Chen Liu

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

(+86) 18810310301
cliu644@cityu.edu.hk
https://liuchen1993.cn

Academic Appointment

City University of Hong Kong — Hong Kong, China
Assistant Professor — 2022.11 -

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: ICML, NeurIPS, ICLR, CVPR.
Journal Reviewer: TMLR, Neural Networks, SIAM Journal on Mathematics of Data Science.

Publications

In reverse chronological order. * indicates equal contribution.

Preprints

2. Zhichao Huang, Yanbo Fan, Chen Liu, Weizhong Zhang, Yong Zhang, Mathieu Salzmann, Sabine Süsstrunk, Jue Wang. "Fast Adversarial Training with Adaptive Steps". *ArXiv:2206.02417*.

1. Chen Liu, Zhichao Huang, Mathieu Salzmann, Tong Zhang, Sabine Süsstrunk. "On the Impact of Hard Adversarial Instances on Overfitting in Adversarial Training". *ArXiv: 2112.07324*.

Refereed Papers & Patents

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

- "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.

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) 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

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 excellence in teaching, 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.

2. Xiang Chen. 2023.01 -
1. Xuyang Zhong. 2023.01 -

Project Students at EPFL.

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

Miscellaneous

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

September 15, 2022