# Xuan Liu

Tel : +852 92973217 | E-mail : xuan18.liu@connect.polyu.hk | LinkedIn : www.linkedin.com/in/xuan-liu-48b038258

## *Education*

**The Hong Kong Polytechnic University** 2021 - 2025

Bachelor (Honors) Electronic & Information Engineering GPA 3.8/4

*(2021/22/23 Best GPA Awards for the Top 3 Students in the Department & Dean's Honor List)*

**University of British Columbia** *(Full-Funding Research Assitant)* Summer 2024

**New York University** ***(****Full-Scholarship Exchange****)*** Spring 2024

**Cambridge University** ***(****Full-Scholarship Summer School****)*** Summer 2022

## *Research*

How vulnerable are AI systems to privacy and ethical breaches? My research emphasizes Trustworthy and Responsible AI, focusing on privacy protection, bias mitigation, and energy sustainability. I explore Attack & Defense Algorithms, along with Federated Learning Systems and Large-scale Model distributed training. Also, I try to investigate AI interpretability by integrating interdisciplinary perspectives.

**Research Experience:**

**Pervasive Intelligence Laboratory, HKUST** *[Prof. Song Guo]*

- Explore the role of Generative Models in Attack & Defense Algorithms. 2023.5 till now
- Raised and studied Privacy Risks of Federated Learning in Multimodal scenarios. 2022.2 to 7

**Laboratory for Agile and Resilient Complex Systems, NYU** *[Prof. Quanyan Zhu]*

- Working on Large-Scale Models and Society System Spring 2024
- Researching the Interpretability of Large Language Models via Cognition View Spring 2024

**2024 Summer intern @ Trust & Efficient AI Lab, UBC** *[Prof. Xiaoxiao Li]*

- Large-Scale Model Distributed Training System, Prunning and Model Merge Working On
- Efficient AI System Working On

**Papers:**

[1] **Xuan Liu*,** Siqi Cai, Lin Li, Rui Zhang, Song Guo**. "**MGIA: Mutual Gradient Inversion Attack in Muti-Modal Federated Learning" ***[Student Abstract AAAI23 https://doi.org/10.1609/aaai.v37i13.26995]***

[2] **Xuan Liu*,** Song Guo, Jie Zhang, Haoyang Shang, Chengxu Yang, Quanyan Zhu. "Exploring Prosocial Irrationality for LLM Agents: A Social Cognition View" ***[AI Conference Under review Preprint:https://arxiv.org/abs/2405.14744]***

[3] **Xuan Liu*,** Siqi Cai, Qihua Zhou, Song Guo, Ruibin Li, Kaiwei Lin. "Gradient Diffusion: A Perturbation-Resilient Gradient Leakage Attack" ***[AI Conference Under review]***

[4] **Xuan Liu*,** Siqi Cai, Renjie He, Jingling Yuan. **"**Mutual Gradient Inversion: Unveiling Privacy Risks of Federated Learning on Multimodal Signals" ***[Journal Under review]***

[5] Nada H. Salam, Shengwu Xiong, **Xuan Liu*** . "Reversible data-hiding exploiting Huffman encoding in dual image using weighted matrix and generalized exploiting modification direction (GEMD)"

***[The Visual Computer 2023 https://doi.org/10.1007/s00371-023-03058-8]***

[6] Siqi Cai, **Xuan Liu***, Jingling Yuan, Qihua Zhou, Song Guo. “Prompt-Ladder: Memory-Efficient Prompt Tuning for Pre-trained Vision-Language Models on Edge” ***[Conference Under review]***

[7] Chuang Hu, Nanxi Wu, Siping Shi, **Xuan Liu***, Bing Luo, Ye Wang, Jiawei Jiang, Dazhao Cheng “PriFairFed: A Local Differentially Private Federated Learning Algorithm for Client-Level Fairness” ***[Journal Under review]***

---

## *Entrepreneurship*

**Eco-friendly Technology Start-Up Founder & Owner** 2022-Present

- Build and lead the Eco-friendly entrepreneurship team **BreathingCORE**
- Transferred my patent into Negative Carbon Emission Sustainable Product while constructing IoTs services which has been selected for the **Hong Kong government incubation program**.

**Related Patent (Copyright Holder & Inventor):**

CN 109589733 B: An environmentally friendly outdoor dust reduction device using solar thermal energy.

**Visit My Team Website:** https://breathingcore.com & **University Offical Interview:** Ins; Linkedin

**Pitching Award & Fundings** **240K HKD**

| | |
|---|---|
| Outstanding Proposal of Belt and Road Initiatives Youth Creative International Challenge | 2024 |
| Hong Kong Science & Technology Park incubation: MicroFund | 2024 |
| Hong Kong Science & Technology Park: Ideation Silver & Golden program | 2023 & 24 |
| Dr Winnie S M Tang PolyU Student Innovation & Entrepreneurship Scholarship | 2022 |
| Shenzhen Innovation & Entrepreneurship Competition Outstanding Award | 2022 |

---

## *Academic & Research Awards and Scholarships*

| | |
|---|---|
| Best Undergraduate Research & Innovation Project Award | 2023&24 |
| International Competition and Conference Scheme Award | 2023&24 |
| Hong Kong Government Scholarship -Talent Development Scholarship | 2023 |
| Hong Kong Government Scholarship – Reaching Out Award | 2023 |
| HK PolyU Microcontroller Application Design Contest Merit Award | 2022&23 |
| HK PolyU Undergraduate Research & Innovation Scholarship | 2022&23 |

---

## *Volunteering & Service:*

**Help with Electronic & Internet in Africa Countryside** 2023.6 - 8

We serviced 400 Households with Solar Panel Installations and helped to design the local IoTs system of Solar MPPT to send back information to Hong Kong **in Rwanda, Africa.**

**IEEE-VTC Fall Volunteer Service Award** 2023.10
Serve as IEEE 98th Vehicular Technology Conference volunteer to help with the organization.

---

## *Industrial Work Experience:*

**Internship as Intern-Engineer in Fiberhome Telecommunication Technologies** 2022.7 - 9

Help to Design the MySQL database caching system based on Redis to improve the system’s efficiency

---

***Skills:*** Python (Pytorch)| C#| Simple PADs| 3D Modeling with SolidWorks | Simple Embedded System Development (STM32) | Management & Cooperation | Promoting & Advertising| Design.