MIKE ROSULEK

rosulekm@eecs.oregonstate.edu
https://garbledcircus.com

EMPLOYMENT

Assistant Professor June 2009 — August 2013
Department of Computer Science
University of Montana

Assistant Professor August 2013 — September 2019
Associate Professor September 2019 — September 2025
Professor September 2025 — present
School of Electrical Engineering & Computer Science
Oregon State University

EDUCATION

B.S. in Computer Science, with distinction May 2003
Iowa State University

Ph.D. in Computer Science June 2009
University of Illinois
Thesis: *The Structure of Secure Multi-Party Computation*
Advisors: Manoj Prabhakaran and Michael C. Loui

RESEARCH INTERESTS

Cryptographic foundations, privacy-enhancing technologies, secure multi-party computation protocols.

PUBLICATIONS

Note: most publications follow the convention of listing authors alphabetically.

Books, book chapters:

B1. Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. *Complexity of Multi-Party Computation Functionalities.* **Chapter** in *Secure Multiparty Computation,* eds. Manoj Prabhakaran and Amit Sahai. Cryptology and Information Security Series. IOS Press, Amsterdam. 2013.

B2. David Evans, Vladimir Kolesnikov, and Mike Rosulek. *A Pragmatic Introduction to Secure Multi-Party Computation.* **Monograph**, Now Publishers, Boston. 183 pages. 2018.

B3. Mike Rosulek, editor. *Topics in Cryptology - CT-RSA 2023 - Cryptographers' Track at the RSA Conference.* Lecture Notes in Computer Science 13871, Springer. 2023. (**Conference proceedings**)

B4. Mike Rosulek. *The Joy of Cryptography: An Undergraduate Course in Provable Security.* MIT Press, January 2026. Open-access at https://joyofcryptography.com/ starting July 2026.

Peer-reviewed conference publications (* = student advisee):

C1. Manoj Prabhakaran and Mike Rosulek. *Rerandomizable RCCA Encryption.* In *CRYPTO: Advances in Cryptology*. Springer Lecture Notes in Computer Science v4622. p517–534. 2007.

C2. Lars Olson, Mike Rosulek, and Marianne Winslett. *Harvesting Credentials in Trust Negotiation as an Honest-But-Curious Adversary* In *WPES: Workshop on Privacy in the Electronic Society.* ACM Press. p64–67. 2007.

C3. Manoj Prabhakaran and Mike Rosulek. *Homomorphic Encryption with CCA Security.* In *ICALP: International Colloquium on Automata, Languages and Programming*. Springer Lecture Notes in Computer Science v5126. p667–678. 2008.

C4. Manoj Prabhakaran and Mike Rosulek. *Cryptographic Complexity of Multi-Party Computation Problems: Classifications and Separations.* In *CRYPTO: Advances in Cryptology*. Springer Lecture Notes in Computer Science v5157. p262–279. 2008.

C5. Manoj Prabhakaran and Mike Rosulek. *Towards Robust Computation on Encrypted Data.* In *ASIACRYPT: Advances in Cryptology*. Springer Lecture Notes in Computer Science v5350. p216–233. 2008.

C6. Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. *Complexity of Multi-party Computation Problems: The Case of 2-Party Symmetric Secure Function Evaluation.* In *TCC: Theory of Cryptography Conference*. Springer Lecture Notes in Computer Science v5444. p256–273. 2009.

C7. Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. *Cryptographic Complexity Classes and Computational Intractability Assumptions.* In *ICS: Innovations in Computer Science*. Tsinghua University Press. p266–289. 2010.

C8. Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. *A Zero-One Law for Cryptographic Complexity with Respect to Computational UC Security.* In *CRYPTO: Advances in Cryptology*. Springer Lecture Notes in Computer Science v6223. p595–612. 2010.

C9. Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. *Attribute-Based Signatures.* In *CT-RSA: RSA Conference, Cryptographers' Track*. Springer Lecture Notes in Computer Science v6558. p376–392. 2011.

C10. Hemanta K. Maji, Pichayoot Ouppaphan, Manoj Prabhakaran, and Mike Rosulek. *Exploring the Limits of Common Coins Using Frontier Analysis of Protocols.* In *TCC: Theory of Cryptography Conference*. Springer Lecture Notes in Computer Science v6597. p486–503. 2011.

C11. Mike Rosulek. *Universal Composability from Essentially Any Trusted Setup.* In *CRYPTO: Advances in Cryptology*. Springer Lecture Notes in Computer Science v7417, p406–423. 2012.

C12. Mike Rosulek. *Must You Know the Code of f to Securely Compute f?* In *CRYPTO: Advances in Cryptology*. Springer Lecture Notes in Computer Science v7417, p87–104. 2012.

