

Qiang Hu

Tel: (086) 13874700355; E-mail: huq2021@mail.sustech.edu.cn



EDUCATION

Southern University of Science and Technology, ShenZhen, China

BS in Data Science and Big Data Technology (*Department of [STAT-DS](#)*)

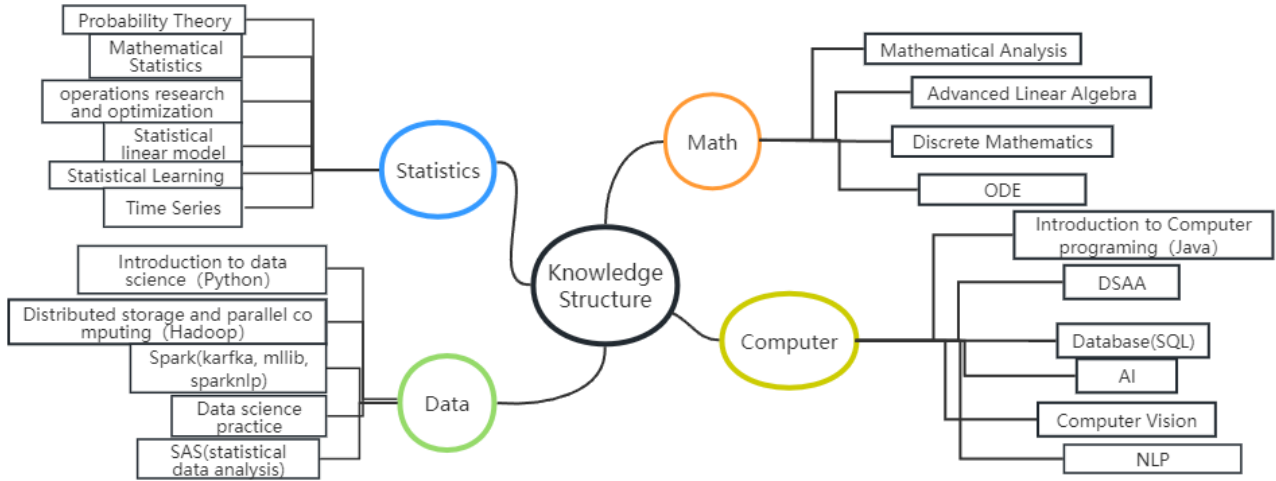
GPA: **3.93/4.00**(1/53)

Research Interests: Trustworthy AI, LLMs, Efficient AI [[Google Scholar](#)]

Sep. 2021-Present

Expected in June 2025

KNOWLEDGE BACKGROUND



RESEARCH EXPERIENCE

Intern in Machine Learning Group of [Hongxin Wei](#), Southern University of Science and Technology

Jul 2023-Present

Vulnerability Disparity Against MIA,

Jul 2023-Mar 2024

Independent Research

- Found an efficient way to distinguish instances with different levels of vulnerability in MIA scenarios;
- Tried some relief methods, including reweighting, kde-flattening, etc.

Top-k ICL for Content Risk Control (A collaborative project with [Deepexi](#)), Mar 2024-Jul 2024

Research Assistant

- Implemented ICL for Content Risk Control;
- Established a [benchmark](#) for large model risk control in domestic scenarios, including building data sets with crawlers (from Twitter, etc).

Defending Membership Inference Attacks via Privacy-aware Sparsity Tuning, Jul 2024-Oct 2024

Co-first Author (Submitted to ICML 2025)[[paper](#)]

- Proposed a state-of-the-art empirical defense method against membership inference attacks, leveraging model sparsification techniques.

ACTIVITIES & AWARDS

Provincial(HuNan) first prize in CPhO 2020(Chinese Physics Olympiad) Oct. 2020

The Second Prize Scholarship, Southern University of Science and Technology 2022, 2023

Provincial(GuangDong) third award in CUMCM 2022

(China Undergraduate Mathematical Contest in Modeling) Sep. 2022

Provincial(GuangDong) second award in CMC 2023(Chinese Mathematics Competitions) Oct. 2023

Outstanding Volunteer of the School of Science 2023

LANGUAGES & SKILLS

Languages: Mandarin (Native), English (TOEFL iBT: [85](#))

Programming Languages: Python, Bash, SQL, R, SAS, Spark(including kafka&Ray), Java, Matlab;