

# TIANYI LIU

435 Nagle St, College Station, Texas, USA

<https://liutianyi.site>    [tianyi@tamu.edu](mailto:tianyi@tamu.edu)

## EDUCATION

---

**UIUC**

*Advised by Yupeng Zhang*

**IL, USA**

*Aug. 2023 - Expected July 2026*

**Texas A&M University**

*Advised by Yupeng Zhang and Juan Garay*

**TX, USA**

*Aug. 2021 - Aug. 2023*

**Shanghai Jiao Tong University**

**Bachelor of Engineering (BE)** in Computer Science

Graduated from **ACM Honor Class**, an elite CS program for top 5% of students.

**Shanghai, China**

*Sept. 2016 - July 2020*

## PUBLICATIONS

---

**Pianist: Scalable ZK-Rollups via Fully Distributed Zero-Knowledge Proofs** [\[slides\]](#)

*(Accepted by S&P 2024)*

**zkCNN: Zero Knowledge Proofs for Convolutional Neural Network Predictions and Accuracy** [\[pdf\]](#) [\[code\]](#)

Tianyi Liu, Xiang Xie, Yupeng Zhang.

*(Accepted by CCS 2021)*

**Doubly Efficient Interactive Proofs for General Arithmetic Circuits with Linear Prover Time** [\[pdf\]](#) [\[code\]](#)

Jiaheng Zhang, Tianyi Liu, Weijie Wang, Yinuo Zhang, Dawn Song, Xiang Xie, Yupeng Zhang.

*(Accepted by CCS 2021)*

## RESEARCH EXPERIENCE

---

**Crypto Group, UIUC**

*Advised by Yupeng Zhang on Cryptography*

**IL, USA**

*Aug. 2021 - Expected July 2026*

- Mainly worked on **interactive zero knowledge proof** and its applications.

**Crypto Group, University of California, Berkeley**

*Advised by Sanjam Garg on Cryptography*

**CA, USA**

*July 2019 - Dec. 2019*

- Mainly worked on **identity-based lossy trapdoor function** and **n-KDM security**.

**LATTICE Lab, Shanghai Jiao Tong University**

*Advised by Yu Yu on Cryptography*

**Shanghai, China**

*July 2018 - July 2020*

- Mainly worked on **lattice-based homomorphic encryption**, **proof of sequential work**, and **PSI**.

## WORK EXPERIENCE

---

**Microsoft Research**

*Research Intern*

**WA, USA**

*May 2023 - Aug. 2023*

- Worked on developing new applications with some succinct argument schemes.

**Google LLC.**

*Software Engineering Intern*

**CA, USA**

*May 2022 - Aug. 2022*

- Worked on supporting certificate-based authentication of IKEv2 in a distributed system, using **Go** as the programming language.

## Matriclements

Shanghai, China

Algorithm Intern, supervised by Xiang Xie

June 2020 - July 2021

- Worked on the first track of **iDASH Privacy & Security Workshop 2020**, reached 91% accuracy in the final test and generate inferences for the testing dataset within only 1min.
- Published **two CCS papers** advised by Prof. Yupeng Zhang and Dr. Xiang Xie which are mainly related to zero knowledge proof.

## HONORS AND AWARDS

---

### Programming Competition

- **The Second Runner-up (3/255)** in The 2017 China Collegiate Programming Contest *Oct. 2017*
- **Champion (1/85)** in The 2017 Chinese Collegiate Programming Contest Woman Final *Mar. 2017*
- Bronze Medal in National Olympiad in Informatics (NOI) *July 2015*

## SELECTED PROJECT

---

### zkCNN [\[Github\]](#)

A ZKP implementation in C++.

2021

- An implementation of GKR-based zero-knowledge proof protocol for CNN model inference.
- Efficient enough to run a vgg16 instance in **less than 2mins**.

### Hyrax-bls12-381 [\[Github\]](#)

An implementation of polynomial commitment in C++.

2021

- Based on **Hyrax** scheme defined on the field of BLS12-381.
- Especially for multilinear extension form that is very common in GKR-based zero-knowledge scheme.

### MaStarCompiler [\[Github\]](#)

A compiler for a simplified C++ language in Java

2018

- Designed and implemented a compiler compiling M\* language (a C++-and-java-like language) into NASM x86 assembly language using 6000 ~ 7000 lines in Java.
- Implemented features such as using ANTLR 4 as a parser tool to build AST, an self-defined IR, and optimizations based on static single assignment form.

### TomRiVer [\[Github\]](#)

A Tomasulo-based CPU in Verilog

2018

- Implemented structures such as branch prediction, forwarding within 2 weeks.

## TEACHING EXPERIENCE

---

**Teaching Assistant** of MS208 @ SJTU: Compiler Design and Implementation

*Spring 2018 - 2019*

**Assistant Coach** of The ACM-ICPC Team @ SJTU

*2018 - 2019*