Jiahui **Lu**

☎ (+1) 404-429-2362　|　✉ lujiahui1@hotmail.com　|　🏠 alanwap.github.io　|　⬛ AlanWaP　|　in AlanWaP

Education

Georgia Institute of Technology (Georgia Tech)　　　　　　　　　　　*Atlanta, Georgia, US*
MS IN COMPUTER SCIENCE　　　　　　　　　　　　　　　　　　　　　　　　　　*Aug 2017 - Dec 2021*

- Institute for Information Security & Privacy, College of Computing
- GPA 3.84/4.0

Shanghai Jiao Tong University (SJTU)　　　　　　　　　　　　　　　*Shanghai, China*
BSE IN COMPUTER SCIENCE　　　　　　　　　　　　　　　　　　　　　　　*Sept 2013 - July 2017*

- ACM Honored Program, Zhiyuan College
- GPA 3.77/4.3

Work Experience

Inspur USA Inc.　　　　　　　　　　　　　　　　　　　　　　*San Jose, California, US*
SOFTWARE ENGINEER　　　　　　　　　　　　　　　　　　　　　　　　*Aug 2022 - Present*

- Develop tools for command line interface (CLI) of database KaiwuDB
- Develop the time series database engine of multi-model KaiwuDB to support streaming data
- Design automatic query optimization algorithms for KaiwuDB to improve time efficiency

JD.com Silicon Valley R&D Center　　　　　　　　　　　*Mountain View, California, US*
RESEARCH SCIENTIST　　　　　　　　　　　　　　　　　　　　　　　*Feb 2022 - Aug 2022*

- Apply multi-party computation (MPC) frameworks to machine learning system for security and privacy

JD.com Silicon Valley R&D Center　　　　　　　　　　　*Mountain View, California, US*
RESEARCH INTERN　　　　　　　　　　　　　　　　　　　　　　　　*May 2021 - Aug 2021*

- Implement a highly efficient protocol to generate distributed RSA key pairs for communication security

Research Experience

Institute for Information Security & Privacy, Georgia Tech　　　　*Atlanta, Georgia, US*
GRADUATE RESEARCH ASSISTANT, ADVISED BY PROF. ALEXENDRA BOLDYREVA & PROF. VLAD KOLESNIKOV　　*Aug 2017 - Dec 2021*

- Design a secure protocol for review Apps to support real-time authorized post and ensure user anonymity
- Redesign the algorithm of a MPC-in-the-head zero knowledge proof (ZKP) scheme to improve its computation speed

Security & Privacy group, Cornell Tech　　　　　　　　　　*New York City, New York, US*
RESEARCH INTERN, ADVISED BY PROF. TOM RISTENPART　　　　　　　　　　*Aug 2016 - Dec 2016*

- Develop a side-channel attack in full-text search systems
- Prove the security of symmetric encryption schemes as cryptographic commitments

Cornell University　　　　　　　　　　　　　　　　　　　　*Ithaca, New York, US*
EXCHANGE STUDENT, ADVISED BY PROF. JOHN E. HOPCROFT　　　　　　　　*Jul. 2016 - Jun. 2016*

- Analyze the functionality of neurons in different convolutional layers of a deep learning network

Publication

Efficient Generic Arithmetic for KKW - Practical Linear MPC-in-the-Head NIZK on Commodity Hardware without Trusted Setup
INTERNATIONAL SYMPOSIUM ON CYBER SECURITY CRYPTOLOGY AND MACHINE LEARNING - CSCML 2021

- Authors: David Heath, Vladimir Kolesnikov, Jiahui Lu
- Conference Talk

Message Franking via Committing Authenticated Encryption
ADVANCES IN CRYPTOLOGY - CRYPTO 2017

- Authors: Paul Grubbs, Jiahui Lu, Thomas Ristenpart

Side-Channel Attacks on Shared Search Indexes

IEEE Symposium on Security and Privacy - Oakland 2017

- Authors: Liang Wang, Paul Grubbs, Jiahui Lu, Vincent Bindschaedler, David Cash, Thomas Ristenpart

Anonymous Review Systems for (Un)linkable Settings

In progress

- Authors: Jiahui Lu, Alexandra Boldyreva

Honors & Awards

3rd round, 2021 Google Code Jam *Online*

Individual *May 2021*

4th place, 2018 ACM-ICPC Southeast USA Regional Contest *Kennesaw, Georiga, US*

Team BuShiMeiguoRen, Georgia Tech *Nov 2018*

- 1st in Kennesaw State University site

9th place, 2018 ITA Tech Challenge *Chicago, Illinois, US*

Individual *Oct 2018*

2nd place, 2018 Mercer University Spring Programming competition *Macon, Georiga, US*

Team Yellow Jackets, Georgia Tech *Feb 2018*

- 1st in Division II

Extracurricular Activities

ACM programming team, Georgia Tech *Atlanta, Georgia, US*

Coach *Aug 2019 - Dec 2021*

- Team meeting lecturer
- College team representative in contests. Participated in
    - 2020 Mercer University Spring Programming competition (1st)
    - 2020 Southeast USA Regional Contest (1st)
    - 2021 ICPC North America Division Championships (3rd)

2020 Mercer University Spring Programming competition *Macon, Georgia, US*

Staff & Problem writer *Feb 2020*

x

ACM programming team, Georgia Tech *Atlanta, Georgia, US*

Contestant *Aug 2017 - Aug 2019*