

# EMILY WENGER

[emily.wenger@duke.edu](mailto:emily.wenger@duke.edu) ♦ [emilywenger.com](https://emilywenger.com)

## RESEARCH OVERVIEW

---

My research goals are twofold: to **make machine learning models safer** and to **give individuals agency to choose how or if they use these models in their daily life**. To accomplish these, I identify security and privacy risks in or caused by ML models and build practical tools that mitigate these vulnerabilities and empower users.

## EDUCATION

---

**Ph.D. in Computer Science**, The University of Chicago 2023

*Thesis*: Reclaiming Data Agency in the Age of Ubiquitous Machine Learning

*Advisors*: Ben Y. Zhao and Heather Zheng

**M.S. in Computer Science**, The University of Chicago 2020

*Thesis*: Backdoor Attacks Against Facial Recognition in the Physical World

**B.S. in Math and Physics**, Wheaton College (IL) 2012-2016

## EMPLOYMENT

---

<b>Assistant Professor</b>	Duke University	2024 - present
<b>Research Scientist</b>	Meta AI	2023 - 2024
<b>Research Assistant</b>	The University of Chicago	2018 - 2023
<b>Researcher</b>	Meta AI Research	Spring 2022
<b>Research Intern</b>	Meta AI Research	Fall 2021
<b>Researcher</b>	Institute for Defense Analysis (IDA)	Summer 2019
<b>Mathematician</b>	Department of Defense	2016-2018
<b>Research Assistant</b>	Wheaton College Physics Department	2013-2016

## AWARDS AND FELLOWSHIPS

---

Forbes 30 under 30, Consumer Technology	2024
Siebel Scholarship	2023
Rising Stars in EECS, UT Austin	2022
University of Chicago Harper Dissertation Fellowship	2022
Harvey Fellowship	2021
Graduate Fellowship for Stem Diversity (GFSD)	2018
University of Chicago Neubauer Fellowship	2018
Wheaton College Chase Senior Merit Scholarship	2016
National Merit Scholar Finalist	2012

## CONFERENCE PUBLICATIONS

---

Niklas Nolte\*, Mohamed Malhou\*, **Emily Wenger\***, Samuel Stevens, Cathy Li, Francois Charton, Kristin Lauter. *The Cool and the Cruel: Separating Hard Parts of LWE Secrets*. Proceedings of AFRICACRYPT, July 2024.

**Emily Wenger**, Xiuyu Li, Ben Y. Zhao, Vitaly Shmatikov. *Data Isotopes for Data Provenance in DNNs*. Proceedings of Privacy Enhancing Technologies Symposium (PETS), July 2024.

Cathy Li, Jana Sotakova, **Emily Wenger**, Zeyuan Allen-Zhu, Francois Charton, Kristin Lauter. *SALSA VERDE: A machine learning attack on Learning With Errors with sparse small secrets*. Proceedings of the 37th Conference on Neural Information Processing Systems (NeurIPS), November 2023.

Cathy Li, Jana Sotakova, **Emily Wenger**, Mohamed Malou, Evrard Garcelon, Francois Charton, Kristin Lauter. *SALSA PICANTE: A machine learning attack on LWE with binary secrets*. Proceedings of the ACM Conference on Computer and Communications Security (CCS), November 2023.

Shawn Shan, Jenna Cryan, **Emily Wenger**, Haitao Zheng, Rana Hanocka, Ben Y. Zhao. *GLAZE: Protecting Artists from Style Mimicry by Text-to-Image Models*. Proceedings of the 32nd USENIX Security Symposium, August 2023. **Winner: Distinguished Paper Award and Internet Defense Prize.**

**Emily Wenger**, Shawn Shan, Haitao Zheng, Ben Y. Zhao. *SoK: Anti-Facial Recognition Technology*. Proceedings of the 44th IEEE Symposium on Security & Privacy, May 2023.

**Emily Wenger\***, Mingjie Chen\*, Francois Charton, Kristin Lauter. *SALSA: Attacking Lattice Cryptography with Transformers*. Proceedings of the 36th Conference on Neural Information Processing Systems (NeurIPS), November 2022.

**Emily Wenger\***, Roma Bhattacharjee\*, Arjun Nitin Bhagoji, Josephine Passananti, Emi Andere. *Finding Naturally Occuring Physical Backdoors in Image Datasets*. Proceedings of the 36th Conference on Neural Information Processing Systems (NeurIPS), November 2022.

