# Zhongtang Luo

**(How to Read: John-Town Law)**

**Curriculum Vitae**
July 23, 2025

## Contact

Lawson Computer Science Building
305 N. University Street
West Lafayette, IN 47907-2107
United States of America

**Institutional Email:** luo401@purdue.edu
**Personal Email:** zhtluo@gmail.com
**Webpage:** https://zhtluo.com/

## Education

**Purdue University** 2021–2026 (Expected)
Ph.D., Computer Science Advisor: Aniket Kate

**Purdue University** 2021–2024
M.S., Computer Science (GPA: 3.9)

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

## Research Interests

My career goal is to advance **network security** by improving the safety, security, and availability of both existing and emerging network protocols. To that end, my research draws on tools from **applied cryptography** and **distributed systems** to analyze real-world network systems and develop secure, efficient designs. I am broadly interested in (1) studying real-life systems, such as Tor, TLS oracles, and blockchains; and (2) designing cryptographic and distributed primitives, including vector commitments, random beacons, and blockchain sharding. My current projects focus on last-mile data integrity in decentralized systems, aiming to ensure that end users receive correct and authenticated data.

## Experiences

**Meta Platforms, Inc.** 2025
Intern (Secure Application Frameworks Team)
*Developed a new Android secure content provider framework, covering 80% of use cases across all apps*
*Developed an auto-migration workflow using Devmate AI that achieves full-auto migration*

**Meta Platforms, Inc.** 2024
Intern (Applied Privacy Team)
*Developed new RSA-based vector commitment schemes for WhatsApp's key transparency project*
*New scheme requires only one 128-byte aggregated proof instead of the ~100-MiB full proof, saving over 99% space*

**University of California, Berkeley** 2019
Visiting Student (Keystone Enclave) Advisor: Dawn Song
*Developed Keyedge, an automatic edge-call transpiler for Keystone Enclave*

# Awards and Honors

**Competitive Programming**
Active participant on Codeforces (handle: zhtluo), highest rating: 2507 (Grandmaster, top 500 (.3%) worldwide)
Silver award in ACM ICPC World Finals 2018, with Wenda Qiu and Boning Li (4 teams worldwide every year)
Gold award in ACM ICPC Asia East Continent League (EC Final) 2017 & 2018 (~30 teams every year)
Gold award in China Collegiate Programming Contest Final (CCPC Final) 2017 & 2018 (~30 teams every year)

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

**Shanghai Jiao Tong University Undergraduate Outstanding Scholarship** 2017–2019

# Publications

Acceptance rates are marked when available.

**[LJSK24] Proxying is Enough: Security of Proxying in TLS Oracles and AEAD Context Unforgeability** **[AFT'25][SBC'24]**
**Zhongtang Luo**, Yanxue Jia, Yaobin Shen, Aniket Kate 35/135 (25.9%) 29/208 (13.9%)
*In 7th Conference on Advances in Financial Technologies (AFT 2025), appeared at the Science of Blockchain Conference 2024*
*https://ia.cr/2024/733*
*Results mentioned and used in Reclaim Protocol*

**[LJGK25] Cauchyproofs: Batch-Updatable Vector Commitment with Easy Aggregation and Application to Stateless Blockchains** **[IEEE SP'25]**
**Zhongtang Luo**, Yanxue Jia, Alejandra Victoria Ospina Gracia, Aniket Kate 257/1740 (14.8%)
*In 2025 IEEE Symposium on Security and Privacy (SP)*
*https://doi.org/10.1109/SP61157.2025.00247*

**[ZLRK25] Optimal Sharding for Scalable Blockchains with Deconstructed SMR** **[VLDB'25]**
Jianting Zhang, **Zhongtang Luo**, Raghavendra Ramesh, Aniket Kate
*To appear in Proceedings of the VLDB Endowment 18 (2025)*
*https://doi.org/10.48550/arXiv.2406.08252*

**[LBNK24] Attacking and Improving the Tor Directory Protocol** **[IEEE SP'24][RWC'25]**
**Zhongtang Luo**, Adithya Bhat, Kartik Nayak, Aniket Kate 258/1449 (17.8%) 43/138 (31.2%)
*In 2024 IEEE Symposium on Security and Privacy (SP), appeared at Real World Crypto 2025*
*https://doi.org/10.1109/SP54263.2024.00083*
*Plugin merged in Tor codebase*

**[LMK22] Last Mile of Blockchains: RPC and Node-as-a-service** **[IEEE TPS'22]**
**Zhongtang Luo**, Rohan Murukutla, Aniket Kate
*In 2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*
*https://doi.org/10.1109/TPS-ISA56441.2022.00044*

**[BLSK21] 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%)
*In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*
*https://doi.org/10.1145/3460120.3484574*

### Preprints and Technical Reports

**[LZNK25] Five Minutes of DDoS Brings down Tor: DDoS Attacks on the Tor Directory Protocol and Mitigations [Preprint]**
**Zhongtang Luo**, Jianting Zhang, Akshat Neerati, Aniket Kate

