

Ning Luo

ning.k.luo@gmail.com · <https://ning0luo.github.io/> · +1 475-223-5898

Education

- Sep. 2017 – Dec. 2022 Yale University – New Haven, CT, US
Ph.D. in Computer Science
Advisor: Prof. Ruzica Piskac
Thesis: Privacy-Preserving Formal Methods
- Sep. 2013 – Jun. 2017 Shandong University – Jinan, Shandong, CN
B.S. in Mathematics

Experience

- Jan. 2023 - Now Northwestern University, Postdoc fellow.
Host: Xiao Wang
- Summer 2022 Galois, Inc, Intern.
Mentors: James Parker
- Spring 2021 Simons Institute, UC Berkeley, Visiting graduate students.
- Summer 2020 Galois, Inc, Intern.
Mentors: Bill Harris and Alex Malozemoff

Honors and Scholarships

- Nov. 2023 Computer Science Distinguished Dissertation Award at Yale
- Nov. 2023 EECS Rising Stars
- Jan. 2023 Yale Roberts Innovation Award
- Nov. 2022 Distinguished Paper Award, ACM CCS 2022 (5 selected from 972 submissions)
- Jun. 2022 USENIX Security 2022 Student Grant
- Jan. 2022 VMCAI 2022 Student Fellowship
- Jun. 2019 CAV 2019 Student Fellowship

Grants

- NSF FMitF: Automating and Synthesizing Parallel Zero-Knowledge Protocols
CCF-2318974/
CCF-2318975 **Proposal development lead**, with Xiao Wang (Northwestern University), Ruzica Piskac (Yale University), and Timos Antonopoulos (Yale University).
\$ 750,000. Oct. 2023 - Sep. 2027

Publications

(* indicates equal contribution)

- 2023 *ZKSMT: A VM for Proving SMT Theorems in Zero Knowledge*
Daniel Luick, John Kolesar, Timos Antonopoulos, William R. Harris, James Parker, Ruzica Piskac, Eran Tromer, Xiao Wang, **Ning Luo**. *eprint*.
- 2023 *Privacy-Preserving Regular Expression Matching using Nondeterministic Finite Automata*
Ning Luo*, Chenkai Weng*, Jaspal Singh, Gefei Tan, Ruzica Piskac, Mariana Raykova. *eprint*.
- 2023 *Ou: Automating the Parallelization of Zero-Knowledge Protocol*
Yuyang Sang*, **Ning Luo***, Samuel Judson, Ben Chaimberg, Timos Antonopoulos, Xiao Wang, Zhong Shao. *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS 2023)*.
- 2022 *Proving UNSAT in Zero Knowledge*
Ning Luo, Timos Antonopoulos, William Harris, Ruzica Piskac, Eran Tromer, Xiao Wang. *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS 2022)*.
Receipt of **Distinguished Paper Award**.
- 2022 *ppSAT: Towards Two-Party Private SAT Solving*
Ning Luo, Samuel Judson, Timos Antonopoulos, and Ruzica Piskac. *Proceedings of the 31st USENIX Security Symposium (USENIX Security 2022)*.
- 2021 *Looking for the Maximum Independent Set: A New Perspective on the Stable Path Problem*
Yichao Cheng, **Ning Luo**, Jingxuan Zhang, Timos Antonopoulos, Ruzica Piskac, Qiao Xiang. *IEEE International Conference on Computer Communications 2021 (INFOCOM 2021)*.
- 2019 *Privacy Preserving CTL Model Checking through Oblivious Graph Algorithms*
Samuel Judson, **Ning Luo**, Timos Antonopoulos, Ruzica Piskac. *Workshop on Privacy in the Electronic Society 2020 (WPES 2020)*.

Service

- 2024 Program Committee: CAV, Euro S&P, CSF, PoPETs
- 2023 External Reviewer: CAV, USENIX Security, IEEE S&P
Artifact Evaluation Committee: USENIX Security
- 2022 POPL Session Chair of TutorialFest

Mentorship

- Fall 2022 Qiuyue Qin, Huisan Xu (Masters at Xiamen University)
Publication: *Toward Privacy-Preserving Interdomain Configuration Verification via Multi-Party Computation* (APNET 2023)
- 2019-2021 Yichao Cheng (Undergraduate at Yale University)
Publication: *Looking for the Maximum Independent Set: A New Perspective on the Stable Path Problem* (INFOCOM 2021)
Thesis advisor: *Methods for Privacy-Preserving Model Checking in LTL*.
- Summer 2020 Michael Chen (Undergraduate at Yale University)

Teaching Experience

- Fall 2022 Teaching Fellow, Law, Security, and Logic (Yale University)
- Spring 2022 Teaching Fellow, Software Engineering (Yale University)
- Fall 2021 Teaching Fellow, Computer System Security (Yale University)
- Spring 2021 Teaching Fellow, Software Engineering (Yale University)
- Fall 2020 Teaching Fellow, Cryptography and Computer Security (Yale University)
- Spring 2020 Teaching Fellow, Artificial Intelligence (Yale University)
- Fall 2019 Teaching Fellow, Algorithm via Continuous Optimization (Yale University)

Talks

- Oct. 2023 Incorporating Privacy-Preserving Constraints into Automated Reasoning
Northeastern Formal Methods Meetup, Yale University
- Oct. 2023 Proving SMT Theorems in Zero Knowledge
DARPA SIEVE PI Meeting
- Apr. 2023 Proving UNSAT in Zero Knowledge
Invited talk at Satisfiability: Theory, Practice, and Beyond Workshop, Simons Institute, University of California, Berkeley
- Apr. 2023 Automating the Parallelization of Zero-Knowledge Protocols
DARPA SIEVE PI Meeting
- Nov. 2022 Proving UNSAT in Zero Knowledge.
ACM SIGSAC Conference on Computer and Communications Security
- Aug. 2022 ppSAT: Towards Two-Party Privacy-Preserving SAT Solving
USENIX Security Symposium
- Jan. 2022 Privacy-Preserving Formal Methods: Proving UNSAT in Zero Knowledge.
Invited talk at New York University
- Dec. 2019 Privacy-Preserving Model Checking
Invited talk at Microsoft Research