Yuanchen (Cathy) Li

(415)509-9350 yuanchen@uchicago.edu https://cathyliyuanchen.github.io/

Research Interests

Machine Learning, Security and Privacy, Cryptography

Education

University of Chicago 2023.9 - Present
Ph.D. in Computer Science.
Awards: Neubauer Fellowship.

University of California, Berkeley 2017.8 - 2020.12
B.A. in Computer Science, Statistics, Applied Mathematics, Cognitive Science, Linguistics, and Data Science.
Awards: Magna cum laude (GPA: 3.88/4.00). Upsilon Pi Epsilon. Phi Beta Kappa.

Publications

1. "Understanding Implosion in Text-to-Image Generative Models"
   Wenxin Ding, Cathy Y. Li, Shawn Shan, Ben Y. Zhao, Haitao Zheng
   Proceedings of the ACM Conference on Computer and Communications Security (CCS), Oct 2024.
2. "Inception Attacks: Immersive Hijacking in Virtual Reality"
   Zhuolin Yang, Cathy Y. Li, Arman Bhalla, Ben Y. Zhao, Haitao Zheng
   In submission.
3. "SALSA Fresca: Angular Embeddings and Pre-Training for ML Attacks on LWE"
   Samuel Stevens, Emily Wenger, Cathy Li, Eshika Saxena, François Charton, Kristin Lauter
   In submission.
4. "The Cool and the Cruel: Separating Hard Parts of LWE Secrets"
   Niklas Nolte*, Mohamed Malhou*, Emily Wenger*, Samuel Stevens, Cathy Y. Li, François Charton, Kristin Lauter
   AFRICACRYPT, July 2024.
5. "An efficient algorithm for integer lattice reduction"
   François Charton, Kristin Lauter, Cathy Y. Li, Mark Tygert
   SIAM Journal on Matrix Analysis and Applications (SIMAX), 45 (1): 353-367, 2024.
6. "SALSA Verde: a machine learning attack on Learning With Errors with sparse small secrets"
   Cathy Y. Li, Emily Wenger, Zeyuan Allen-Zhu, François Charton, Kristin Lauter
   Proceedings of the 37th Conference on Neural Information Processing Systems (NeurIPS), Nov 2023.
7. "SALSA Picante: a machine learning attack on LWE with binary secrets"
   Cathy Y. Li, Jana Sotáková, Emily Wenger, Mohamed Malhou, Evrard Garcelon, François Charton, Kristin Lauter
   Proceedings of the ACM Conference on Computer and Communications Security (CCS), Nov 2023.

Employment

Ph.D. Student, University of Chicago 2023.9 - Present
Advisors: Prof. Ben Y. Zhao and Prof. Heather Zheng

- Leading a research project on certifying human-created images using cryptographic signatures.
- Proposed a theoretical framework to understand poison attacks on generative models.
- Proposed a multifaceted defense pipeline on an immersive hijacking attack on virtual reality systems.

AI Resident, Meta 2022.7 - 2023.7
Mentors: Prof. Kristin Lauter and François Charton

- Main contributor of the cryptanalysis with ML project. Proposed and implemented innovative ideas to improve data preprocessing, model training, and secret recovery algorithms.

- Scaled up the attack to solve LWE problems of larger dimensions (from 128 to 512), smaller modulus, and broader secret type. Improved the attack time to outperform state-of-the-art.

Software Engineer, Productiv 2021.6 - 2022.7

- Built a workflow engine to standardize workflows. Wrote backend APIs and shipped features in the product that allows customers to automatically off-board employees, and customize license management configurations according to app engagement data. Presented a demo in the company all-hands.
- Provided timely technical solutions to customer inquiries as the backend on-call of the engineering team.

Research Assistant, Real-time Intelligent Secure Explainable Systems Lab, UC Berkeley 2019.5 - 2021.5

Mentor: Prof. Joseph Gonzalez

- Worked with PhD students on Computer Vision and Machine Learning projects, and presented in lab seminars.
- Observed spatial bias in data and sparsity of feature maps and demonstrated a tradeoff between restriction for a convolution and accuracy on a segmentation model. Proposed leveraging spatial biases to save computation.
- Designed a CNN to predict diagnosis from electrocardiograms (EKG) signals; implemented the neural network from scratch and trained on a large scale EKG dataset from UCSF, visualizing the attention.

Teaching

Teaching Assistant, University of Chicago 2024.1 - 2024.3

Course: CMSC 23400: Mobile Computing

(Head) Undergraduate Student Instructor, UC Berkeley 2019.8 - 2020.12

Course: CS 188 - Artificial Intelligence, an upper division course with 800 enrolled students

- 4 Semesters as (Head) TA. Led staff of TAs and readers; assisted in course logistics and administrative responsibilities; organized staff meetings and mentored new TAs; worked on content (notes and assignments) creation.
- Organized exam creation/proctoring/grading; created exam questions; made and revised exam drafts.
- Held discussions and office hours, and answered student questions on the online Q&A platform.

Volunteer

Organizer, Diversifying Access to Research in Engineering, UC Berkeley 2019.8 - 2020.6

- Helped matching undergraduate students with research opportunities in EECS and to promote diversity.

Skills

Proficient in Python (Pytorch, NumPy, Pandas, Scikit-learn, Matplotlib), Node.js, R (ggplot2), SQL, Unix, Git, Latex.
Spoken languages: Mandarin (native), English (working proficiency), Swedish (elementary).