Curriculum Vitæ

Lawrence Roy

February 4, 2026

Cryptography · Multi-Party Computation · Cybersecurity

Homepage ldr709.gitlab.io
GitHub github.com/ldr709
GitLab gitlab.com/ldr709
Email ldr709@gmail.com
Discord lance_roy
Google Scholar tinyurl.com/RoyGScholar

Research Interests

I research a range of topics related to secure multi-party computation, including oblivious transfer (OT), OT extension, garbled circuits, homomorphic secret sharing, and advanced lattice primitives. I am also interested in formal verification and proofs for cryptography and cybersecurity more generally.

Education

Sep. 2017 – Oct. 2022 **Ph.D.** in Computer Science – Cryptography — Oregon State University

Thesis: "Communication-Efficient Secure Two-Party Computation From Minicrypt and OT".
Advisor: Mike Rosulek.

Sep. 2017 – Mar. 2020 **M.S.** in Computer Science – Cryptography — Oregon State University

Admitted following high school, undergraduate degree requirement waived.
Project: "A Complete Characterization of Security for Linicrypt Block Cipher Modes".

Skills

Learning programming languages is something of a hobby for me, and so I will only list my favorites. For high-level work I like to do functional programming in Haskell or Idris. For practical work I prefer Rust, and I have contributed to the standard library. I often need to use C, C++, or Python because of the large amount of existing code. I have a working knowledge of LaTeX, as can be seen from this document, or my papers.

Publications

I started my research in computer graphics. During my internship at IBM in 2018, I gained some experience in systems security, and its intersection with cryptography. I

then switched fully to cryptography in 2019, though I maintain a side interest in systems security. These fields have different author ordering conventions.

Peer-Reviewed Publications

2019 – Present

Cryptography

Authors are ordered alphabetically.

1. Damiano Abram, Giulio Malavolta, and Lawrence Roy. "Slightly Sublinear Trapdoor Hash Functions and PIR from Low-Noise LPN". in: *TCC 2025, Part I*. ed. by Benny Applebaum and Huijia (Rachel) Lin. Vol. 16268. LNCS. Springer, Cham, Dec. 2025, pp. 280–300. DOI: 10.1007/978-3-032-12287-2_10. URL: https://eprint.iacr.org/2025/416
2. Amik Raj Behera, Pierre Meyer, Claudio Orlandi, Lawrence Roy, and Peter Scholl. "Privately Constrained PRFs from DCR: Puncturing and Bounded Waring Rank". In: *TCC 2025, Part I*. ed. by Benny Applebaum and Huijia (Rachel) Lin. Vol. 16268. LNCS. Springer, Cham, Dec. 2025, pp. 301–332. DOI: 10.1007/978-3-032-12287-2_11. URL: https://eprint.iacr.org/2025/230
3. Ran Cohen, Jack Doerner, Eysa Lee, Anna Lysyanskaya, and Lawrence Roy. "An Unstoppable Ideal Functionality for Signatures and a Modular Analysis of the Dolev-Strong Broadcast". In: *TCC 2025, Part IV*. ed. by Benny Applebaum and Huijia (Rachel) Lin. Vol. 16271. LNCS. Springer, Cham, Dec. 2025, pp. 675–708. DOI: 10.1007/978-3-032-12290-2_22. URL: https://eprint.iacr.org/2024/1807
4. Carsten Baum, Ward Beullens, Lennart Braun, Cyprien Delpech de Saint Guilhem, Michael Klooß, Christian Majenz, Shibam Mukherjee, Emmanuela Orsini, Sebastian Ramacher, Christian Rechberger, Lawrence Roy, and Peter Scholl. "Shorter, Tighter, FAESTer: Optimizations and Improved (QROM) Analysis for VOLE-in-the-Head Signatures". In: *CRYPTO 2025, Part VI*. ed. by Yael Tauman Kalai and Seny F. Kamara. Vol. 16005. LNCS. Springer, Cham, Aug. 2025, pp. 124–156. DOI: 10.1007/978-3-032-01887-8_5. URL: https://eprint.iacr.org/2026/164
5. Jake Januzelli, Mike Rosulek, and Lawrence Roy. "Lower Bounds for Garbled Circuits from Shannon-Type Information Inequalities". In: *CRYPTO 2025, Part IV*. ed. by Yael Tauman Kalai and Seny F. Kamara. Vol. 16003. LNCS. Springer, Cham, Aug. 2025, pp. 589–618. URL: https://eprint.iacr.org/2025/876
6. Damiano Abram, Giulio Malavolta, and Lawrence Roy. "Key-Homomorphic Computations for RAM: Fully Succinct Randomised Encodings and More". In: *CRYPTO 2025, Part III*. ed. by Yael Tauman Kalai and Seny F. Kamara. Vol. 16002. LNCS. Springer, Cham, Aug. 2025, pp. 236–268. DOI: 10.1007/978-3-032-01881-6_8. URL: https://eprint.iacr.org/2025/339
7. Pierre Meyer, Claudio Orlandi, Lawrence Roy, and Peter Scholl. "Silent Circuit Relinearisation: Sublinear-Size (Boolean and Arithmetic) Garbled Circuits from DCR". in: *CRYPTO 2025, Part IV*. ed. by Yael Tauman Kalai and Seny F. Kamara. Vol. 16003. LNCS. Springer, Cham, Aug. 2025, pp. 426–458. DOI: 10.1007/978-3-032-01884-7_14. URL: https://eprint.iacr.org/2025/245
8. Sebastian Kolby, Lawrence Roy, Jure Sternad, and Sophia Yakoubov. "Information-Theoretic Random-Index PIR". in: *ITC 2025*. Ed. by Niv Gilboa. Vol. 343. LIPIcs. Schloss Dagstuhl, Aug. 2025, 5:1–5:15. DOI: 10.4230/LIPIcs.ITC.2025.5. URL: https://eprint.iacr.org/2025/1574

