Jin Hu

hujin066 | hujin@buaa.edu.cn
Google Scholar | 0009-0000-5564-9331 | https://hujincn.github.io
Haidian, Beijing, China

Research Area: AI Safety, Adversarial ML, Generative Modeling.

About Me

I am currently a PhD student (2023-) at *Zhongguancun Laboratory* and *State Key Laboratory of Complex & Critical Software Environment, Beihang University*, advised by Prof. Xianglong Liu, Prof. Ke Xu, and Dr. Jiakai Wang. I plan to graduate around the end of 2027.

My current research focuses on **Physical Adversarial Machine Learning** (AdvML) and **Visual Generative Modeling**, aiming to explore and measure the defects in AI models and introduce new scalable paradigms for trustworthy AI systems, as well as their interdisciplinary applications. I am an organizer of the 6^{th} AdvML workshop in CVPR 2026 and a committee member of the 5^{th} AdvML workshop in CVPR 2025.

Publications

C=Conference, J=Journal, P=Patent, S=In Submission, T=Thesis

[J.1] **Jin Hu**, et al. (2025). **DynamicPAE: Generating Scene-Aware Physical Adversarial Examples in Real-Time**. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 2026*. DOI: 10.1109/TPAMI.2025.3626068.
In this work, we overcome the technical challenges and establish the first end-to-end training framework for scene-conditional physical adversarial examples, and verify its effectiveness in edge devices.

[C.1] **Jin Hu**, et al. (2025). **Exploring Semantic-constrained Adversarial Example with Instruction Uncertainty Reduction**. In *Neural Information Processing Systems, 2025*.
In this work, we directly generate robust, transferable adversarial examples with semantic constraints derived from the given instruction using diffusion models, and establish the first 3D generation pipeline in this scenario.

[P.1] **Jin Hu**, et al. (2022). **Neural Architecture Search Method, Apparatus, Device, and Storage Medium**. Patent ID: CN115272825A. Technical report: https://arxiv.org/pdf/2207.14524.

[J.2] Jiakai Wang, Xianglong Liu, **Jin Hu**, et al. (2024). **Adversarial Examples in the Physical World: A Survey**. Submitted to IJCV.

Academic Experience

- **Zhongguancun Laboratory** — *June 2023 -*, Beijing, China
  Student assistant researcher. Our work focus on the R&D project on autonomous driving safety.
- **State Key Laboratory of Complex & Critical Software Environment, Beihang Universiy** — *Mar. 2022 - April. 2023*, Beijing, China
  Postgraduate student. I participated in the research project of structural information theory and applications with Prof. Hao Peng and under the supervision of Prof. Angsheng Li.
- **SenseTime Research** — *May 2021 - May 2022*, Beijing, China
  Research Intern. I improved the neural network automatic structure optimization method for AI codec models.
- **Beihang University** — *Sep. 2019 - June 2020*, Beijing, China
  Teaching Assistant for Basic Programming Training.

Education

- **Beihang University** — *Sep. 2023 -*, Beijing, China
  PhD Student.
- **Beihang University, majored in computer science and technology. GPA 3.84 / 4.0** — *Sep. 2022 - Sep. 2023*, Beijing, China
  Master's student
- **Beihang University, majored in computer science and technology. GPA 3.75 / 4.0** — *Sep. 2018 - June 2022*, Beijing, China
  Bachelor's student. Joint cultivation program, degree from Beijing University of Technology.
  All courses completed at Beihang University.

Honors

- **Outstanding Graduate of Beijing** — *July 2022*
- **ICPC Regional Contest - Silver Medal** — *Dec. 2020*
  International Collegiate Programming Contest (ICPC) - Shanghai Regional Contest. (previously known as ACM-ICPC) [🌐]
- **Merit Student (Top 5%)** — *2018 - 2019*, *2020 - 2021*
  Beihang University