Zesen Liu

Email: ang.sagapo@gmail.com
Mobile: (+86) 150-9774-0991

Education

- **Xidian University** Xi'an, P.R. China
  B.Eng. of Information Security 09/2021 - Present
  09/2021-Present: GPA: 3.9/4.0, Rank: 1/132, top 0.8%

  09/2021-09/2022: Rank: 1/1438, top 0.07%

  Selected courses:
  Advanced Mathematics A(I) 98/100 Advanced Mathematics A(II) 95/100 Linear Algebra 100/100
  Introduction of Computer and Program Design 100/100 Discrete Mathematics(I) 99/100 Modern Cryptography 100/100
  Probability Theory and Mathematical Statistics 97/100 Computer Networks Principle 94/100

Research Experience

- **Data privacy protection and Applied cryptography** 05/2023 - 11/2023
  Research Assistant at Xidian University, advised by Prof. Xiangyu Wang & Prof. Jianfeng Ma
  - Searchable encryption and Data privacy
- **Trustworthy Machine Learning** 11/2023 - 04/2024
  Research Assistant at Tsinghua University NISL, advised by Prof. Qi Li
  - Large language model security and privacy protection.

Research Topics

- **Secure and Efficient Indexing for Spatial and Text Keywords** submit to SIGMOD
  Advisor: Prof. Xiangyu Wang & Prof. Jianfeng Ma, Xidian University 05/2023 - 11/2023
  - In this paper, we introduce an innovative indexing architecture known as the OBIR-tree, specifically tailored to address top-k queries for text retrieval and spatial proximity queries. Furthermore, we incorporate TEE to minimize the number of interactions required, and we have developed RDT to enhance the efficiency of redundant operations within the system.
  - Our approach achieves a substantial optimization efficiency enhancement, outperforming existing baseline schemes by an impressive 40-fold margin.
- **The Robustness of LLM IP Protection Methods Against Model Merging** submit to CCS workshop
  Advisor: Dr. Tianshuo Cong & Prof. Xinlei He, Tsinghua University 11/2023 - 03/2024
  - In this paper, we conduct the first study on the robustness of IP protection methods in model merging scenarios. We investigate two state-of-the-art IP protection techniques: Quantization Watermarking and Instructional Fingerprint along with various advanced model merging technologies.
  - The experiment results present that current watermark method can defend against model merge which highlight that model merging should be an indispensable consideration in the robustness assessment of model IP protection techniques.
- **The Robustness of Watermark in Large Language Model** submit to IEEE S&P(Oakland) First author
  Advisor: Dr. Tianshuo Cong & Prof. Xinlei He, Tsinghua University 11/2023 - 06/2024
  - We make the first comprehensive study to the performance of SOTA watermark schemes against attack methods for machine generated texts. To evaluate the robustness of watermark methods, we propose two main metrics which are quality and watermark percent. In addition to the previous attack methods, we propose two attack methods which are called model merge attack and LoRA attack respectively.
  - Our results present that every watermark to the attack is vulnerable and highlight that the privacy protection to LLMs is urgent and has a great potential for studying.

Honors and Awards

First Prize Scholarship, Xidian University	11/2022
First Prize Scholarship, Xidian University	11/2023
Third Prize, National Cryptography Competition (CACR)	11/2023
Honorable Mention, International Mathematical Contest in Modeling (MCM/ICM)	05/2023
First Prize, China Undergraduate Mathematical Contest in Modeling (CUMCM)	12/2023
First Prize, Chinese Mathematics Competition	10/2022

Skills Summary

- **Programming Languages**: Python, C/C++, LaTeX.
- **Frameworks**: PyTorch, NumPy.
- **Tools**: Git, Anaconda.

Student Experience

- **Xidian University Science and Technology Association, Quality Group** Xi'an, P.R. China
  Responsibility: administrator 10/2021 - 10/2022