9. Damiano Abram, Giulio Malavolta, and Lawrence Roy. "Succinct Oblivious Tensor Evaluation and Applications: Adaptively-Secure Laconic Function Evaluation and Trapdoor Hashing for All Circuits". In: *57th ACM STOC*. ed. by Michal Koucký and Nikhil Bansal. STOC '25. ACM Press, June 2025, pp. 1875–1886. ISBN: 9798400715105. DOI: 10.1145/3717823.3718164. URL: https://eprint.iacr.org/2025/336

10. Jake Januzelli, Lawrence Roy, and Jiayu Xu. "Under What Conditions Is Encrypted Key Exchange Actually Secure?" In: *EUROCRYPT 2025, Part II*. ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15602. LNCS. Springer, Cham, May 2025, pp. 451–481. DOI: 10.1007/978-3-031-91124-8_16. URL: https://eprint.iacr.org/2024/324

11. Ivan Damgård, Divya Ravi, Lawrence Roy, Daniel Tschudi, and Sophia Yakoubov. "Efficient Secure Communication over Dynamic Incomplete Networks with Minimal Connectivity". In: *TCC 2024, Part IV*. ed. by Elette Boyle and Mohammad Mahmoody. Vol. 15367. LNCS. Springer, Cham, Dec. 2024, pp. 266–292. DOI: 10.1007/978-3-031-78023-3_9. URL: https://eprint.iacr.org/2024/972

12. Pierre Meyer, Claudio Orlandi, Lawrence Roy, and Peter Scholl. "Rate-1 Arithmetic Garbling From Homomorphic Secret Sharing". In: *TCC 2024, Part IV*. ed. by Elette Boyle and Mohammad Mahmoody. Vol. 15367. LNCS. Springer, Cham, Dec. 2024, pp. 71–97. DOI: 10.1007/978-3-031-78023-3_3. URL: https://eprint.iacr.org/2024/820

13. Carsten Baum, Ward Beullens, Shibam Mukherjee, Emmanuela Orsini, Sebastian Ramacher, Christian Rechberger, Lawrence Roy, and Peter Scholl. "One Tree to Rule Them All: Optimizing GGM Trees and OWFs for Post-Quantum Signatures". In: *ASIACRYPT 2024, Part I*. ed. by Kai-Min Chung and Yu Sasaki. Vol. 15484. LNCS. Springer, Singapore, Dec. 2024, pp. 463–493. DOI: 10.1007/978-981-96-0875-1_15. URL: https://eprint.iacr.org/2024/490

