Yuhan Liu

⊙ Beijing, China   ✉ liuyh2019@ruc.edu.cn   📞 +86 13581609286   ⌨ liuyuhannn

About Me

I am currently a Ph.D. candidate in the School of Information at Renmin University of China (RUC) ⬈. I am super lucky to be advised by Prof. Hong Chen ⬈ in the Key Laboratory of Data Engineering and Knowledge Engineering (DEKE) ⬈ at RUC. After a year of research internship supervised by Dr. Sheng Wang ⬈ at Alibaba DAMO Academy, I was extremely fortunate to be a visiting student studying under the supervision of Prof. Yves-Alexandre de Montjoye ⬈ in the Computational Privacy Group (CPG) ⬈ at Imperial College London. Before that, I spent four splendid years at Xiamen University (XMU) as an undergraduate.

Education

BS	**Xiamen University**, Computer Science	Sept. 2015 – June 2019

- GPA: 3.6/4.0 , **Distinguished Graduate**
- **Coursework:** Data structure, Algorithm, Machine Learning, Linear Algebra, Statistics

Ph.D	**Renmin University of China**, Big data engineering	Sept. 2019 - June 2025

- GPA: 3.9/4.0
- **Research interests:** Data privacy, Differential Privacy, Privacy attacks, Private machine learning

Visit	**Imperial College London**, Data privacy	Oct. 2023 - Oct.2024

- **Project:** Membership inference attacks against differentially private location aggregates.

Experience

DAMO Academy, Alibaba Group, Research Intern	Beijing, China June 2023 - Aug. 2024

- **Project:** Differentially private crowd selection
- **Achievement:** Research paper published at VLDB

Publications

Sub-optimal Learning in Meta-Classifier Attacks: A Study of Membership Inference on Differentially Private Location Aggregates ⬈ — S&P'2025 (Under review)

Yuhan Liu, Florent Guepin, Igor Shilov

Unleash the Power of Ellipsis: Accuracy-enhanced Sparse Vector Technique with Exponential Noise ⬈ — VLDB'2025

Yuhan Liu, Sheng Wang, Yixuan Liu, Feifei Li, Hong Chen

Enhanced Privacy Bound for Shuffle Model with Personalized Privacy ⬈ — CIKM'2024

Yixuan Liu, *Yuhan Liu*, Li Xiong, Yujie Gu, Hong Chen

Edge-Protected Triangle Count Estimation Under Relationship Local Differential Privacy ⬈ — TKDE'2024

Yuhan Liu, Tianhao Wang, Yixuan Liu, Hong Chen, Cuiping Li

Echo of Neighbors: Privacy Amplification for Personalized Private Federated Learning with Shuffle Model ⬈ — AAAI'2023

Yixuan Liu, Suyun Zhao, Li Xiong, *Yuhan Liu*, Chong Chen

Collecting Triangle Counts with Edge Relationship Local Differential Privacy ↗   ICDE'2022
Yuhan Liu, Suyun Zhao, Yixuan Liu, Dan Zhao, Hong Chen, Cuiping Li

State-of-the-Art Privacy Attacks and Defenses on Graphs   CJC'2022
Yuhan Liu, Hong chen, Yixuan Liu, Dan Zhao, Cuiping Li

Privacy-preserving Techniques in Federated Learning   JoS'2022
Yixuan Liu, Hong Chen, *Yuhan Liu*, Cuiping Li

Skills

Coding Languages: C++, C, Python

Languages: English (fluent)