# EMILY WENGER

emily.wenger@duke.edu ◇ emilywenger.com

## RESEARCH OVERVIEW

I study novel security and privacy issues arising as machine learning models become bigger, better, and ubiquitous, and I build practical, user-centric tools to solve these problems.

## 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) 2016

## EMPLOYMENT

| | | |
|---|---|---|
| **Assistant Professor** | Duke University | 2024 - now |
| **Research Scientist** | Meta AI | 2023 - 2024 |
| **Research Assistant** | The University of Chicago | 2018 - 2023 |
| **Mathematician** | Department of Defense | 2016 - 2018 |

## 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

15. **Emily Wenger**, Eshika Saxena, Mohamed Malhou, Ellie Thieu, Kristin Lauter. *Benchmarking Attacks on Learning with Errors.* Proceedings of the 46th IEEE Symposium on Security & Privacy, May 2025 (to appear).

14. 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.

13. **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.

12. 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.

11. 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.

10. 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.**

9. **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.

8. **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.

7. **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.

6. 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.

5. 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.

4. **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.

3. **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.

2. Shawn Shawn*, **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.

1. 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

4. Eshika Saxena, Alberto Alfarano, **Emily Wenger**, Kristin Lauter. *Teaching Transformers Modular Arithmetic at Scale.* In Sumbmission.

3. 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.

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

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

## TEACHING

| | | |
|---|---|---|
| **AI Security and Privacy** | Duke University | Fall 2024 |
| **Cryptocurrencies** (TA) | The University of Chicago | Winter 2019 |
| **Introductory Cryptography** (TA) | 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

| | | |
|---|---|---|
| Kaden Chien | B.S. Computer Science & Math, Duke University (exp. 2027) | 2024-present |
| Karstan Bock | B.S. Computer Science & ECE, Duke University (exp. 2027) | 2024-present |
| Claire Luo | B.S. Computer Science & Statistics, Duke University (exp. 2027) | 2024-present |
| Sahana Sreerem | B.S. Computer Science & Statistics, Duke University (exp. 2027) | 2024-present |
| Caroline Zhang | B.S. Computer Science & Math, Duke University (exp. 2027) | 2024-present |
| Taein Kim | B.S. Computer Science & ECE, Duke University (exp. 2027) | 2024-present |
| Josiah Crossman | B.S. Computer Science, Duke University (exp. 2027) | 2024-present |
| Andres Torrubia Bustos | B.S. Computer Science, Duke University (exp. 2027) | 2024-present |
| Amir Ergashev | B.S. Computer Science, Duke University (exp. 2025) | 2024-present |
| 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 |

## THESIS COMMITTEES

| | | |
|---|---|---|
| Sohini Saha | PhD Thesis: "Robust Deep Learning (DL)-based approach for speech enhancement in Cochlear Implants (CI) in dynamic acoustic environments" | Duke University, exp. 2025 |
| Mariia Zameshina | PhD Thesis: "Advancing ethical AI: fairness, diversity, and privacy in generative modeling" | EISEE/Meta, 2024 |

## SELECTED MEDIA

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*

Op-Eds and External Writing

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

## INVITED TALKS

"Reclaiming Data Agency in the Age of Ubiquitous Machine Learning"

**UCSD**, August 2024

"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-Ingleheim**, 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, *ACM CCS* | 2025 |
| PC Member, *IEEE Security & Trustworthy ML (SatML)* | 2025 |
| PC Member, *IEEE Security & Privacy* | 2024, 2025 |
| PC Member, *NeurIPS Trustworthy and Socially Responsible Machine Learning (TSRML)* | 2022 |
| Reviewer, *NeurIPS Datasets and Benchmarks Track* | 2022 |
| External Revewier, *ACM Conference on Computer and Communications Security (CCS)* | 2022 |
| PC Member, *Workshop on Dependable and Secure Machine Learning (DSML)* (co-located with DSN) | 2022 |
| Reviewer, *IEEE Transactions on Pattern Analysis and Machine Intelligence* | 2021 |

## EVENTS ORGANIZED

Session Organizer, Special Session on AI & Cryptography, Joint Mathematics Meetings (JMM), 2025 (joint with Shi Bai and Kristin Lauter)

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

## LEADERSHIP/EXTERNAL SERVICE

Faculty Advisor, Duke Applied Machine Learning Club (2024-present)

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)

## OUTREACH AND VOLUNTEERISM

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

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