14. Carsten Baum, Jens Berlips, Walther Chen, Ivan Bjerre Damgård, Kevin M. Esvelt, Leonard Foner, Dana Gretton, Martin Kysel, Ronald L. Rivest, Lawrence Roy, Francesca Sage-Ling, Adi Shamir, Vinod Vaikuntanathan, Lynn Van Hauwe, Theia Vogel, Benjamin Weinstein-Raun, Daniel Wichs, Stephen Wooster, Andrew C. Yao, and Yu Yu. "Efficient Maliciously Secure Oblivious Exponentiations". In: *CiC* 1.3 (2024), p. 10. DOI: 10.62056/a66cy7qiu

15. Maciej Obremski, João Ribeiro, Lawrence Roy, François-Xavier Standaert, and Daniele Venturi. "Improved Reductions from Noisy to Bounded and Probing Leakages via Hockey-Stick Divergences". In: *CRYPTO 2024*. Ed. by Leonid Reyzin and Douglas Stebila. Vol. 14925. LNCS. Aug. 2024, pp. 461–491. DOI: https://doi.org/10.1007/978-3-031-68391-6_14. URL: https://eprint.iacr.org/2024/1009

16. Damiano Abram, Lawrence Roy, and Peter Scholl. "Succinct Homomorphic Secret Sharing". In: *EUROCRYPT 2024, Part VI*. ed. by Marc Joye and Gregor Leander. Vol. 14656. LNCS. May 2024, pp. 301–330. DOI: 10.1007/978-3-031-58751-1_11. URL: https://eprint.iacr.org/2024/814

17. Carsten Baum, Lennart Braun, Cyprien Delpech de Saint Guilhem, Michael Klooß, Emmanuela Orsini, Lawrence Roy, and Peter Scholl. "Publicly Verifiable Zero-Knowledge and Post-Quantum Signatures from VOLE-in-the-Head".

In: *CRYPTO 2023, Part V*. ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14085. LNCS. Aug. 2023, pp. 581–615. DOI: 10.1007/978-3-031-38554-4_19. URL: https://eprint.iacr.org/2023/996

18. Yashvanth Kondi, Claudio Orlandi, and Lawrence Roy. "Two-Round Stateless Deterministic Two-Party Schnorr Signatures from Pseudorandom Correlation Functions". In: *CRYPTO 2023, Part I*. ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14081. LNCS. Aug. 2023, pp. 646–677. DOI: 10.1007/978-3-031-38557-5_21. URL: https://eprint.iacr.org/2023/216

19. Diego F. Aranha, Michele Battagliola, and Lawrence Roy. "Faster coercion-resistant e-voting by encrypted sorting". In: *Proceedings of E-Vote-ID 2023*. https://e-vote-id.org/. Tartu University Press, June 2023. URL: https://eprint.iacr.org/2023/837

20. Lawrence Roy and Jiayu Xu. "A Universally Composable PAKE with Zero Communication Cost (And Why It Shouldn't Be Considered UC-Secure)". In: *PKC 2023, Part I*. ed. by Alexandra Boldyreva and Vladimir Kolesnikov. Vol. 13940. May 2023. URL: https://eprint.iacr.org/2022/1607

21. Lawrence Roy. "SoftSpokenOT: Quieter OT Extension from Small-Field Silent VOLE in the Minicrypt Model". In: *CRYPTO 2022, Part I*. ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13507. LNCS. Aug. 2022, pp. 657–687. DOI: 10.1007/978-3-031-15802-5_23. URL: https://eprint.iacr.org/2022/192

22. Tommy Hollenberg, Mike Rosulek, and Lawrence Roy. "A Complete Characterization of Security for Linicrypt Block Cipher Modes". In: *CSF 2022 Computer Security Foundations Symposium*. IEEE Computer Society Press, Aug. 2022, pp. 439–454. DOI: 10.1109/CSF54842.2022.9919676. URL: https://eprint.iacr.org/2022/1033

23. Ian McQuoid, Mike Rosulek, and Lawrence Roy. "Batching Base Oblivious Transfers". In: *ASIACRYPT 2021, Part III*. ed. by Mehdi Tibouchi and Huaxiong Wang. Vol. 13092. LNCS. Dec. 2021, pp. 281–310. DOI: 10.1007/978-3-030-92078-4_10. URL: https://eprint.iacr.org/2021/682

Honorable Mention for Best Paper!

