu, Michael Backes, Yang Zhang: Games and Beyond: Analyzing the Bullet Chats of Esports Livestreaming. In Proceedings of International AAAI Conference on Web and Social Media 2024 (ICWSM 2024).

Prior to Ph.D. Studies

Yukun Jiang, Xiaoyu Cao, Chen Hao, Neil Gong: FedER: Communication-Efficient Byzantine-Robust Federated Learning. In Proceedings of International Conference on Learning Representations 2022 Workshop on Socially Responsible Machine Learning (ICLR 2022-SRML).

Beibei Li, **Yukun Jiang**, Qingqi Pei, Tao Li, Liang Liu, Rongxing Lu: FEEL: Federated End-to-End Learning with Non-IID Data for Vehicular Ad Hoc Networks. In IEEE Transactions on Intelligent Transportation Systems (T-ITS).

Beibei Li, **Yukun Jiang**, Wenbin Sun, Weina Niu, Peiran Wang: FedVANET: Efficient Federated Learning with Non-IID Data for Vehicular Ad Hoc Networks. In Proceedings of IEEE Global Communications Conference 2021 (GLOBECOM 2021).

Beibei Li, Yaxin Shi, Yuqing Guo, Qinglei Kong, **Yukun Jiang**: Incentive-Based Adaptive Federated Knowledge Distillation for Cross-Silo Applications. In Proceedings of IEEE International Conference on Computer Communications Workshops (INFOCOM 2022 WORKSHOPS)

Beibei Li, Peiran Wang, Hanyuan Huang, Shang Ma, **Yukun Jiang**: FLPhish: Reputation-Based Phishing Byzantine Defense in Ensemble Federated Learning. In Proceedings of IEEE Symposium on Computers and Communications 2021 (ISCC 2021). **Best Paper Award**

Honors & Activities

Best Paper Award, IEEE Symposium on Computers and Communications 2021. *Sep. 2021*

1st Prize, Outstanding Student Scholarship, Sichuan Univ. *Sep. 2021*