

# Xiangming Gu

Homepage: <https://guxm2021.github.io>

Email : [xiangming@u.nus.edu](mailto:xiangming@u.nus.edu)

Mobile : +65-86691662

## EDUCATION

### National University of Singapore

Singapore

- *PhD candidate, Integrative Sciences and Engineering Programme*  
*Majored in Computer Science, Advisor: Prof. Ye Wang, GPA: 4.80/5.0*

2021/08 – Present

### Tsinghua University

Beijing, China

- *B.E. in Electronic Engineering, B.S. in Finance, GPA: 3.80/4.0*

2017/08 – 2021/06

## RESEARCH INTERESTS

- **Machine Learning:** Memorization/Interpretability of Diffusion Models [Arxiv'2023], Attention/Interpretability of LLMs [ATTRIB @ NeurIPS'2024], Safety of (multimodal) LLM agents [ICML'2024].
- **Singing/Speech:** Application of machine learning, e.g. multimodal learning [MM'2022 Oral], multi-distribution learning (domain adaptation [ISMIR'2022, TOMM'2024], fairness [MM'2023]), to singing/speech techniques.

## RESEARCH (GOOGLE SCHOLAR)

### During the Ph.D.

1. **Xiangming Gu**, Tianyu Pang†, Chao Du, Qian Liu, Fengzhuo Zhang, Cunxiao Du, Ye Wang†, Min Lin. When Attention Sink Emerges in Language Models: An Empirical View. *Annual Conference on Neural Information Processing Systems Workshop on Attributing Model Behavior at Scale. (ATTRIB @ NeurIPS)*, 2024.
2. Hongfu Liu†, Hengguan Huang, Hao Wang, **Xiangming Gu**, Ye Wang. On Calibration of LLM-based Guard Models for Reliable Content Moderation. *Annual Conference on Neural Information Processing Systems Workshop on Safe Generative AI (SafeGenAI @ NeurIPS)*, 2024. (**Oral**)
3. **Xiangming Gu**\*, Xiaosen Zheng\*, Tianyu Pang\*†, Chao Du, Qian Liu, Ye Wang†, Jing Jiang†, Min Lin. Agent Smith: A Single Image Can Jailbreak One Million Multimodal LLM Agents Exponentially Fast. *International Conference on Machine Learning. (ICML)*, 2024.
4. **Xiangming Gu**, Chao Du†, Tianyu Pang†, Chongxuan Li, Min Lin, Ye Wang†. On Memorization in Diffusion Models. *arXiv preprint arXiv:2310.02664*, 2023
5. **Xiangming Gu**, Longshen Ou, Wei Zeng, Jianan Zhang, Nicholas Wong, Ye Wang†. Automatic Lyric Transcription and Automatic Music Transcription from Multimodal Singing. *ACM Transactions on Multimedia Computing Communications and Applications (TOMM)*, 2024.
6. **Xiangming Gu**, Wei Zeng, Ye Wang†. Elucidate Gender Fairness in Singing Voice Transcription. *ACM International Conference on Multimedia (MM)*, 2023.
7. **Xiangming Gu**\*, Longshen Ou\*, Danielle Ong, Ye Wang†. MM-ALT: A Multimodal Automatic Lyric Transcription System. *ACM International Conference on Multimedia (MM)*, 2022. (**Oral, Top Paper Award**)
8. Hengguan Huang†, **Xiangming Gu**, Hao Wang, Chang Xiao, Hongfu Liu, Ye Wang†. Extrapolative Continuous-time Bayesian Neural Network for Predictive Streaming Domain Adaptation. *Annual Conference on Neural Information Processing Systems (NeurIPS)*, 2022.
9. Longshen Ou\*, **Xiangming Gu**\*, Ye Wang†. Transfer Learning of wav2vec 2.0 for Automatic Lyric Transcription. *International Society for Music Information Retrieval Conference (ISMIR)*, 2022.
10. Yixin Wang, Wei Wei, **Xiangming Gu**, Xiaohong Guan, Ye Wang†. Disentangled Adversarial Domain Adaptation for Phonation Mode Detection in Singing and Speech. *IEEE Transactions on Audio, Speech and Language Processing (TASLP)*, 2023.

11. Wei Wei\*, Hengguan Huang\*, **Xiangming Gu**, Hao Wang, Ye Wang†. Unsupervised Mismatch Localization in Cross-Modal Sequential Data with Application to Mispronunciations Localization. *Transactions on Machine Learning Research (TMLR)*, 2022.