24. Mike Rosulek and Lawrence Roy. "Three Halves Make a Whole? Beating the Half-Gates Lower Bound for Garbled Circuits". In: *CRYPTO 2021, Part I*. ed. by Tal Malkin and Chris Peikert. Vol. 12825. LNCS. Virtual Event, Aug. 2021, pp. 94–124. DOI: 10.1007/978-3-030-84242-0_5. URL: https://eprint.iacr.org/2021/749

25. Lawrence Roy and Jaspal Singh. "Large Message Homomorphic Secret Sharing from DCR and Applications". In: *CRYPTO 2021, Part III*. ed. by Tal Malkin and Chris Peikert. Vol. 12827. LNCS. Virtual Event, Aug. 2021, pp. 687–717. DOI: 10.1007/978-3-030-84252-9_23. URL: https://eprint.iacr.org/2021/274

26. Ian McQuoid, Mike Rosulek, and Lawrence Roy. "Minimal Symmetric PAKE and 1-out-of-N OT from Programmable-Once Public Functions". In: *ACM CCS 2020*. Ed. by Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna. ACM Press, Nov. 2020, pp. 425–442. DOI: 10.1145/3372297.3417870. URL: https://eprint.iacr.org/2020/1043

2018 – Present

Systems

Authors are ordered by contribution.

27. Lawrence Roy, Stanislav Lyakhov, Yeongjin Jang, and Mike Rosulek. "Practical Privacy-Preserving Authentication for SSH". in: *USENIX Security 2022*. Ed. by

Kevin R. B. Butler and Kurt Thomas. USENIX Association, Aug. 2022, pp. 3345–3362. URL: https://eprint.iacr.org/2022/740

28. Guerney D. H. Hunt, Ramachandra Pai, Michael V. Le, Hani Jamjoom, Sukadev Bhattiprolu, Rick Boivie, Laurent Dufour, Brad Frey, Mohit Kapur, Kenneth A. Goldman, Ryan Grimm, Janani Janakirman, John M. Ludden, Paul Mackerras, Cathy May, Elaine R. Palmer, Bharata Bhasker Rao, Lawrence Roy, William A. Starke, Jeff Stuecheli, Enriquillo Valdez, and Wendel Voigt. "Confidential Computing for OpenPOWER". in: *Proceedings of the Sixteenth European Conference on Computer Systems*. New York, NY, USA: Association for Computing Machinery, 2021, pp. 294–310. ISBN: 9781450383349. URL: https://doi.org/10.1145/3447786.3456243

2016 – 2019 COMPUTER GRAPHICS Authors are ordered by contribution.

29. Yue Zhang, Lawrence Roy, Ritesh Sharma, and Eugene Zhang. "Maximum Number of Transition Points in 3D Linear Symmetric Tensor Fields". In: *Topological Methods in Data Analysis and Visualization V*. ed. by Hamish Carr, Issei Fujishiro, Filip Sadlo, and Shigeo Takahashi. Springer International Publishing, 2020, pp. 237–250. ISBN: 978-3-030-43036-8. URL: linear_3d_tensor_field_transition_point.pdf

30. Botong Qu, Lawrence Roy, Yue Zhang, and Eugene Zhang. "Mode Surfaces of Symmetric Tensor Fields: Topological Analysis and Seamless Extraction". In: *IEEE Transactions on Visualization and Computer Graphics* (2020). URL: https://arxiv.org/pdf/2009.04601

31. Fariba Khan, Lawrence Roy, Eugene Zhang, Botong Qu, Shih-Hsuan Hung, Harry Yeh, Robert S Laramee, and Yue Zhang. "Multi-Scale Topological Analysis of Asymmetric Tensor Fields on Surfaces". In: *IEEE Transactions on Visualization and Computer Graphics* 26.1 (2019), pp. 270–279. URL: https://web.engr.oregonstate.edu/~zhange/images/2Dasymmetric_multiscale.pdf

32. Lawrence Roy, Prashant Kumar, Yue Zhang, and Eugene Zhang. "Robust and Fast Extraction of 3D Symmetric Tensor Field Topology". In: *IEEE Transactions on Visualization and Computer Graphics* 25.1 (2018), pp. 1102–1111. URL: http://web.engr.oregonstate.edu/~zhange/images/3DTensorTopology_Detection.pdf