C13. Hemanta Maji, Manoj Prabhakaran, and Mike Rosulek. *A Unified Characterization of Completeness and Triviality for Secure Function Evaluation.* In *INDOCRYPT: International Conference on Cryptology in India.* Springer Lecture Notes in Computer Science v7668, p40–59. 2012.

C14. R. Amzi Jeffs* and Mike Rosulek. *Characterizing the Cryptographic Properties of Reactive 2-Party Functionalities.* In *TCC: Theory of Cryptography Conference.* Springer Lecture Notes in Computer Science v7785, p263–280. 2013.

C15. Dov Gordon, Tal Malkin, Mike Rosulek, and Hoeteck Wee. *Multi-Party Computation for Polynomials and Branching Programs without Simultaneous Interaction.* In *EUROCRYPT: International Cryptology Conference.* Springer Lecture Notes in Computer Science v7881, p575–591. 2013.

C16. Vladimir Kolesnikov, Payman Mohassel, Mike Rosulek. *FleXOR: Flexible Garbling of XOR Gates that Beats Free-XOR.* In *CRYPTO: Advances in Cryptology.* Springer Lecture Notes in Computer Science v8617, p440-457. 2014.

C17. Vladimir Kolesnikov, Payman Mohassel, Ben Riva, Mike Rosulek. *Richer Efficiency/Security Tradeoffs in 2PC.* In *TCC: Theory of Cryptography Conference.* Springer Lecture Notes in Computer Science v9014, p229-259. 2015.

C18. Arash Afshar, Zhangxiang Hu*, Payman Mohassel, Mike Rosulek. *How to Efficiently Evaluate RAM Programs with Malicious Security.* In *EUROCRYPT: International Cryptology Conference.* Springer Lecture Notes in Computer Science v9056, p702-729. 2015.

C19. Samee Zahur, Mike Rosulek, David Evans. *Two Halves Make a Whole: Reducing Data Transfer in Garbled Circuits using Half Gates.* In *EUROCRYPT: International Cryptology Conference.* Springer Lecture Notes in Computer Science v9057, p220-250. 2015.

C20. Zhangxiang Hu*, Payman Mohassel, Mike Rosulek. *Efficient Zero-Knowledge Proofs of Non-Algebraic Statements with Sublinear Amortized Cost.* In *CRYPTO: International Cryptology Conference.* Springer Lecture Notes in Computer Science v9216, p150-169. 2015.

C21. Brent Carmer* and Mike Rosulek. *Vamonos: Embeddable Visualizations of Advanced Algorithms.* In *IEEE Frontiers in Education.* p1465-1472. 2015.

C22. Payman Mohassel, Mike Rosulek, Ye Zhang. *Fast and Secure Three-party Computation: The Garbled Circuit Approach.* In *ACM Conference on Computer and Communications Security.* ACM Press, p591-602. 2015.

C23. Peter Rindal* and Mike Rosulek. *Faster Malicious 2-party Secure Computation with Online/Offline Dual Execution.* In *USENIX Security Symposium.* p297-314. 2016.

C24. Brent Carmer* and Mike Rosulek. *Linicrypt: A Model for Practical Cryptography.* In *CRYPTO: Advances in Cryptology.* Springer Lecture Notes in Computer Science v9816, p416-445. 2016.

C25. Marshall Ball, Tal Malkin, Mike Rosulek. *Garbling Gadgets for Boolean and Arithmetic Circuits.* In *ACM Conference on Computer and Communications Security.* ACM Press, p565-577. 2016.

C26. Vladimir Kolesnikov, Ranjit Kumaresan, Mike Rosulek, Ni Trieu*. *Efficient Batched Oblivious PRF with Applications to Private Set Intersection.* In *ACM Conference on Computer and Communications Security.* ACM Press, p818-829. 2016.

C27. Peter Rindal* and Mike Rosulek. *Improved Private Set Intersection against Malicious Adversaries.* In *EUROCRYPT: International Cryptology Conference.* Springer Lecture Notes in Computer Science v10210, p235-259. 2017.

C28. Payman Mohassel and Mike Rosulek. *Non-Interactive Secure 2PC in the Offline/Online and Batch Settings.* In *EUROCRYPT: International Cryptology Conference.* Springer Lecture Notes in Computer Science v10212, p425-455. 2017.

C29. Payman Mohassel, Mike Rosulek, Alessandra Scafuro. *Sublinear Zero-Knowledge Arguments for RAM Programs.* In *EUROCRYPT: International Cryptology Conference.* Springer Lecture Notes in Computer Science v10210, p501-531. 2017.

C30. Peter Rindal* and Mike Rosulek. *Malicious-Secure Private Set Intersection via Dual Execution.* In *ACM Conference on Computer and Communications Security.* ACM Press, p1229-1242. 2017.

