Chen Liu

Department of Computer Science
City University of Hong Kong
Hong Kong, China

+852 34428679
chen.liu@cityu.edu.hk
https://liuchen1993.cn

Academic Appointment

City University of Hong Kong — Hong Kong, China
Assistant Professor — 2022.09 -
Research Interests: Machine Learning, Optimization, Deep Neural Networks, Robustness, Privacy.

Education

École Polytechnique Fédérale de Lausanne (EPFL) — Lausanne, Switzerland
Ph.D. in Computer Science — 2017.09 - 2022.09
Supervisors: Prof. Sabine Süsstrunk, Dr. Mathieu Salzmann
Thesis: *Towards Verifiable, Generalizable and Efficient Robust Deep Neural Networks*

École Polytechnique Fédérale de Lausanne (EPFL) — Lausanne, Switzerland
M.Sc in Computer Science — 2015.09 - 2017.08
GPA: 5.73 / 6.00 - *Transcripts*

Tsinghua University — Beijing, China
B.Eng in Computer Science and Technology — 2011.08 - 2015.07
GPA: 91.34 / 100.00, Rank 9 / 123 - *Transcripts*

Internship

Swisscom Digital Lab — Lausanne, Switzerland
Research Intern — 2017.02 - 2017.08
Master Thesis Project: Automatic Document Summarization.

Siemens Research (USA) — Princeton, New Jersey, USA
Research Intern — 2016.07 - 2017.02
Automatic Parameter Tuning Algorithm for 3D Medical Imaging Renderer.

Academic Service

Conference Reviewer: International Conference on Machine Learning (ICML), Conference on Neural Information Processing Systems (NeurIPS), International Conference on Learning Representations (ICLR), Conference on Computer Vision and Pattern Recognition (CVPR).

Top Reviewer: NeurIPS 2024.

Journal Reviewer: Transactions on Machine Learning Research (TMLR), IEEE Transactions on Neural Networks and Learning Systems (TNNLS), Neural Networks (NN), SIAM Journal on Mathematics of Data Science (SIMODS), IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI).

Funded Projects

4. **Industry Donation, No. 9220132.** PI, HKD 330,000. 2024.05 -
   Towards Robust and Privacy-preserving Large Language Models
3. **NSFC - Young Scientist Fund, No. 62306250.** PI, CNY 300,000. 2024.01 -
   Efficient Adversarial Attacks and Adversarial Training Algorithms for Discrete Targets.
2. **CityU Seed Grant, No. 9229130.** PI, HKD 237,590. 2023.06 -
   Towards More Efficient and Robust Object Detection Models against Adversarial Patches for Auto-driving.
1. **Start-up Project, No. 9610614.** PI, HKD 1,060,000. 2022.12 -
   Training Robust Deep Neural Networks: Better and More Efficient.

Publications

In reverse chronological order. * indicates equal contribution.

Preprints

2. Xuyang Zhong, **Chen Liu**. "Sparse-PGD: A Unified Framework for Sparse Adversarial Perturbations Generation". *Arxiv: 2405.05075*.
1. Ding Chen, **Chen Liu**. "Differentially Private Neural Network Training under Hidden State Assumption". *Arxiv: 2407.08233*.

Refereed Papers & Patents

13. Xuyang Zhong, **Chen Liu**. "Towards Mitigating Architecture Overfitting in Dataset Distillation". *IEEE Transactions on Neural Network and Learning Systems 2025*.
12. **Chen Liu**, Zhichao Huang, Mathieu Salzmann, Tong Zhang, Sabine Süsstrunk. "On the Impact of Hard Adversarial Instances on Overfitting in Adversarial Training". *Journal of Machine Learning Research (JMLR) 2024*.
11. Xu Yang, **Chen Liu**, Ying Wei. "Mixture of Adversarial LoRAs: Boosting Robust Generalization in Meta-tuning". *Neural Information Processing Systems (NeurIPS) 2024*.
10. Shuangqi Li, **Chen Liu**, Tong Zhang, Hieu Le, Sabine Süsstrunk, Mathieu Salzmann. "Controlling the Fidelity and Diversity of Deep Generative Models via Pseudo Density". *Transactions on Machine Learning Research (TMLR) 2024*.
9. Xuyang Zhong, Yixiao Huang, **Chen Liu**. "Towards Efficient Training and Evaluation of Robust Models against l_0 Bounded Adversarial Perturbations". *International Conference on Machine Learning (ICML) 2024*.
8. Zhichao Huang, Yanbo Fan, **Chen Liu**, Weizhong Zhang, Yong Zhang, Mathieu Salzmann, Sabine Süsstrunk, Jue Wang. "Fast Adversarial Training with Adaptive Steps". *IEEE Transactions on Image Processing 2023*.
7. Yulun Jiang*, **Chen Liu***, Zhichao Huang, Mathieu Salzmann, Sabine Süsstrunk. "Towards Stable and Efficient Adversarial Training against l_1 Bounded Adversarial Attacks". *International Conference on Machine Learning (ICML) 2023*.
6. **Chen Liu***, Ziqi Zhao*, Sabine Süsstrunk, Mathieu Salzmann. "Robust Binary Models by Pruning Randomly-initialized Networks". *Advances in Neural Information Processing Systems (NeurIPS) 2022*.

