

# Leslie Rice

7121 Gates Hillman Center  
Carnegie Mellon University  
Pittsburgh, PA 15213

larice@cs.cmu.edu  
<http://cs.cmu.edu/~larice>

## Education

**Carnegie Mellon University**  
Ph.D. in Computer Science

Pittsburgh, PA, *August 2018 - Present*

**The University of Texas at Austin**  
B.S. in Computer Science  
B.S. in Mathematical Sciences, Specialization in Statistics, Probability & Data Analysis

Austin, TX, *August 2013 - May 2017*

## Research Experience

**Carnegie Mellon University**  
*Graduate Research Assistant* (Advisor: J. Zico Kolter)  
Research on adversarial robustness in deep learning.

Pittsburgh, PA, *August 2018 - Present*

**Bosch Center for Artificial Intelligence**, *Machine Learning Research Intern*  
Researched certified defenses against adversarial patch attacks.

Pittsburgh, PA, *May - Present*

**The University of Texas at Austin**  
*Undergraduate Research Assistant* (Advisor: Robert A. van de Geijn)  
Researched practical, Strassen-like fast matrix multiplication algorithms and performance optimization for the k-nearest neighbors kernel.

Austin, TX, *August - December 2016*

**Texas Institute for Computational Engineering and Sciences**  
*Moncrief Undergraduate Summer Research Intern* (Advisor: Robert A. van de Geijn)  
Researched dense matrix multiplication performance optimization using Strassen's algorithm.

Austin, TX, *June - August 2016*

**Applied Research Laboratories at the University of Texas at Austin**, *Undergraduate Research Assistant*, Space and Geophysics Lab  
Developed anomaly detection algorithms for geospatial data.

Austin, TX, *September 2014 - May 2015*

## Publications

**Robustness between the worst and average case**  
Leslie Rice, Anna Bair, Huan Zhang, J. Zico Kolter  
*Neural Information Processing Systems (NeurIPS) 2021*

**Overfitting in adversarially robust deep learning**  
Leslie Rice\*, Eric Wong\*, J. Zico Kolter  
*International Conference on Machine Learning (ICML) 2020*

**Fast is better than free: Revisiting adversarial training**  
Eric Wong\*, Leslie Rice\*, J. Zico Kolter  
*International Conference on Learning Representations (ICLR) 2020*

**Generating Families of Practical Fast Matrix Multiplication Algorithms**  
Jianyu Huang, Leslie Rice, Devin A. Matthews, Robert A. van de Geijn  
*IEEE International Parallel & Distributed Processing Symposium (IPDPS) 2017*

**Performance Optimization for the K-Nearest Neighbors Kernel using Strassen's Algorithm**  
Leslie Rice  
*Undergraduate Honors Thesis, The University of Texas at Austin, 2017*

\*Equal contribution

## Industry Experience

**Uber Advanced Technologies Group**, *Software Engineer*  
Developed web-based camera image labeling tools, built active learning system for image classification, and engineered autolabeling capabilities.

Pittsburgh, PA, *March 2017 - August 2018*

**Able Lending**, *Software Engineer*  
Built data science pipeline for finding small business customers, and developed internal and customer-facing software for managing small business loans.

Austin, TX, *June 2015 - January 2016*

## Invited Talks

**Implementing Strassen-Like Fast Matrix Multiplication Algorithms  
with BLIS** (*with Jianyu Huang*), BLIS Retreat, The University of Texas at Austin

Austin, TX, *September 2016*

## Teaching

**Carnegie Mellon University**, *Graduate Teaching Assistant*  
Deep Learning Systems: Algorithms and Implementation (10-414/714)

Pittsburgh, PA, *August - December 2021*

**Carnegie Mellon University**, *Graduate Teaching Assistant*  
Practical Data Science (15-388/688)

Pittsburgh, PA, *August - December 2018*

**The University of Texas at Austin**, *Undergraduate Teaching Assistant*  
Principles of Computer Systems (CS-439)

Austin, TX, *January - May 2016*

## Professional Activities

Reviewer for NeurIPS 2021

Reviewer for the ICLR 2021 workshop “Robust and Reliable Machine Learning in the Real World”

Organizer of the ICML 2021 workshop “A Blessing in Disguise: The Prospects and Perils of Adversarial Machine Learning”

Served on the 2021 PhD admissions committee for the CMU Computer Science Department