

# Anna Yoo Jeong Ha

[annaha@uchicago.edu](mailto:annaha@uchicago.edu) • [annaha.net](http://annaha.net)

## RESEARCH INTERESTS

---

Security and Privacy; Adversarial Machine Learning

## EDUCATION

---

<b>University of Chicago</b> PhD Student, Computer Science Advised by Prof. Ben Y. Zhao and Prof. Heather Zheng	Sep. 2023 - Present
<b>Korea University, Seoul, Republic of Korea</b> Master of Electrical and Computer Engineering	Mar. 2021 – Fed. 2023
<b>Korea University, Seoul, Republic of Korea</b> Bachelor of Mechanical Engineering	Mar. 2017 - Feb. 2021

## AWARDS

---

<b>Distinguished Paper Award, 2024 CCS</b>	Oct. 2024
--	-----------

## PUBLICATIONS

---

- Anna Yoo Jeong Ha**, Josephine Passananti, Ronik Bhaskar, Shawn Shan, Reid Southen, Haitao Zheng, Ben Y. Zhao. “*Organic or Diffused: Can We Distinguish Human Art from AI-generated Images?*” Conference on Computer and Communications Security (CCS) 2024. **Distinguished Paper Award**. [\[pdf\]](#)
- Yoo Jeong Ha**, Gusang Lee, Minjae Yoo, Soyi Jung, Seehwan Yoo, and Joongheon Kim. “*Feasibility Study of Multi-Site Split Learning for Privacy-Preserving Medical Systems under Data Imbalance Constraints in COVID-19, X-Ray, and Cholesterol Dataset*”. Nature Scientific Reports, 12:1534, January 2022. [\[pdf\]](#)
- Yoo Jeong Ha**, Minjae Yoo, Gusang Lee, Soyi Jung, Sae Won Choi, Joongheon Kim, and Seehwan Yoo. “*Spatio-Temporal Split Learning for Privacy-Preserving Medical Platforms: Case Studies with COVID-19 CT, X-Ray, and Cholesterol Data*”. IEEE Access, 9:121046-121059, September 2021. [\[pdf\]](#)
- Won Joon Yun, **Yoo Jeong Ha**, Soyi Jung, and Joongheon Kim. “*Autonomous Aerial Mobility Learning for Drone-Taxi Flight Control*”. IEEE ICTC (Jeju, Korea), October 2021. [\[pdf\]](#)
- Gusang Lee, Won Joon Yun, **Yoo Jeong Ha**, Soyi Jung, Jiyeon Kim, Sunghoon Hong, Joongheon Kim, and Youn Kyu Lee. “*Measurement Study of Real-Time Virtual Reality Contents Streaming over IEEE 802.11 ac Wireless Link*”. MDPI Electronics, vol.10, no.16, pp.1967, 2021. [\[pdf\]](#)
- Yoo Jeong Ha**, Minjae Yoo, Soohyun Park, Soyi Jung, and Joongheon Kim. “*Secure Aerial Surveillance using Split Learning*”. IEEE ICUFN (Jeju, Korea), August 2021. [\[pdf\]](#)
- Hankyul Baek, **Yoo Jeong Ha**, Soyi Jung, and Joongheon Kim. “*Noise Rejection in mmWave Radar Images using Deep Learning Image Processing Methods*”. ITC-CSCC (Jeju, Korea), June 2021. [\[pdf\]](#)
- Minjae Yoo, **Yoo Jeong Ha**, Soyi Jung, and Joongheon Kim. “*CNN-based Hand Gesture Recognition Using mmWave Radar*”. ITC-CSCC (Jeju, Korea), June 2021. [\[pdf\]](#)

## PATENTS

---

- Video Processing System and Video Processing Method Using Split Learning (US Patent 11,915,477)  
Control and Recording Medium for A Medical Data Split Learning System (KR2021/016408), *waiting US*

## TEACHING ASSISTANT

---

College of Engineering - Department of Semiconductor Engineering

Sep. 2021 – Feb. 2022

## RESEARCH EXPERIENCE

---

### Computer Science Researcher

Jul. 2023 – Present

Research Assistant; Advisors: Prof. Ben Y. Zhao and Prof. Heather Zheng (University of Chicago)

- Research on the security and privacy of AI systems from an adversarial perspective to enhance model robustness and ensure safety for users.
- Develop technical solutions to protect against unethical AI practices and mitigate security vulnerabilities.

### Quantum Hyper-Driving: Quantum-Inspired Hyper-Connected and Hyper-Sensing Autonomous Mobility Technologies – NRF

Mar. 2022 – Dec. 2022

Research Assistant; Advisor: Prof. Joongheon Kim (Korea University)

- Research on ultra-dense vehicle network environment using quantum computing and build an autonomous driving system.
- Understanding network and security optimization for multimodal sensing based on quantum computing and quantum-based optimization algorithms to efficiently use large amounts of data.

### Autonomous Intelligent COA Search Methods for Cyber-Attacks – ADD

Dec. 2021 - Nov. 2022

Research Assistant; Advisor: Prof. Joongheon Kim (Korea University)

- Research on autonomous intelligent cyber threat COA detection technology (DRL, hierarchical attack representation model) in a large-scale distributed military network environment.

### Development of Privacy-reinforcing Distributed Transfer-Iterative Learning Algorithm - MHW

Research Assistant; Advisor: Prof. Joongheon Kim (Korea University)

Jul. 2019 - Nov. 2022

- Research on DisTIL, a distributed deep learning federated learning algorithm with enhanced personal information protection by utilizing three institutions' Common Data Model (CDM).

## SKILLS AND ADDITIONAL INFORMATION

---

### Languages

- Native in Korean; Fluent in English (I grew up in Australia for 12 years)

### Experimental Skills

- Python (Pytorch, Tensorflow, Matplotlib, Numpy, Pandas), Arduino, Linux, MATLAB, Latex
- AutoCAD, CREO, NX, Solidworks, Adobe Illustrator