5. **Chen Liu**, Mathieu Salzmann, Sabine Süsstrunk. "Training Provably Robust Models by Polyhedral Envelope Regularization". *IEEE Transactions on Neural Networks and Learning Systems 2021*.
4. **Chen Liu**, Mathieu Salzmann, Tao Lin, Ryota Tomioka, Sabine Süsstrunk. "On the Loss Landscape of Adversarial Training: Identifying Challenges and How to Overcome Them". *Advances in Neural Information Processing Systems (NeurIPS) 2020*.
3. **Chen Liu**, Ryota Tomioka, Volkan Cevher. "On Certifying Non-uniform Bounds against Adversarial Attacks". *International Conference on Machine Learning (ICML) 2019*.
2. Ya-Ping Hsieh, **Chen Liu**, Volkan Cevher. "Finding the Mixed Nash Equilibria of Generative Adversarial Networks". *International Conference on Machine Learning (ICML) 2019*.
1. **Chen Liu**, Shun Miao, Kaloian Petkov, Sandra Sudarsky, Daphne Yu, Tommaso Mansi. "Consistent 3D Rendering in Medical Imaging". *European Patent No. 18160956.1 - 1208*.

Invited Talks

- Differentially Private SGD under the Hidden State Assumption
  - Abu Dhabi, UAE. 2024.12. Invited talk at special sessions of AIMS Conference.
- Towards Differentially Private Deep Learning under Hidden State Assumption
  - Zhejiang University, Hangzhou, China. 2024.08. Invited by Prof. Junhong Lin.
  - Shanghai Jiao Tong University, Shanghai, China. 2024.08. Invited by Prof. Xiaolin Huang.
  - EPFL, Lausanne, Switzerland. 2024.07. Invited by Prof. Sabine Süsstrunk.
- The Loss Landscape of Adversarial Training
  - Online. 2020.12. Invited by Prof. Yisen Wang from Peking University.
  - Online. 2020.10. EPFL Adversarial Machine Learning Workshop.
- On Certifying Non-uniform Bounds against Adversarial Attacks
  - Long Beach, California, USA. 2019.06. ICML oral talk.

Awards & Honors

7. Qualcomm Innovation Fellowship Europe 2020 Finalist (Top 15 in Europe) 2020.03
6. ICML Travel Award 2019.06
5. Microsoft Research Scholarship. (Region EMEA - Europe, Middle East and Africa) 2017.09 - 2019.04
4. Outstanding Undergraduate Students in Department of Computer Science and Technology in Tsinghua University. (Top 10%) 2015.07
3. Scholarship of Academic Excellence in Tsinghua University. 2014.10
2. Scholarship of Social Work in Tsinghua University. 2013.10
1. Scholarship of Academic Excellence in Tsinghua University. 2013.10

Teaching

Instructor at CityU HK

3. CS8659: Research in Computer Science. (co-lecturer) Semester A, 2023 - 2024
2. GE2340: Artificial Intelligence: Past, Present and Future. Semester A, 2023 - 2024
1. CS1102: Introduction to Computer Studies. Semester B, 2022 - 2024

Teaching Assistant at EPFL

4. MATH-111(e): Linear Algebra. Autumn 2019, Autumn 2020.
3. CS-413: Computational Photography. Spring 2020, Spring 2021.
    - 2020 EPFL AGEPoly IC Polysphere Awards for teaching excellence, one course selected annually.
2. EE-618: Theory and Methods for Reinforcement Learning. Spring 2019.
1. EE-556: Mathematics of Data: From Theory to Computation. Autumn 2018.

Supervison and Mentorship

Ph.D. Students Supervised at CityU HK.

5. Jingning Xu. 2024.09 -
4. Xu Yang. (with Prof. Ying Wei from Zhejiang University) 2023.09 -
3. Xinping Chen. 2023.09 -
2. Ding Chen. 2023.06 -
1. Xuyang Zhong. 2023.01 -

MPhil Students Supervised at CityU HK

1. Haochen Luo. 2025.01 -

Research Assistants Supervised at CityU HK.

1. Yixiao Huang. ($\longrightarrow$ Ph.D. student at UC Berkeley) 2024.02 - 2024.07

Project Students at EPFL.

9. Shuangqi Li. "On the Robustness of Generative Adversarial Networks". Spring 2022.
8. Francisco Ferrari. "Towards Neural Networks Robust Against Sparse Attacks". Spring 2022.
7. Ningwei Ma. "Adversarial Robustness for Neural Ordinary Differential Equations". Autumn 2021.
6. Yulun Jiang. "Adversarial Robustness for Multiple Threat Models". Autumn 2021.
5. Ziqi Zhao. "Network Pruning in Adversarial Training". Spring 2021.
4. Majdouline Ait Yahia. "Robust Binary Network". Spring 2021.
3. Zhenyu Zhu. "Robust Binary Network". Spring 2020.
2. Julien Leal. "Learning Representations via Weak Supervision". Spring 2018.
1. Shengzhao Lei. "Learning Representations via Weak Supervision". Spring 2018.

Miscellaneous

- Languages: Mandarin (Native Speaker), English (Fluent).
- Github: https://github.com/liuchen11.

January 1, 2025