ZHONGTANG LUO

Purdue University zhtluo.com zhtluo@gmail.com

EDUCATION

Purdue University 2021 - now
Ph.D., Computer Science (GPA 3.89) *Advisor: Aniket Kate*

University of California, Berkeley 2019
Visiting Student (Keystone Enclave) *Advisor: Dawn Song*

Shanghai Jiao Tong University 2016 - 2020
B.S., Computer Science (Zhiyuan Honors Program)

RESEARCH INTEREST

In my research, I look at how to make industry and academic work on **cryptography**, **distributed systems**, **blockchains** and **applied security** match up better, especially in how they handle efficiency and security. I've looked at things like consensus and data provenance. I see that companies focus on making their prototypes fast and efficient, while academia cares more about making sure these prototypes are formalized and secure. This difference creates a gap. My main question is: Can we find a way to make prototypes that are both fast and formalized?

PUBLICATION

Attacking and Improving the Tor Directory Protocol **[IEEE SP'24]**
Zhongtang Luo, Adithya Bhat, Kartik Nayak, Aniket Kate

Last Mile of Blockchains: RPC and Node-as-a-service **[IEEE TPS'22]**
Zhongtang Luo, Rohan Murukutla, Aniket Kate

RandPiper - Reconfiguration-Friendly Random Beacons with Quadratic Communication **[CCS'21]**
Adithya Bhat, Nibesh Shrestha, **Zhongtang Luo**, Aniket Kate, Kartik Nayak

PROJECT

A Tor Consensus Monitor that Detects Equivocation
`https://gitlab.torproject.org/zhtluo/depictor`

OrgAn: Organizational Anonymity with Low Latency
`https://github.com/zhtluo/organ`

Keyedge: Edge call protocol helper for Keystone Enclave
`https://github.com/keystone-enclave/keyedge`

TEACHING

CS41100 - CP3 Competitive Programming III (Spring 2024) (Instructor) 2024, Purdue University

CS31100 - CP2 Competitive Programming II (Fall 2023) (Instructor) 2023, Purdue University

CS25100 Data Structures & Algorithms (Fall 2021) (Teaching Assistant) 2021, Purdue University

Programming Contest (Instructor) 2015 - 2019, Children's Palace in Shanghai

ENGAGEMENT

External Reviewer
- ACM CCS 2022

Competitive Programming
- Active participant in Codeforces (handle: `zhtluo`)
- Silver award in ACM ICPC World Final 2018 in team *Nightfall*, together with Wenda Qiu and Boning Li
- Gold award in ACM ICPC Asia East Continent League (EC Final) 2017 & 2018
- Gold award in China Collegiate Programming Contest Final (CCPC Final) 2017 & 2018

Capture the Flag (CTF)
- First place in Raymond James CTF 2023 USD 10000
- Third place in HackIN 2021 USD 1000

SKILL

Languages: Chinese (Native), Japanese (JLPT N1)

Programming: Python, C, C++, Rust, Java, Javascript

COURSES TAKEN

All courses are taken at graduate level.

Software Security

Network Security

Trusted & Confidential Computing

Data Communication & Computer Network

Cryptography

Advanced Cryptology

Blockchains From Theory to Practice

Computational Complexity

Theoretical Computer Science Toolkit

Algorithm Design, Analysis & Implementation

OTHER AWARD

Shanghai Jiao Tong University Undergraduate Outstanding Scholarship 2017-2019