Shawn Shan, Wenxin Ding, **Emily Wenger**, Haitao Zheng, Ben Y. Zhao. *Post-breach Recovery: Protection against White-Box Adversarial Examples for Leaked DNN Models*. Proceedings of the ACM Conference on Computer and Communications Security (CCS), November 2022.

Huiying Li, Shawn Shan, **Emily Wenger**, Jiayun Zhang, Yuanshun Yao, Haitao Zheng, Ben Y. Zhao. *Blacklight: Scalable Defense for Neural Networks against Query-Based Black-Box Attacks*. Proceedings of the 31st USENIX Security Symposium, August 2022.

**Emily Wenger**, Max Bronckers, Christian Cianfarani, Jenna Cryan, Angela Sha, Haitao Zheng, Ben Y. Zhao. *“Hello, It’s Me”: Deep Learning-based Speech Synthesis Attacks in the Real World*. Proceedings of the ACM Conference on Computer and Communications Security (CCS), November 2021.

**Emily Wenger**, Josephine Passananti, Arjun Bhagoji, Yuanshun Yao, Haitao Zheng, Ben Y. Zhao. *Backdoor Attacks Against Deep Learning Systems in the Physical World*. Proceedings of the IEEE / CVF Computer Vision and Pattern Recognition Conference (CVPR), June 2021.

Shawn Shan\*, **Emily Wenger\***, Jiayun Zhang, Huiying Li, Haitao Zheng, Ben Y. Zhao. *Fawkes: Protecting Personal Privacy against Unauthorized Deep Learning Models*. Proceedings of the 29th USENIX Security Symposium, August 2020.

Shawn Shan, **Emily Wenger**, Bolun Wang, Bo Li, Haitao Zheng, Ben Y. Zhao. *Gotta Catch ‘Em All: Using Honeypots to Catch Adversarial Attacks on Neural Networks*. Proceedings of the ACM Conference on Computer and Communications Security (CCS), November 2020.

## PREPRINTS

**Emily Wenger**, Eshika Saxena, Mohamed Malhou, Ellie Thieu, Kristin Lauter. *Benchmarking Attacks on Learning with Errors*. In Submission.

Samuel Stevens, **Emily Wenger**, Cathy Li, Eshika Saxena, Francois Charton, Kristin Lauter. *SALSA Fresca: Angular Embeddings and Pre-Training for ML Attacks on LWE*. In Submission.

**Emily Wenger\***, Francesca Falzon\*, Josephine Passananti, Haitao Zheng, Ben Y. Zhao. *Assessing Privacy Risks from Feature Vector Reconstruction Attacks*.

Huiying Li, **Emily Wenger**, Ben Y. Zhao, Haitao Zheng. *Piracy Resistant Watermarks for Deep Neural Networks*.

## TEACHING

---

<b>AI Security and Privacy</b>	Duke University	Fall 2024
<b>Cryptocurrencies (TA)</b>	The University of Chicago	Winter 2019
<b>Introductory Cryptography (TA)</b>	WAM Program at the Institute for Advanced Studies	May 2018

## GRADUATE RESEARCH ADVISING

---

\*co-first authors

Steven Seiden	PhD, Electrical & Computer Engineering, Duke University	2024-present
Hung Ahn Vu	PhD, Electrical & Computer Engineering, Duke University	2024-present

## UNDERGRADUATE RESEARCH ADVISING

Emilio Andere	B.S. Computer Science, University of Chicago	2022
William Zhu	B.S. Computer Science, Yale (exp. 2026)	Summer 2022
Irene Liu	Illinois Math and Science Academy	Summer 2022
Josephine Passananti	B.S. Computer Science, University of Chicago → Ph.D., UChicago	2018-22
Roma Bhattacharjee	B.S. Computer Science, Princeton University (exp. 2025)	2021-22
Angela Sha	B.S. Computer Science, University of Chicago → Apple	2020-21
Maximiliaan Bronckers	B.S. Computer Science, University of Chicago → M.S., Cambridge	2020-21
Talia Gifford	B.S. Physics, University of Chicago→ US Government	2019-21
Esin Onal	B.S. Computer Science, University of Chicago → Deloitte	2020-21

## MEDIA COVERAGE

SALSA: Attacking LWE using ML

- **NewsWeek:** *How AI and quantum computing are challenging the security of our digital future*