**[LuoDic25] Evaluating Performance Consistency in Competitive Programming: Educational Implications and Contest Design Insights [arXiv]**
**Zhongtang Luo**, Ethan Dickey
*https://doi.org/10.48550/arXiv.2505.04143*

**[Luo25b] Curriculum Design of Competitive Programming: a Contest-based Approach [arXiv]**
**Zhongtang Luo**
*https://doi.org/10.48550/arXiv.2504.00533*

**[Luo25a] ICLR Points: How Many ICLR Publications Is One Paper in Each Area? [arXiv]**
**Zhongtang Luo**
*https://doi.org/10.48550/arXiv.2503.16623*
*Results available at https://cspubs.org/*

## Software and Code Projects

**CSPubs: How Many ICLR Publications Is One Paper in Each Area?** 2025
*Online visualization tool developed in support of paper [Luo25a] to measure ICLR points in different areas*
*https://cspubs.org/*

**cp-reference: Competitive Programming Reference** 2025
*Comprehensive reference for competitive programming, developed to support my competitive programming courses*
*https://github.com/zhtluo/cp-reference/*

**buvc-rs: Batch Updatable Vector Commitment in Rust** 2024
*Rust implementation of the batch updatable vector commitment scheme in our IEEE SP paper [LJGK25]*
*https://github.com/zhtluo/buvc-rs*

**DirCast: Prototype for Tor Directory Protocol** 2023
*Secure Tor directory protocol proposed in our IEEE SP paper [LBNK24]*
*https://github.com/zhtluo/DirCast*

**A Tor Consensus Monitor that Detects Equivocation** 2023
*Consensus monitor proposed in our IEEE SP paper [LBNK24] to detect equivocation, merged into Tor codebase*
*https://gitlab.torproject.org/zhtluo/depictor*

**OrgAn: Organizational Anonymity with Low Latency** 2022
*Implementation of protocol proposed in PETS'22 paper OrgAn: Organizational Anonymity with Low Latency*
*https://github.com/zhtluo/organ*

**randpiper-rs: Reconfiguration-Friendly Random Beacon in Rust** 2021
*Rust implementation of the random beacon scheme in our CCS paper [BLSK21]*
*https://github.com/zhtluo/randpiper-rs*

**libpolycrypto: Golang Library Implementing Cryptography Primitives** 2020
*Includes KZG-based accumulator, polynomial commitment, and verifiable secret sharing scheme*
*https://github.com/zhtluo/libpolycrypto*

## Talks

**ICLR Points: How Many ICLR Publications Is One Paper in Each Area?** [Luo25a]
IEEE Symposium on Security and Privacy (Short Talk) 2025

**Cauchyproofs: Batch-Updatable Vector Commitment with Easy Aggregation and Application to Stateless Blockchains** [LJGK25]
IEEE Symposium on Security and Privacy 2025

**Proxying is Enough: Security of Proxying in TLS Oracles and AEAD Context Unforgeability** [LJSK24]
Science of Blockchain Conference 2024

**Attacking and Improving the Tor Directory Protocol** [LBNK24]
Purdue CS Graduate Symposium 2025
IEEE Symposium on Security and Privacy 2024
UIUC CS 591 SP, Security and Privacy (Seminar) 2023

**Last Mile of Blockchains: RPC and Node-as-a-service** [LMK22]
Purdue CS 59100, Blockchains: Theory to Practice (Seminar) 2022

## Mentoring

*Mentored undergraduate students from various programs at Purdue.*

**Alejandra Victoria Ospina Gracia** (Universidad San Francisco de Quito, Ecuador) Aug 2024–Jan 2025
*Through GoBoiler 2024 Internship, an outreach program partnering with Latin American Universities*
*Worked on IEEE SP paper [LJGK25] that builds a batch-updatable vector commitment scheme*

**Akshat Neerati** (Purdue University) Aug 2024–Jan 2025
*Through Future Mentors Program, a Purdue mentorship program for graduate and undergraduate students*
*Worked on paper [LZNK25] that explores DDoS attacks on Tor directory protocol*

## Teaching

**CS 41100, Competitive Programming III (Purdue University) (Instructor)** Spring 2025
*In charge of course design & delivery, students advanced to ICPC North America Championship 2025*

**CS 41100, Competitive Programming III (Purdue University) (Instructor)** Spring 2024
*In charge of course design & delivery, students advanced to ICPC World Finals 2022 (held in 2024)*

**CS 31100, Competitive Programming II (Purdue University) (Instructor)** Fall 2023
*In charge of course design & delivery*

**CS 25100, Data Structures & Algorithms (Purdue University) (Teaching Assistant)** Fall 2021

**Programming Contest (2015–2019) (Instructor)** Children’s Palace in Shanghai

## Services

**IEEE SP 2024, 2025** External Reviewer
*IEEE Symposium on Security and Privacy*

**ACM CCS 2022** External Reviewer
*ACM SIGSAC Conference on Computer and Communications Security*

**Asiacrypt 2025** External Reviewer
*International Conference on the Theory and Application of Cryptology and Information Security*

**ACM TOIT 2023, 2024** Reviewer
*ACM Transactions on Internet Technology*

**CVC 2025** Program Committee
*Crypto Valley Conference*