

# Chia-Hung Yuan

6F, No. 18, Aly. 6, Ln. 485, Sec. 1, Guangfu Rd., Hsinchu City 300, Taiwan

+886 988812983 | jimmy.chyuan@gmail.com | Homepage | Google Scholar | GitHub | LinkedIn

## Research Interests

---

### Robust Machine Learning

I'm broadly interested in machine learning and computer security. My goal is to develop robust machine learning to reliably interact with a dynamic and uncertain world. This goal has many layers – from how to quantify uncertainty and improve robustness in decision-making procedures, to how the algorithm converges and generalizes to the unseen data.

## Education

---

### National Tsing Hua University

MASTER OF SCIENCE

Sep. 2019 – Jul. 2021

*Hsinchu, Taiwan*

- Major: Computer Science
- Advisor: Shan-Hung Wu
- Overall GPA: 4.29/4.30

### National Tsing Hua University

BACHELOR OF SCIENCE

Sep. 2014 – Jun. 2019

*Hsinchu, Taiwan*

- Major: Interdisciplinary Program of Engineering (Material Science & Quantitative Finance)
- Overall GPA: 3.95/4.30, Major GPA: 4.01/4.30, CS-related GPA: 4.16/4.30

### Eberhard Karls University of Tübingen

EXCHANGE PROGRAM

Oct. 2016 – Jul. 2017

*Tübingen, Germany*

- Major: Nano-Science

## Publications

---

### Meta Adversarial Perturbations | [Paper](#)

AAAI Workshop'22

Chia-Hung Yuan, Pin-Yu Chen, Chia-Mu Yu

*Vancouver, Canada*

- Proposed a meta adversarial perturbation (MAP), a better initialization that causes data to be misclassified with high probability after being updated through only a one-step gradient ascent update.
- MAP achieves 10-20% improvement, compared with naïve fast gradient signed method.

### Neural Tangent Generalization Attacks | [Paper](#) | [Video](#) | [Code](#) | [Competitions](#)

ICML'21

Chia-Hung Yuan, Shan-Hung Wu

*Virtual*

- Proposed generalization attack, a new direction for poisoning attacks, where an attacker aims to modify training data in order to spoil training process such that a trained network lacks generalizability.
- Devised neural tangent generalization attack (NTGA), a first efficient work enabling clean-label, black-box generalization attacks against deep neural networks.
- NTGA decreases the generalization ability sharply, i.e. 99% -> 15%, 92% -> 33%, 99% -> 72% on MNIST, CIFAR10 and 2-class ImageNet, respectively.

### Adversarial Robustness via Runtime Masking and Cleansing | [Paper](#) | [Video](#) | [Code](#)

ICML'20

Yi-Hsuan Wu, Chia-Hung Yuan, Shan-Hung Wu

*Virtual*

- Devised runtime masking and cleansing (RMC), a new defense method, to improve adversarial robustness.
- RMC achieves robustness ~98% on MNIST, ~85% on CIFAR-10, ~60% on ImageNet, respectively.

## Experiences

---

### MIT-IBM Watson AI Lab

EXTERNAL STUDENT

Oct. 2021 – Present

*Massachusetts, USA*

- Advisor: Pin-Yu Chen / Co-advisor: Chia-Mu Yu (National Chiao Tung University)

- Researched on the intersection of meta learning, neural tangent kernel (NTK) and adversarial machine learning and published a paper “**Meta Adversarial Perturbations**” in **AAAI Workshop’22**.

#### DataLab, Department of Computer Science, NTHU

Sep. 2019 – Jul. 2021

GRADUATE RESEARCH ASSISTANT

Hsinchu, Taiwan

- Advisor: Shan-Hung Wu
- Researched on neural tangent kernel (NTK) and neural network Gaussian process (NNGP). Studied properties of neural networks, including trainability and generalization ability and published a paper “**Neural Tangent Generalization Attacks**” in **ICML’21**.
- Researched on the intersection of machine learning and computer security, with a focus on adversarial example and adversarial robustness and published a paper “**Adversarial Robustness via Runtime Masking and Cleansing**” in **ICML’20**.
- Researched on computer vision, with a focus on face recognition. Designed a face recognition model with the ability to detect and resist adversarial examples, especially for real-world attacks.

#### DataLab, Department of Computer Science, NTHU

Sep. 2018 – Aug. 2019

UNDERGRADUATE RESEARCH ASSISTANT

Hsinchu, Taiwan

- Advisor: Shan-Hung Wu
- Researched on natural language processing, with focus on document ranking and passage retrieval. Designed a model for search engine query-document ranking and achieved **13<sup>th</sup> place** in MS MARCO(Microsoft MACHINE Reading COmprehensive) passage retrieval task.

#### Advanced Optoelectronic Materials Research Group, Department of Materials Science and Engineering, NTHU

Sep. 2017 – Jun. 2018

UNDERGRADUATE RESEARCH ASSISTANT

Hsinchu, Taiwan

- Advisor: Hao-Wu Lin
- Researched on next-generation organic-inorganic hybrid and nano-materials. Fabricated OLED on transparent conducting oxide by solution-process and vacuum-deposition and improved external quantum efficiency and remodeled the thin film with various materials.

#### Physics of Molecular and Biological Matter, Institute of Applied Physics, University of Tübingen

Oct. 2016 – Jul. 2017

UNDERGRADUATE RESEARCH ASSISTANT

Tübingen, Germany

- Advisor: Frank Schreiber
- Researched on topography and morphology of solar cell and coupled organic-inorganic nanostructure.

## Honors & Awards

- |   |                  |
|---|------------------|
| • <b>Honorary Member of The Phi Tau Phi Scholastic Honor Society of R.O.C.</b> (top 3% master’s graduands)      | 2021             |
| • <b>Honorary Member of The Phi Tau Phi Scholastic Honor Society of R.O.C.</b> (top 1% undergraduate graduands) | 2018             |
| • <b>Academic Achievement Award 3 times</b> (top 5% students in the class with highest GPA)                     | 2015, 2016, 2018 |
| • <b>International Exchange Scholarship</b> (200,000 NTD/~\$7,000)  | 2016             |
| • <b>1<sup>st</sup> place, Business Case Competition of Seminar on International Trade and Economy</b>          | 2016             |

## Relevant Courses

<b>ML/AI</b>	Deep Learning, Machine Learning, Quantum Machine Learning, Deep Multi-task and Meta Learning, Computer Vision, Natural Language Processing, Reinforcement Learning, Robotic Navigation and Exploration
<b>Mathematics</b>	Calculus, Linear Algebra, Probability, Engineering Mathematics

## Skills & Others

<b>Teaching Assistant</b>	CS565600 Deep Learning, National Tsing Hua University: Fall 2019, Fall 2020
<b>Paper Review</b>	NeurIPS’19-21, ICML’20-21, ICLR’21, AAAI’20-21, CVPR’21, IJCAI’20, CIKM’19-20

**Languages** Mandarin (Native); English (Fluent, TOEFL 109/120); German (Intermediate)  
**Programming** C/C++, Python, Swift, React Native, HTML, CSS, JavaScript, Matlab  
**Libraries/Tools** TensorFlow, Keras, Jax, PyTorch, OpenCV, Scikit-learn  
**Interests** Football (I have a YouTube channel!), Photography, Travel, Bartending, Ice Skating