## During the Undergraduate

1. Boyu Zhang, **Xiangming Gu**, Jiayuan Liu, Jingyi Kang, Chengquan Hu, Hongen Liao†. Spring-reinforced Pneumatic Actuator and Soft Robotic Applications. *Smart Materials and Structures*, 2024.
2. Youze Xue, Jiansheng Chen†, **Xiangming Gu**, Huimin Ma, Hongbing Ma. Boosting Monocular 3D Human Pose Estimation with Part Aware Attention. *IEEE Transactions on Image Processing (TIP)*, 2022.
3. Boyu Zhang, Penghui Yang, **Xiangming Gu**, Hongen Liao†. Laser Endoscopic Manipulator Using Spring-reinforced Multi-DoF Soft Actuator. *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, also *IEEE Robotics and Automation Letter (RA-L)*, 2021.

## EXPERIENCE

---

- **Sea AI Lab (Shopee’s parent company)** Singapore  
*Research Intern* 2023/03 – Present
  - **Host:** Dr. Tianyu Pang and Dr. Chao Du.
  - **Activity:** Conduct research projects on (i) memorization in diffusion models; (ii) infectious jailbreak on (multimodal) large language models based multi-agent systems; (iii) attention sink in large language models.
- **Tsinghua University** Beijing, China  
*Undergraduate Researcher* 2020/09 – 2021/06
  - **Host:** Prof. Jiansheng Chen (supervisor) and Dr. Youze Xue (mentor).
  - **Activity:** Conduct research projects on (i) monocular 3D human pose estimation; (ii) multi-view 3D human pose estimation for medical applications.
- **National University of Singapore** Singapore  
*Exchange Student and Summer Intern* 2020/01 – 2020/08
  - **Host:** Department of Electrical and Computer Engineering and Prof. Cheng Xiang.
  - **Activity:** Take courses with a GPA of 4.88/5.00; conduct research about interpretable artificial intelligence.
- **Tsinghua University** Beijing, China  
*Undergraduate Researcher* 2018/09 – 2019/06
  - **Host:** Prof. Hongen Liao (supervisor) and Prof. Boyu Zhang (mentor).
  - **Activity:** Conduct research projects on soft robotics design and applications.

## HONORS AND AWARDS

---

- Participant for Global Young Scientists Summit 2025
- Dean’s Graduate Research Excellence Award (School of Computing, National University of Singapore) 2024
- Research Incentive Award (School of Computing, National University of Singapore) 2023
- Research Achievement Award (School of Computing, National University of Singapore) 2022
- MM’22 Top Paper Award (Association for Computing Machinery) 2022
- MM’22 Student Travel Grant (Association for Computing Machinery) 2022
- President’s Graduate Fellowship (National University of Singapore) 2021
- Visiting Undergraduate Student Scholarship (Tsinghua University) 2020
- Tsinghua’s Friend- Zheng Geru Scholarship (Tsinghua University) 2018

## PROFESSIONAL SERVICES

---

- **Conference Reviewer:** CVPR 2025, ICLR 2025, ACL ARR 2024 June/August/October, NeurIPS 2024, MM 2024, ECCV 2024, IJCAI 2024, ICCV 2023, AISTATS 2025/2021
- **Workshop Reviewer:** NeurIPS 2024 Workshop on Attributing Model Behavior at Scale, NeurIPS 2024 Safe Generative AI Workshop
- **Journal Reviewer:** TOMM, TASLP, RA-L

## TEACHING

---

- |   |  |
|---|--|
| • <b>Teaching Assistant</b><br><i>CS4347/CS5647, Sound and Music Computing</i>        | National University of Singapore<br><i>Fall 2024</i>   |
| • <b>Teaching Assistant</b><br><i>CS6212, Topics in Media</i>                         | National University of Singapore<br><i>Spring 2024</i> |
| • <b>Teaching Assistant</b><br><i>CS5242, Neural Networks and Deep Learning</i>       | National University of Singapore<br><i>Spring 2023</i> |
| • <b>Teaching Assistant</b><br><i>CS3244: Machine Learning</i>                        | National University of Singapore<br><i>Fall 2022</i>   |
| • <b>Teaching Assistant</b><br><i>CS4243: Computer Vision and Pattern Recognition</i> | National University of Singapore<br><i>Spring 2022</i> |

## TECHNICAL SKILLS

---

- **Coding:** Python, Matlab, Shell, C/C++, HTML, Verilog, Assembly language, L<sup>A</sup>T<sub>E</sub>X, ...
- **Libraries:** PyTorch, Huggingface, SpeechBrain, ...