Ping-yeh Chiang

4717 Cherokee St. | College Park, MD, 20740 | (215) 688-3312 | pingyeh.chiang@gmail.com

EDUCATION

University of Maryland - College Park - College Park, MD **Sept. 2018 - Current**
Department of Computer Science
Expected Graduation Date: August 2023
Doctor of Philosophy: Computer Science
GPA: 3.88

Skills

- Computer Vision, NLP, Security & Privacy
- 7 publications in top tier ML conferences with 2 spotlights and 1 oral in 2022
- Pytorch, Tensorflow, Python, Slurm

PROFESSIONAL EXPERIENCE

Meta— Boston, MA **May 2022 - August 2022**
Research Scientist Intern
- Researched efficient method for training models robust to distribution shifts.
- Trained ViTs efficiently on AWS with PyTorch and FFCV.
- Publication resulting from the research: "Universal Pyramid Adversarial Training for Improved ViT Performance" Preprint.

Waymo— Mountain View, CA (Remote) **June 2021 - August 2021**
Perception Research Intern
- Researched methods of improving reliability of modern large scale computer vision models, such as point cloud detectors and segmentation models.
- Efficiently trained large scale vision models on hundreds of TPUs with Tensorflow.

Adobe— College Park, MD **May 2020 - August 2020**
Machine Learning Engineer Intern
- Researched robust methods of authenticating the ownership of deep learning models
- Implemented prototype for watermarking deep learning models for Adobe Document Reader, which is eventually incorporated into the product.
- Publication resulting from the research: "Certified Neural Network Watermarks with Randomized Smoothing." ICML 2022.

Amplio.ai— Chantilly, VA **May 2019 - August 2019**
Machine Learning Engineer Intern
- Built weight lifting posture analysis prototype that analyzes correctness of forms/fatigue level/strength gain using python.
- Fine tuned the state of the art pose estimation models for weight lifting analysis.
- Gathered and cleaned data from Amazon cloudcam for joints annotation.

*Equal contributors

PUBLICATIONS

Universal Pyramid Adversarial Training for Improved ViT Performance *Ping-yeh Chiang, Yipin Zhou, Omid Poursaeed, Satya Narayan Shukla, Tom Goldstein, Ser-Nam Lim*	**Under Review**
Gradient-based optimization is not necessary for generalization in neural networks *Ping-yeh Chiang, Renkun Ni, David Yu Miller, Arpit Bansal, Jonas Geiping, Micah Goldblum, Tom Goldstein*	**ICLR 2022** ***Spotlight***
Can neural nets learn the same model twice? investigating reproducibility and double descent from the decision boundary perspective *Gowthami Somepalli, Liam Fowl, Arpit Bansal, Ping Yeh-Chiang, Yehuda Dar, Richard Baraniuk , Micah Goldblum, Tom Goldstein*	**CVPR 2022** ***Oral***
Certified Watermarks for Neural Networks **Arpit Amit Bansal, *Ping-yeh Chiang, Michael Curry, Hossein Souri, Rama Chellappa, John P Dickerson, Rajiv Jain, Tom Goldstein*	**ICML 2022** ***Spotlight***
Adversarial Examples Make Strong Poisons *Liam Fowl*, Micah Goldblum*, Ping-yeh Chiang*, Jonas Geiping, Wojtek Czaja, Tom Goldstein*	**NeurIPS 2021**
Detection as Regression: Certified Object Detection by Median Smoothing *Ping-yeh Chiang, Michael J. Curry, Ahmed Abdelkader, Aounon Kumar, John Dickerson, Tom Goldstein*	**NeurIPS 2020**
Certifying Strategyproof Auction Networks **Michael J Curry, *Ping-Yeh Chiang, Tom Goldstein, John Dickerson*	**NeurIPS 2020**
Certified Defenses for Adversarial Patches **Ping-Yeh Chiang, *Renkun Ni, Ahmed Abdelkader, Chen Zhu, Chris Studor, Tom Goldstein*	**ICLR 2020**
Witchcraft: Efficient PGD Attack with Random Step Size *Ping-Yeh Chiang, Jonas Geiping, Micah Goldblum, Tom Goldstein, Renkun Ni, Steven Reich, Ali Shafahi*	**ICASSP 2020**
Compressing GANs Using Knowledge Distillation **Angeline Aguinaldo, *Ping-Yeh Chiang, *Alex Gain, *Ameya Patil, *Kolten Pearson, Soheil Feizi*	**Preprint**