Chen Liu

Education

- **École polytechnique fédérale de Lausanne(EPFL)** **Lausanne, Switzerland**
  PhD in Computer Science *2017-2022(expected)*
  Topic: Adversarial Robustness in Deep Learning. Supervisors: Prof. Sabine Süsstrunk, Dr. Mathieu Salzmann
- **École Polytechnique Fédérale de Lausanne(EPFL)** **Lausanne, Switzerland**
  MS in Computer Science *2015-2017*
  GPA: 5.73/6.00 Transcript
- **Tsinghua University** **Beijing, China**
  BS in Computer Science and Technology *2011-2015*
  GPA: 91.34/100.00 Rank 9/123 Transcript Graduated with Distinction

Research Interests

Machine Learning.
High-Dimensional Optimization, specializing in Deep Learning.
Adversarial Robustness, including Provable Robustness.

Publications

In reverse chronological order, * indicates equal contributions.

Submitted Works

- Chen Liu*, Ziqi Zhao*, Sabine Sösstrunk, Mathieu Salzmann. "Robust Binary Models by Pruning Randomly-initialized Networks", *Submitted to ICML 2022*.
- Zhichao Huang, Yanbo Fan, Chen Liu, Weizhong Zhang, Yong Zhang, Mathieu Salzmann, Sabine Süsstrunk, Jue Wang. "Fast Adversarial Training with Adaptive Steps", *Submitted to ICML 2022*.
- Chen Liu, Zhichao Huang, Mathieu Salzmann, Tong Zhang, Sabine Süsstrunk. "On the Impact of Hard Adversarial Instances on Overfitting in Adversarial Training". *Submitted to ICML 2022*.
- Zhichao Huang, Chen Liu, Mathieu Salzmann, Sabine Süsstrunk, Tong Zhang. "Improving Adversarial Defense with Self-supervised Test-time Fine-tuning". *Submitted to ICLR 2022*.

Refereed Papers & Patent

- Chen Liu, Mathieu Salzmann, Sabine Süsstrunk. "Training Provably Robust Models by Polyhedral Envelope Regularization". *IEEE Transactions on Neural Networks and Learning Systems 2021*.
- Chen Liu, Mathieu Salzmann, Tao Lin, Ryota Tomioka, Sabine Süsstrunk. "On the Loss Landscape of Adversarial Training: Identifying Challenges and How to Overcome Them". *Neural Information Processing Systems (NeurIPS) 2020*.
- Chen Liu, Ryota Tomioka, Volkan Cevher. "On Certifying Non-uniform Bounds against Adversarial Attacks". *International Conference on Machine Learning (ICML) 2019*.
- Ya-Ping Hsieh, Chen Liu, Volkan Cevher. "Finding the Mixed Nash Equilibria of Generative Adversarial Networks". *International Conference on Machine Learning (ICML) 2019*. **Oral Presentation** in *Smooth Games Optimization and Machine Learning Workshop in NeurIPS 2018*.
- Chen Liu, Shun Miao, Kaloian Petkov, Sandra Sudarsky, Daphne Yu, Tommaso Mansi. "Consistent 3D Rendering in Medical Imaging". *European Patent No. 18160956.1 - 1208*.

Professional Service

Reviewer: ICML, NeurIPS, ICLR.

Work Experiences

- **Swisscom Digital Lab** **Feb, 2017–Aug,2017**
  Lausanne, Switzerland *Internship*
  - Master's Thesis Project: Automatic Document Summarization.
- **Siemens Research (USA)** **Jul,2016–Feb,2017**
  Princeton, New Jersey, USA *Research Intern*
  - Automatic parameter tuning algorithm for a 3D medical-imaging renderer.

Awards & Honors

- Qualcomm Innovation Fellowship Europe 2020 Finalist (15 candidates in Europe)
- ICML Travel Award (2019)
- Microsoft Research Scholarship.(MSR sponsored student 2017 - 2019)
- Outstanding Undergraduate Students in Department of Computer Science and Technology in Tsinghua University. (Top 10%, 2015)
- Scholarship of Academic Excellence in Tsinghua University. (2014)
- Scholarship of Social Work in Tsinghua University. (2013)
- Scholarship of Academic Excellence in Tsinghua University. (2013)
- First Prize in Beijing College Student Physics Competition. (2012)

Talks

- "The Loss Landscape of Adversarial Training".
  - Online, December 2020. Invited by Prof. Yisen Wang from Peking University.
  - Online, October 2020. EPFL Adversarial Robustness Workshop.
- "On Certifying Non-uniform Bounds against Adversarial Attacks".
  - Long Beach, June 2019. ICML.

Mentorship

EPFL Master's students:
- Shuangqi Li. "On the Robustness of Generative Adversarial Networks."
- Francisco Ferrari. "Towards Neural Networks Robust Against Sparse Attacks".
- Ningwei Ma. "Adversarial Robustness for Neural Ordinary Differential Equations".
- Yulun Jiang. "Adversarial Robustness for Multiple Threat Models".
- Ziqi Zhao. "Network Pruning in Adversarial Training".
- Zhenyu Zhu. "Robust Binary Network".
- Julien Leal, Shengzhao Lei. "Learning Representations via Weak Supervision".

EPFL Bachelor's students:
- Majdouline Ait Yahia. "Robust Binary Network".

Teaching

Teaching Assistant at EPFL
- MATH-111(e) Linear Algebra. 2019-Fall, 2020-Fall.
- CS-413 Computational Photography. 2020-Spring, 2021-Spring.
  - 2020 EPFL AGEPoly IC Polysphere Awards for excellence in teaching, one course selected annually.
- EE-618 Theory and Methods for Reinforcement Learning. 2019-Spring.
- EE-556 Mathematics of Data: from Theory to Computation. 2018-Fall.