Yitong Zhang (张奕彤)

Email: zhangyt42@buaa.edu.cn
Homepage: https://zhangyitonggg.github.io/

Education

- 2026.09 (expected), Ph.D. Student, College of AI, Tsinghua University, under the supervision of Prof. Jia Li
- 2022.09 - 2026.06 (expected), Undergraduate Student, School of Computer Science and Engineering, Beihang University, under the supervision of Prof. Xianglong Liu and Prof. Aishan Liu

Academic Performance

- Weighted Score: **95.3**/100 Rank: **3**/241
- GPA: **3.90**/4.00 Rank: **4**/241
- Selected Core Courses:
  Advanced Algebra (100) Probability Theory and Statistics (100) Computer Vision and Computation (99)
  Mathematical Analysis (99) Object-Oriented Designand Construction (100) Computer Organization (98)
  Algorithm Design and Analysis (100) Data Structures and Programming (99) Discrete Mathematics (99)

Honors and Awards

- **Shen Yuan Medal (top 0.1%, only 10 undergraduates university-wide, the highest scholarship of Beihang University)**, 2025
- **Beihang Youth May Fourth Medal, (the highest honor for youth members at Beihang University)**, 2026
- **China National Scholarship (3rd time)**, 2025
- **China National Scholarship (2nd time)**, 2024
- **China National Scholarship**, 2023
- **Xiaomi Special Scholarship** (only **5** undergraduates university-wide), 2024
- **Outstanding Student of Beijing**, 2025
- **Outstanding Student of Shandong**, 2022
- **First Prize**, Chinese Mathematics Competitions for Undergraduates, 2023

Grants

2026.09 – 2024.10 | Large Model Driven End-to-End Autonomous Driving Model Adversarial Attacks
- **Principal Investigator**, Beijing Natural Science Foundation (Grant No. QY24136).
- One of 40 students selected university-wide.

Publications

**** indicates author with equal contribution.***

- DAVSP: Safety Alignment for Large Vision-Language Models via Deep Aligned Visual Safety Prompt
  Yitong Zhang, Jia Li, Liyi Cai, Ge Li
  AAAI 2026 (Oral)
- Environmental Injection Attacks against GUI Agents in Realistic Dynamic Environments
  Yitong Zhang, Ximo Li, Liyi Cai, Jia Li
  ISSTA 2026 Directly Accepted
- Lookahead-then-Verify: Reliable Constrained Decoding for Diffusion LLMs under Context-Free Grammars
  Yitong Zhang, Yongmin Li, Yuetong Liu, Jia Li, Xiaoran Jia, Zherui Li, Ge Li
  ISSTA 2026 Major Revision
- To See is Not to Master: Teaching LLMs to Use Private Libraries for Code Generation
  Yitong Zhang*, Chengze Li*, Ruize Chen, Guowei Yang, Xiaoran Jia, Yijie Ren, Jia Li
  Under Review

- Beyond Autoregression: An Empirical Study of Diffusion Large Language Models for Code Generation
  Chengze Li*, **Yitong Zhang***, Jia Li, Liyi Cai, Ge Li
  Under Review
- AI-Driven Self-Evolving Software: A Promising Path Toward Software Automation
  Liyi Cai*, Yijie Ren*, **Yitong Zhang***, Jia Li
  Preprint
- PackMonitor: Enabling Zero Package Hallucinations Through Decoding-Time Monitoring
  Xiting Liu, Yuetong Liu, **Yitong Zhang**, Jia Li, Shi-Min Hu
  ISSTA 2026 Directly Accepted
- DiffuGuard: How Intrinsic Safety is Lost and Found in Diffusion Large Language Models
  Zherui Li, Zheng Nie, Zhenhong Zhou, Yue Liu, **Yitong Zhang**, Yu Cheng, Qingsong Wen, Kun Wang, Yufei Guo, Jiaheng Zhang
  ICLR 2026
- Enhancing the Transferability of Adversarial Attacks with Stealth Preservation
  Xinwei Zhang, Tianyuan Zhang, **Yitong Zhang**, Shuangcheng Liu
  CVPR 2024 Workshop
- Visual Adversarial Attack on Vision-Language Models for Autonomous Driving
  Tianyuan Zhang, Lu Wang, Xinwei Zhang, **Yitong Zhang**, Boyi Jia, Siyuan Liang, Shengshan Hu, Aishan Liu, Xianglong Liu
  Machine Intelligence Research
- Omni-Safety under Cross-Modality Conflict: Vulnerabilities, Dynamics Mechanisms and Efficient Alignment
  Kun Wang*, Zherui Li*, Zhenhong Zhou, **Yitong Zhang**, Yan Mi, Kun Yang, Yiming Zhang, Junhao Dong, Zhongxiang Sun, Qiankun Li, Yang Liu
  Under Review
- DiffuTester: Accelerating Unit Test Generation for Diffusion LLMs via Mining Structural Pattern
  Lekang Yang, Yuetong Liu, **Yitong Zhang**, Jia Li
  Under Review
- Improving Sampling for Masked Diffusion Models via Information Gain
  Kaisen Yang, Jayden Teoh, Kaicheng Yang, **Yitong Zhang**, Alex Lamb
  Under Review
- What Papers Don’t Tell You: Recovering Tacit Knowledge for Automated Paper Reproduction
  Lehui Li, Ruining Wang, Haochen Song, Yaoxin Mao, Tong Zhang, Yuyao Wang, Jiayi Fan, **Yitong Zhang**, Jieping Ye, Chengqi Zhang, Yongshun Gong
  Under Review

Teaching and Service

- Reviewer: AAAI 2026
- Teaching Assistant: Discrete Mathematics, Beihang University, Spring 2025
- Teaching Assistant: Computer Organization, Beihang University, Fall 2024
- Senior Teaching Assistant: Data Structures and Programming, Beihang University, Spring 2024