33. Jonathan Palacios, Lawrence Roy, Prashant Kumar, Chen-Yuan Hsu, Weikai Chen, Chongyang Ma, Li-Yi Wei, and Eugene Zhang. "Tensor Field Design in Volumes". In: *ACM Trans. Graph.* 36.6 (Nov. 2017). ISSN: 0730-0301. DOI: 10.1145/3130800.3130844. URL: https://web.engr.oregonstate.edu/~zhange/images/3Dtensor_design.pdf

34. Lawrence Roy, Prashant Kumar, Sanaz Golbabaei, Yue Zhang, and Eugene Zhang. "Interactive Design and Visualization of Branched Covering Spaces". In: *IEEE Transactions on Visualization and Computer Graphics* 24.1 (2017), pp. 843–852. DOI: 10.1109/TVCG.2017.2744038. URL: http://web.engr.oregonstate.edu/~zhange/images/Paper_BCSVis.pdf

35. Sanaz Golbabaei, Lawrence Roy, Prashant Kumar, and Eugene Zhang. "Construction and Visualization of Branched Covering Spaces". In: *SIGGRAPH ASIA 2016 Technical Briefs*. SA '16. Macau: Association for Computing Machinery, 2016. ISBN: 9781450345415. DOI: 10.1145/3005358.3005367

Preprint Publications

Publications not in a peer-reviewed conference or journal. These are available only through IACR ePrint or other non-peer-reviewed repositories.

2019 – Present

Cryptography

Authors are ordered alphabetically.

36. Ivan Damgård, Shravani Patil, Arpita Patra, and Lawrence Roy. *New Upper and Lower Bounds for Perfectly Secure MPC*. Cryptology ePrint Archive, Paper 2025/1206. 2025. URL: https://eprint.iacr.org/2025/1206
37. Carsten Baum, Ward Beullens, Lennart Braun, Cyprien Delpech de Saint Guilhem, Michael Klooß, Christian Majenz, Shibam Mukherjee, Emmanuela Orsini, Sebastian Ramacher, Christian Rechberger, Lawrence Roy, and Peter Scholl. *FAEST: Algorithm Specifications (Version 2.0)*. Part of NIST PQC Digital Signature Schemes, Round 2. 2025. URL: https://faest.info/faest-spec-v2.0.pdf
38. Damiano Abram, Lawrence Roy, and Mark Simkin. *Time-Based Cryptography From Weaker Assumptions: Randomness Beacons, Delay Functions and More*. Cryptology ePrint Archive, Report 2024/769. 2024. URL: https://eprint.iacr.org/2024/769

Presentations

Recorded Talks

Aug. 2025 — IACR Crypto — Santa Barbara, California
Shorter, Tighter, FAESTer: Optimizations and Improved (QROM) Analysis for VOLE-in-the-Head Signatures
Video (19 min)
Silent Circuit Relinearisation: Sublinear-Size (Boolean and Arithmetic) Garbled Circuits from DCR
Video (21 min)

Dec. 2024 — IACR TCC — Milan, Italy
Rate-1 Arithmetic Garbling from Homomorphic Secret-Sharing
Video (15 min)

Aug. 2024 — IACR Crypto — Santa Barbara, California
Improved Reductions from Noisy to Bounded and Probing Leakages via Hockey-Stick Divergences
Video (20 min)

Jun. 2024 — Theory and Practice of Multi-Party Computation Workshop — Darmstadt, Germany
Distributed Discrete Logarithms and Applications
Presented jointly with Pierre Meyer.
Pierre's Part (36 min), My Part (34 min)

May. 2024 — IACR Eurocrypt — Zurich, Switzerland
Succinct Homomorphic Secret Sharing
Video (22 min)

Apr. 2024 — NIST Fifth PQC Standardization Conference — Rockville, Maryland
One Tree to Rule Them All: Optimizing GGM Trees and OWFs for Post-Quantum Signatures
Video (20 min)

May 2023 — IACR PKC — Atlanta, Georgia
A Universally Composable PAKE with Zero Communication Cost (And Why It Shouldn't Be Considered UC-Secure)
Video (17 min)

Aug. 2022 — IACR Crypto — Santa Barbara, California
SoftSpokenOT: Quieter OT Extension From Small-Field Silent VOLE in the Minicrypt Model
Video (23 min)

Jul. 2022 — DOE CSGF Program Review — Arlington, Virginia
Communication-Efficient Secure Two-Party Computation From Minimal Assumptions
Video (16 min)

