Statement of Purpose

Qiang Hu, huq2021@mail.sustech.edu.cn

Why Purdue IE PhD?

I am enthusiastic about pursuing a PhD in Industrial Engineering at Purdue University under the guidance of Professor Gesualdo Scutari because of the program's strong emphasis on distributed optimization and statistical learning, areas that align perfectly with my research interests and academic background. Purdue's reputation as a leading institution for industrial engineering and Professor Scutari's expertise in these fields provide an exceptional platform to engage in cutting-edge research. The guaranteed support for the entire PhD and the opportunity to work in a stimulating environment focused on mathematical rigor and impactful applications further solidify my interest in this program. I am particularly motivated by the chance to contribute to forefront advancements in optimization and machine learning, which have broad implications for both academia and industry.

Research Statement

This is a brief statement about my research experiences, research interest, and future research plans.

Research Experience

Since the summer of 2023, I have been interning in Prof. Hongxin Wei's machine learning group at our department (Department of Statistics and Data Science). My primary research experience focuses on ML privacy and large language models (LLMs), specifically on membership inference attacks (MIA) and in-context learning for LLMs.

Under the guidance of Professor Hongxin Wei, I have been involved in three research projects. The first focused on the vulnerability differences of data under membership inference attacks, with an attempt to mitigate these disparities, which could be identified as outliers in terms of features. Although this work did not lead to a published paper due to various reasons, including the immature MIA settings, it greatly enhanced my understanding of MIA at the data level. The second project was related to content risk control for large language models (LLMs) using top-k in-context learning, with the goal of establishing a benchmark for LLM risk control in domestic contexts. Most recently, I proposed PAST, a method for defending against membership inference attacks through adaptive sparsification, which has been submitted to ICLR 2025.

I also deeply appreciate Prof. Guanhua Chen, whose courses on NLP and Spark (with NLP being a graduate-level course) provided me with a profound understanding of various LLM tasks and sparked my interest in areas such as distributed training, efficient fine-tuning, model quantization, retrieval-augmented generation (RAG).

Research Interest

My research interests primarily lie in trustworthy AI, efficient AI, and LLMs. Specifically, my main research experience is in Privacy (Membership Inference Attacks, Machine Unlearning) and LLMs (In-Context Learning, Safety Benchmark). Additionally, I have taken several research-oriented courses on NLP and CV, covering topics such as efficient AI and various tasks in NLP and CV. Other intriguing applications of AI or ML may also capture my interest.

Future Research Plans

For the near future, I may work on topics at the intersection of privacy and optimization or continue to delve deeper into research on trustworthy machine learning. My tentative research directions include:

1. **Privacy in Distributed Optimization**: Investigate how privacy concerns can be addressed in distributed optimization frameworks, particularly in scenarios where sensitive data is shared across decentralized systems. This could involve designing privacy-preserving algorithms that balance computational efficiency and data protection.
2. **Parameter Significance and Privacy Defense**: Explore the integration of sparse methods in transformers with considerations of parameter significance for privacy defenses, aiming to achieve both trustworthy and efficient NLP systems.
3. **Privacy Risks in Fine-Tuning LLMs**: Examine the potential privacy risks associated with the fine-tuning of LLMs, especially considering that the efficiency of pre-training and fine-tuning processes could inadvertently increase data leakage. My goal is to assess whether the data used during fine-tuning introduces significant privacy vulnerabilities and to develop strategies for mitigating these risks.