

ZHONGTANG LUO

📍 Purdue University

🌐 zhtluo.com ✉ zhtluo@gmail.com

EDUCATIONS

Purdue University <i>Ph.D., Computer Science</i>	2021 - now <i>Advisor: Aniket Kate</i>
Purdue University <i>M.S., Computer Science (GPA: 3.9)</i>	2021 - 2024 <i>Advisor: Aniket Kate</i>
Shanghai Jiao Tong University <i>B.S., Computer Science (Zhiyuan Honors Program)</i>	2016 - 2020

EXPERIENCES

Meta Platforms, Inc. <i>Intern (Applied Privacy Team)</i>	2024
University of California, Berkeley <i>Visiting Student (Keystone Enclave)</i>	2019 <i>Advisor: Dawn Song</i>

RESEARCH INTERESTS

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?

PUBLICATIONS

Proxying is Enough: Security of Proxying in TLS Oracles and AEAD Context Unforgeability [ePrint] Zhongtang Luo, Yanxue Jia, Yaobin Shen, Aniket Kate	
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 [ACM CCS'21] Adithya Bhat, Nibesh Shrestha, Zhongtang Luo, Aniket Kate, Kartik Nayak	

PROJECTS

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

SERVICES

ACM TOIT 2023	Reviewer
ACM CCS 2022	External Reviewer

ACTIVITIES

Competitive Programming

- Active participant in Codeforces (handle: zh1luo)
- 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

SKILLS

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

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

OTHER AWARDS

Shanghai Jiao Tong University Undergraduate Outstanding Scholarship	2017-2019
--	-----------