Jun. 2022 — Theory and Practice of Multi-Party Computation Workshop — Aarhus, Denmark
SoftSpokenOT: Communication–Computation Tradeoffs in OT Extension
Video (23 min)

Aug. 2021 — IACR Crypto — Virtual
Three Halves Make a Whole? Beating the Half-Gates Lower Bound for Garbled Circuits
Prerecorded Video (25 min), Live Presentation (10 min)

Nov. 2020 — ACM Conference on Computer and Communications Security — Virtual
Minimal Symmetric PAKE and 1-out-of-N OT from Programmable-Once Public Functions (10 min)

Honors and Awards

Academic

2023 — Dissertation of the Year — OSU School of EECS
2021 — Honorable Mention for Best Paper Award — IACR Crypto
2018 — Computational Science Graduate Fellowship — Department of Energy

Capture The Flag (CTF) Competitions[1]

2024 — 1st place, Team Kalmarunionen, qualified for DEF CON CTF — hxp 38C3 CTF
2023 — 5th place, Team Kalmarunionen — Black Hat MEA CTF
2022 — 16th place, Team OSUSEC — DEF CON 30 CTF
2022 — 15th place, Team OSUSEC, qualified for DEF CON CTF — DEF CON 30 CTF Quals
2020 — 6th place, Team Samurai — DEF CON 28 CTF

Service

Program Committees

Sorted by conference year, not submission year.

2026 IACR Crypto
2025 IACR Eurocrypt; ProTeCS; IACR Asiacrypt
2024 IACR Crypto
2023 Cryptology and Network Security

Ad Hoc Reviewing

2026 IACR Eurocrypt
2025 Designs, Codes, and Cryptography; IACR Crypto; Selected Areas in Cryptography
2024 IACR Public Key Cryptography; IACR Eurocrypt; Designs, Codes, and Cryptography; IACR Journal of Cryptology; Security and Cryptography for Networks; IACR Theory of Cryptography Conference; IACR Asiacrypt
2023 IACR Eurocrypt; Cryptographers' Track at RSA Conference; IACR Crypto; IACR Asiacrypt; IACR Theory of Cryptography Conference
2022 IACR Crypto; IET Information Security; IACR Asiacrypt; IACR Theory of Cryptography Conference; Transactions on Information Forensics and Security; Transactions on Emerging Topics in Computing; IACR Journal of Cryptology; Journal of Information Security and Applications
2021 IACR Crypto
2020 IACR Crypto; Conference on Security and Cryptography for Networks
2019 ACM Transactions on Graphics; IEEE Transactions on Visualization and Computer Graphics
2018 SIGGRAPH; ACM Transactions on Graphics
2017 Pacific Graphics; Graphical Models; Computer Graphics Forum

Other

Mar. 2025 Challenge Author, KalmarCTF — Virtual
Mar. 2024 Challenge Author, KalmarCTF — Virtual
Apr. 2023 Challenge Author, DamCTF — Virtual
Mar. 2023 Challenge Author, KalmarCTF — Virtual
Nov. 2021 Challenge Author, DamCTF — Virtual
Oct. 2020 Challenge Author, DamCTF — Virtual
Oct. 2017 Student Volunteer, IEEE Visualization Conference — Phoenix, Arizona

Employment

Nov. 2022 – Present **Aarhus University** — Postdoctoral Researcher

Sep. 2018 – Sep. 2022 **DOE Computational Science Graduate Fellowship** — Graduate Fellow

Jun. – Aug. 2019 **DOE CSGF Practicum** — Intern at SLAC

Worked with Elliott Slaughter to improve the Regent high-performance computing language.

Jun. – Aug. 2018 **IBM** — Intern

Worked on the Ultravisor project for secure computation on the IBM Power Architecture.

[1] A CTF is a competition to hack as many challenges as possible in a given time, while (in some events) preventing others from doing the same. DEF CON CTF is one of the oldest and most prestigious CTF events.

Sep. 2017 – Jun. 2018 Oregon State University Graduate Research Assistant

Jun. – Aug. 2017 IBM Intern

Worked with Ram Pai on data compression, memory models, and other aspects of the Linux kernel. Also continued earlier collaboration on formal verification and SRCU with Dr. Paul McKenney, IBM Distinguished Engineer.