Yang Du | CS

University of Michigan – Ann Arbor – MI, United States

+1 (734)747-3879 • duyung@umich.edu • young-du.github.io

Ph.D. student in Computer Science. Research interests: applied cryptography, secure and trustworthy system.

Education

University of Michigan (Ann Arbor) — Michigan, United States
Ph.D. in Computer Science — *Aug, 2021 - current*

University of Michigan (Ann Arbor) — Michigan, United States
B.S.E. in Computer Science — *Sep, 2019 - May, 2021*

Shanghai Jiao Tong University — Shanghai, China
B.S.E. in Electrical and Computer Engineering — *Sep, 2017 - Aug, 2019*

Research Projects

Snapshot-Oblivious RAMs: Sub-Logarithmic Efficiency for Short Transcripts
Advisor: Prof. Paul Grubbs, CSE Dept, University of Michigan — *Jun, 2021 - Present*

- Devise a new oblivious RAM emulator to hide the access pattern from an adversary that can only observe memory access from a short transcript.
- Determine the statistical and computational lower bound for such an oblivious RAM that uses constant client storage, for ball-and-bin model.

Oblivious Data Structure and Searching Algorithm
Advisor: Prof. Elaine Shi, CS Dept, Carnegie Mellon University — *Apr, 2020 - Present*

- Devise an oblivious range searching data structure and a searching algorithm based on path and circuit ORAM, using the idea of k-d tree, range tree, fractional cascading and compare the efficiency. Create a reference implementation.
- Determine a way to obliviously build the oblivious range tree and extend to higher dimension. Find a real life application on Covid-19 exposure tracking.
- Implement an oblivious AVL tree data structure with Path ORAM and reverse deterministic lexicographic eviction.

Efficient Algorithm to Find Number of Prime Factors of Integer with Oracle
Advisor: Dr. Ilya Volkovich, CSE Dept, University of Michigan — *Apr, 2020 - Sep, 2020*

- Devise the first efficient deterministic algorithm for approximating $\omega(N)$ the number of prime factors of an integer given in addition oracle access to Euler's Totient function.
- Show that the algorithm can be extended to handle a more general class of additive functions that "depend solely on the exponents in the prime factorization of an integer"
- Gives the first algorithm that approximates $\omega(N)$ without necessarily factoring N.

Publication

Yang Du, Ilya Volkovich, ***Approximating the Number of Prime Factors Given an Oracle to Euler's Totient Function***, in proceedings of FSTTCS 2021.

Key Academic Projects

Cryptocurrency and Blockchain
Guide: Prof. Mahdi Cheraghchi, CSE Dept, University of Michigan — *Mar, 2020 - Apr, 2020*

- Study Bitcoin (public key encryption) and Z-cash (zero-knowledge proof).
- Blockchain application to e-voting and supply chain tracking.

Deep Learning Techniques for Classification and Feature Learning
Guide: Dr. Kutty Sindhu Krishnan, CSE Dept, University of Michigan — *Feb, 2020 - Apr, 2020*

- Use Pytorch to classify pictures different types of food.
- Compare different methods: NN, CNN, Autoencoder.

Probablisitic methods to analyze Police Shootings in the United States
Guide: Dr. Horst Hohberger, Shanghai Jiao Tong University *Feb, 2019 - Apr, 2019*

- Derive confidence intervals for a parameter of a Poisson distribution.
- Using Nelson's formula, obtain 95% prediction intervals for the number of mass shootings in 2019.

Teaching Experience and Internship

Introduction to Cryptography, Instructional Aide
Instructor: Prof. Mahdi Cheraghchi, CSE Dept, University of Michigan *Jan, 2021 - May, 2021*

- Lead weekly discussion session, hold office hours.
- Grade homework and exam paper.

Linear Algebra, Proof Tutor
Instructor: Dr. Scott Schneider, Maths Dept, University of Michigan *Jan, 2020 - Dec, 2021*

- Hold office hours to discuss homework questions with students.

Foundation of Computer Science, Grader
Instructor: Dr. Amir Kamil, CSE Dept, University of Michigan *Sep, 2019 - May, 2020*

- Grade homework and exam paper.

Linear Algebra, Teaching Assistant
Instructor: Prof. Olga Danilkina, Shanghai Jiao Tong University *Feb, 2019 - May, 2019*

- Lead weekly discussion session.
- Grade homework and exam paper.

Honors Mathematics II, Teaching Assistant
Instructor: Prof. Horst Hohberger, Shanghai Jiao Tong University *Sep, 2018 - Dec, 2018*

- Lead weekly discussion session.
- Grade homework and exam paper.

Software Engineer of Developing a Teaching Management System
Shanghai Suxun Education Ltd. *Dec, 2018 - Feb, 2019*

- Front end(Android) development.
- Design and format API and design data structure to minimize data transferred.

Scholastic Achievements

- **James B. Angell Scholar** awarded by University of Michigan *Mar, 2021*
- **Roger King Scholarship** awarded by University of Michigan *Aug, 2020*
- **Dean's Honors List** awarded by University of Michigan *Dec, 2019; Dec, 2020*
- **University Honors** awarded by University of Michigan *Dec, 2019; Apr, 2020; Dec, 2020*
- **Fuda Scholarship** awarded by Shanghai Jiao Tong University *Nov, 2018*
- **Bronze Medalist of the 9th University Physics Competition** *Oct, 2018*
- **Undergraduate Merit Scholarship** awarded by Shanghai Jiao Tong University *Nov, 2018; Nov, 2019*

Technical Strengths

- **Programming Languages:** C/C++, Python, Java
- **Development:** Android
- **Others:** LaTeX, Matlab, Mathematica, Origin