ZHONGTANG LUO

📍 Purdue University 🔗 zhtluo.com ✉ zhtluo@gmail.com

EDUCATIONS

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

Purdue University 2021 - 2024
M.S., Computer Science (GPA: 3.9) *Advisor: Aniket Kate*

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

EXPERIENCES

Meta Platforms, Inc. 2024
Intern (Applied Privacy Team)

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

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

Acceptance rates are marked in Italic.

Cauchyproofs: Batch-Updatable Vector Commitment with Easy Aggregation and Application to Stateless Blockchains **[Preprint]**
Zhongtang Luo, Yanxue Jia, Alejandra Victoria Ospina Gracia, Aniket Kate

Sharding SMR with Optimal-size Shards for Highly Scalable Blockchains **[arXiv]**
Jianting Zhang, **Zhongtang Luo**, Raghavendra Ramesh, Aniket Kate

Proxying is Enough: Security of Proxying in TLS Oracles and AEAD Context Unforgeability **[SBC'24]**
Zhongtang Luo, Yanxue Jia, Yaobin Shen, Aniket Kate *29/208 (13.94%)*

Attacking and Improving the Tor Directory Protocol **[IEEE SP'24]**
Zhongtang Luo, Adithya Bhat, Kartik Nayak, Aniket Kate *258/1449 (17.8%)*

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 *196/879 (22.3%)*

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`

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, 2024	Reviewer
ACM CCS 2022	External Reviewer

ACTIVITIES

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

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