Glaze: Protecting Artists from Style Mimicry

- **CNN:** *‘It gave us some way to fight back’: New tools aim to protect art and images from AI’s grasp*
- **BBC News:** *Can artists protect their work from AI?*
- **TechCruch:** *Glaze protects art from prying AIs*
- **New York Times:** *This Tool Could Protect Artists From A.I.-Generated Art That Steals Their Style*
- And many more (see [here](#) for a full list)

Fawkes: Image Cloaking for Personal Privacy

- **MIT Tech Review:** *How to stop AI from recognizing your selfies*
- **New York Times:** *This Tool Could Protect Your Photos From Facial Recognition*
- **Nature Communications:** *Resisting the Rise of Facial Recognition*
- **Verge:** *Cloak your photos with this AI privacy tool to fool facial recognition*
- **The Register (UK):** *Sick of AI engines scraping your pics for facial recognition? Here’s a way to Fawkes them right up*
- **Die Zeit (Germany):** *Die unsichtbare Maske (The Invisible Mask)*
- And many more (see [here](#) for a full list)

Deep-Learning Based Speech Synthesis Attacks

- **New Scientist:** *AI-generated deepfake voices can fool both humans and smart assistants*

## EXTERNAL WRITING

“AI produces gibberish when trained on too much AI-generated data”, **Nature News & Views**, July 2024.

## INVITED TALKS

“Benchmarking Attacks on Learning with Errors”

**Joint Mathematics Meeting**, January 2025

**US National Institute of Standards and Technology**, August 2024

“Towards Security and Regulated Machine Learning Systems”

**Duke University**, March 2023

**University of Washington**, March 2023

**University of Virginia**, March 2023

**Northeastern University**, March 2023

**Carnegie Mellon University**, March 2023

**University of Texas - Austin**, February 2023

**University of Wisconsin - Madison**, February 2023

**Boston University**, January 2023

“Towards More Realistic Threat Models in Adversarial Machine Learning”

**SPML Seminar**, September 2022

**Duke University**, April 2022

**University of Wisconsin - Madison**, April 2022

**Northeastern University**, May 2022

“Hello, It’s Me: Deep Learning-based Speech Synthesis Attacks in the Real World”

“**Speech as PII**” **Lorentz Center Workshop**, November 2021

**Facebook**, October 2021

“Fawkes: Protecting Personal Privacy against Unauthorized Deep Learning Models”

**Royal Holloway, University of London**, February 2022

**Microsoft Research Privacy & Cryptography Group**, June 2021

**Facebook**, October 2020

“**Are You a Robot?**” **Podcast** October 2020

**The Brave Foundation**, August 2020

**Boehringer-Ingelheim**, August 2020

**Infosec Podcast**, July 2020

“Piracy Resistant Watermarks for Deep Neural Networks,” EE380, **Stanford University**, November 2019

Plenary speaker, **Beyond the Binary Conference** at The University of Hartford, April 2019

## CONFERENCE AND WORKSHOP COMMITTEES

---

PC Member, <i>IEEE Security &amp; Trustworth ML (SatML)</i>	2025
PC Member, <i>IEEE Security &amp; Privacy</i>	2024, 2025
PC Member, <i>NeurIPS Trustworthy and Socially Responsible Machine Learning (TSRML)</i>	2022
Reviewer, <i>NeurIPS Datasets and Benchmarks Track</i>	2022
External Reviewer, <i>ACM Conference on Computer and Communications Security (CCS)</i>	2022
PC Member, <i>Workshop on Dependable and Secure Machine Learning (DSML)</i> (co-located with DSN)	2022
Reviewer, <i>IEEE Transactions on Pattern Analysis and Machine Intelligence</i>	2021

## LEADERSHIP

---

Advisor and Contributing Fellow, [AI & Faith](#) (2023-present)

Founding Member and Senior Editor, [AI & Faith](#) (2020-2023)

Curatorial team member for “Traced & Traced” exhibit, [Science Gallery Detroit](#) (2020-2021)

Student Organizer, Graduate Research Opportunities for Women (GROW) Conference (2020)

Member of UChicago CS student leadership team (2020-2021)

Student representative for UChicago CS graduate admissions committee (2019-2020)

## **OUTREACH AND VOLUNTEERISM**

---

Elementary school visit host (University of Chicago Computer Science Department)

Math tutor for Hope Scholars after-school program (Woodlawn, Chicago)