Marina Zhang

Email: marinazhang2000@gmail.com
Website: marinazhang.github.io

Education

2017 - 2021 **Massachusetts Institute of Technology (MIT)**, *Cambridge, MA*
B.S. in Computer Science and Engineering, B.S. in Mathematics, Minor in Economics
GPA: 5.0/5.0
Relevant Coursework: Machine Learning, Computer Vision, Computational Cognitive Science, Cryptography, Algorithms, Information Theory, Statistics, Real Analysis

Experience

Jun 2021 - Present **Google**, Security & Anti-Abuse Research Team
Senior Software Engineer

- Building adversarially robust, multilingual, and efficient NLP models using novel metric learning techniques, such as RETSim [1] and RETVec [3]. Deployed large-scale security and anti-abuse protections based on our research in multiple Google products (Gmail, YouTube, Workspace), e.g. blocking billions of spam emails in Gmail daily.
- Investigating novel applications of ML for security, such as LLMs for code vulnerability detection, AI-powered file-type detection [2], and side-channel attacks on cryptographic hardware [4].
- Conducting research on the security and privacy of LLMs, including on-device text safety protections (Google I/O 2023 demo and launched for Android), as well as data-centric approaches to reduce privacy risk and improve generalization capabilities.

Sep 2020 - Jun 2021 **University of Pennsylvania**, Department of Neuroscience
Research Assistant, advised by Prof. Wenqin Luo

- Designed the convolutional recurrent neural network (CRNN) used for Scratch-AID, a deep learning-based tool which can automatically identify and quantify mouse scratching behavioral patterns from raw video footage [6].
- Investigated the neurobiological relationship between behavioral states and breathing patterns using clustering techniques; built a classifier capable of distinguishing between 9 different behavioral states in rodents using breathing recordings [5].

Jun 2020 - Aug 2020 **Google**, Security & Anti-Abuse Research Team
Software Engineer Intern, hosted by Elie Bursztein

- Built a deep-learning model training framework for security research, which supported state-of-the-art model training techniques including hyperparameter tuning, semi-supervised labeling, and transfer learning.
- Designed and wrote a TensorFlow/Keras package which automates searching for and applying the best data augmentation policies during model training.

Sep 2019 - Dec 2019 **MIT CSAIL**, Medical Vision Group
Research Assistant, advised by Prof. Polina Golland

- Built an ML model for automatically quantifying the severity of pulmonary edema from patients' x-ray images and radiology reports, helping to improve clinicians' abilities to provide more accurate and personalized treatment plans for heart failure patients.

Jun 2019 - Aug 2019 **Microsoft**, Edge Browser Experiences Team
Software Engineer Intern

- Designed and shipped the quick-access Favorites toolbar button and drop-down menu in Microsoft Edge.

Papers

[1] **Marina Zhang**, Owen Vallis, Aysegul Bumin, Tanay Vakharia, and Elie Bursztein. "RETSim: Resilient and Efficient Text Similarity." In *International Conference on Learning Representations (ICLR)*, 2024. [Link]

[2] Yanick Frantantonio, Luca Invernizzi, Loua Farah, Kurt Thomas, **Marina Zhang**, ..., Elie Bursztein. "Magika: AI-Powered Content Type Detection." Under review at *International Conference on Software Engineering (ICSE) 2025*. [Link]

[3] Elie Bursztein, **Marina Zhang**, Owen Vallis, Xinyu Jia, and Alexey Kurakin. "RETVec: Resilient and Efficient Text Vectorizer." In *Advances in Neural Information Processing Systems (NeurIPS)*, 2023. [Link]

[4] Elie Bursztein, Luca Invernizzi, Karel Král, Daniel Moghimi, Jean-Michel Picod, and **Marina Zhang**. "Generic Attacks against Cryptographic Hardware through Long-Range Deep Learning." In *Conference on Cryptographic Hardware and Embedded Systems (CHES)*, 2024. [Link] *(alphabetical authorship)*

[5] Emma Janke, **Marina Zhang**, Sang Eun Ryu, Janardhan Bhattarai, Mary Schreck, Andrew Moberly, Wenqin Luo, Long Ding, Daniel Wesson, and Minghong Ma. "Machine Learning-based Clustering and Classification of Mouse Behaviors via Respiratory Patterns." In *iScience (Cell Press) Vol. 25*, 2022. [Link]

[6] Huasheng Yu, et al. "Scratch-AID: A Deep-learning Based System for Automatic Detection of Mouse Scratching Behavior with High Accuracy." In *eLife Vol. 11*, 2022. [Link]

Open-Source Projects

2024 **Magika: AI-Powered Content-Type Detection**, *Contributor*
Package for efficiently and accurately detecting file content types with deep learning [2]. 7k+ stars on GitHub.

2024 **UniSim: Universal Similarity**, *Main Contributor*
UniSim is a Python package for efficient similarity computation, fuzzy matching, and data clustering using similarity embeddings [1].

2023 **RETVec: Resilient and Efficient Text Vectorizer**, *Main Contributor*
The RETVec package offers an easy-to-use TensorFlow/Keras API for RETVec, an efficient, multilingual, and robust text vectorizer from our research [3].

2021 **TensorFlow Similarity: Metric Learning for Humans**, *Contributor*
TensorFlow Similarity is a TensorFlow library for similarity learning, including algorithms and models for self-supervised learning, metric learning, and contrastive learning.

Awards & Honors

2024 NSF GRFP Fellowship Recipient
2020 Tau Beta Pi (TBP) Honor Society
2020 IEEE Eta Kappa Nu (IEEE-HKN) Honor Society
2020 MIT EECS Undergraduate Research and Innovation Scholar
2018, 2019 2x ITA Scholar-Athlete Award
2018, 2019 2x NCAA Championship Elite Eight (MIT Women's Tennis)
2017 National Merit Scholarship Winner
2017 National AP Scholar

Activities

2022 - 2024 **Google Intern Host**
Hosted/co-hosted two Research Scientist interns and two SWE interns at Google

2020 - 2021 **MIT IEEE-HKN Tutor for EECS**
Tutor for 6.009 Fundamentals of Programming and 6.006 Introduction to Algorithms

2019 - 2020 **MIT xFair Committee**
Organizational committee for xFair, MIT's largest student-run career fair and tech expo

2019 - 2020 **MIT UA Innovation Committee**
Worked on projects to improve student life, study spaces, and mental health at MIT

2017 - 2019 **MIT Varsity Tennis Team**
2x NCAA Elite 8; 2x ITA Scholar-Athlete; 2x NEWMAC First Team All-Conference