Xinbao Qiao (乔鑫宝)

Email: xinbaoqiao@zju.edu.cn | Mobile: (+86)-195-5833-7916 | Zhejiang, China

Education

- **Zhejiang University** *09/2022 - 06/2025 [Expected]*
  Master in Artificial Intelligence
  - Relevant courses: Artificial Intelligence Algorithm and Systems (100), Secure Artificial Intelligence (97)
  - Advisor: Prof. Meng Zhang
  - Major GPA: 85/100 (Rank: 3/25)

- **Shandong University** *09/2018 - 06/2022*
  Bachelor in Communication Engineering
  - Relevant courses: Data and Computer Communications (95), Modern Cryptography (90)

Research Interests

- Trustworthy Machine Learning (Privacy, Fairness, Robustness, and Explainable Artificial Intelligence)

  Specifically in Machine Unlearning, Federated Learning, Differential Privacy and Exploring the trade-offs between different pillars of trust in ML, including fairness, robustness, privacy, and utility.

Publications

[1] Hessian-Free Online Certified Unlearning
Xinbao Qiao, Meng Zhang, Ming Tang, Ermin Wei. ICLR, 2025.

[2] DynFrs: An Efficient Framework for Machine Unlearning in Random Forest
Shurong Wang, Zhuoyang Shen, **Xinbao Qiao**, Meng Zhang. ICLR, 2025.

[3] Federated Unlearning with Differential Privacy: A Trilemma
Xinbao Qiao, Ming Tang, Meng Zhang, Ermin Wei. 2024. (Journal, Under review.)

[4] Soft Weighted Machine Unlearning
Xinbao Qiao, Ningning Ding, Yushi Cheng, Meng Zhang. 2025, (Conference, Under review)

[5] Less is More: Influence-Based Node Pruning in Decentralized Learning
Xinbao Qiao, Meng Zhang, Ming Tang, Ermin Wei. 2025, (Conference, Under review)

Research Experience

- **Research on Machine Unlearning** *03/2023 - Present*
  Advisor: Prof. Meng Zhang, ZJU-UIUC Institute
  - Focused on the development of auditable approximate and exact algorithms for Machine Unlearning , and the exploration of trade-offs between different pillars of trust in machine learning.
  - Analyzed the inherent conflicts between unlearning and privacy in federated learning system. Conducted a detailed study on the three-way trade-off amongst utility, unlearning, and privacy, resolving such conflicts by leveraging the dual-use of noise framework with rigorous mathematical guarantees.
  - Developed a Hessian-free approximate machine unlearning algorithm with millisecond-level unlearning execution time, achieving the most efficient data removal and state-of-the-art theoretical results, including unlearning guarantee, generalization guarantee, and deletion capacity guarantee.
  - Developed an exact machine unlearning framework for random forests by combining the subsampling method with a lazy tag strategy, solving inefficiencies in handling large-scale deletions and enhancing performance compared to existing unlearning methods for random forests.
  - Conducted analysis on machine unlearning in non-privacy tasks, such as fairness and robustness, identifying and providing deeper insights into the over-unlearning challenge, and addressed this issue by proposing a soft-weighted framework that enables fine-grained model adjustments.

Honors and Awards

- **Scholarship** *2019*
  Third-Class Scholarship, Shandong University
- **Honor** *2023*
  Merit Graduate Student, Zhejiang University

Skills

- **Programming:** Python (advanced), MATLAB (advanced), Latex (advanced), Markdown, C/C++, VHDL, etc.
- **Research Foundation:** Solid base knowledge of Artificial Intelligence and its Security aspects. Solid base knowledge of data-driven Machine Learning approaches. Foundation in Decentralized Learning.