C31. Vladimir Kolesnikov, Naor Matania, Benny Pinkas, Mike Rosulek, Ni Trieu*. *Practical Multi-party Private Set Intersection from Symmetric-Key Techniques.* In *ACM Conference on Computer and Communications Security.* ACM Press, 1257-1272. 2017.

C32. Vladimir Kolesnikov, Jesper Buus Nielsen, Mike Rosulek, Ni Trieu*, Roberto Trifiletti. *DUPLO: Unifying Cut-and-Choose for Garbled Circuits.* In *ACM Conference on Computer and Communications Security.* ACM Press, p3-20. 2017.

C33. Byron Marohn, Charles V Wright, Wu-chi Feng, Mike Rosulek, Rakesh Bobba. *Approximate Thumbnail Preserving Encryption.* In *Workshop on Multimedia Privacy and Security.* ACM Press, 33-43. 2017.

C34. Mike Rosulek. *Improvements for Gate-Hiding Garbled Circuits.* In *Indocrypt: International Conference on Cryptology in India.* Springer Lecture Notes in Computer Science v10698, p325-345. 2017.

C35. Vladimir Kolesnikov, Mike Rosulek, Ni Trieu*. *SWiM: Secure Wildcard Pattern Matching From OT Extension.* In *Financial Cryptography.* 2018.

C36. Daniel Demmler, Peter Rindal*, Mike Rosulek, Ni Trieu*. *PIR-PSI: Scaling Private Contact Discovery.* In *Privacy Enhancing Technologies Symposium (PETS).* 2018.

C37. Jonathan Katz, Samuel Ranellucci, Mike Rosulek, Xiao Wang. *Optimizing Authenticated Garbling for Faster Secure Two-Party Computation.* In *CRYPTO: Advances in Cryptology.* 2018.

C38. Rouzbeh Behnia, Muslum Ozgur Ozmen, Attila A Yavuz, Mike Rosulek. *TACHYON: Fast Signatures from Compact Knapsack.* In *ACM Conference on Computer and Communications Security (CCS).* 2018.

C39. Mike Rosulek & Morgan Shirley*. *On the Structure of Unconditional UC Hybrid Protocols.* In *Theory of Cryptography Conference (TCC).* 2018.

C40. Kimia Tajik, Akshith Gunasekaran, Rhea Dutta, Brandon Ellis, Rakesh B. Bobba, Mike Rosulek, Charles V. Wright, Wu-Chi Feng. *Balancing Image Privacy and Usability with Thumbnail-Preserving Encryption.* In *Network and Distributed System Security Symposium (NDSS).* 2019.

C41. Adam Groce, Peter Rindal*, Mike Rosulek. *Cheaper Private Set Intersection via Differentially Private Leakage.* In *Privacy Enhancing Technologies Symposium (PETS).* 2019.

C42. Benny Pinkas, Mike Rosulek, Ni Trieu*, Avishay Yanai. *SpOT-Light: Lightweight Private Set Intersection from Sparse OT Extension.* In *CRYPTO: Advances in Cryptology.* 2019.

C43. Ran Gilad-Bachrach, Kim Laine, Kristin Lauter, Peter Rindal, Mike Rosulek. *Secure Data Exchange: A Marketplace in the Cloud.* In *ACM Cloud Computing Security Workshop (CCSW).* 2019.

C44. Ian McQuoid*, Trevor Swope*, Mike Rosulek. *Characterizing Collision and Second-Preimage Resistance in Linicrypt.* In *TCC: Theory of Cryptography Conference.* 2019.

C45. Vladimir Kolesnikov, Mike Rosulek, Ni Trieu*, Xiao Wang. *Scalable Private Set Union from Symmetric-Key Techniques.* In *ASIACRYPT: Advances in Cryptology.* 2019.

C46. Benny Pinkas, Mike Rosulek, Ni Trieu*, Avishay Yanai. *PSI from PaXoS: Fast, Malicious Private Set Intersection.* In *EUROCRYPT: International Cryptology Conference.* 2020.

C47. Payman Mohassel, Mike Rosulek, Ni Trieu. *Practical Privacy-Preserving K-means Clustering.* In *Privacy Enhancing Technologies Symposium (PETS).* 2020.

C48. Payman Mohassel, Peter Rindal, Mike Rosulek. *Fast Database Joins and PSI for Secret Shared Data.* In *ACM Conference on Computer and Communications Security (CCS).* 2020.

C49. Ian McQuoid*, Mike Rosulek, Lawrence Roy*. *Minimal Symmetric PAKE and 1-out-of-N OT from Programmable-Once Public Functions.* In *ACM Conference on Computer and Communications Security (CCS).* 2020.

C50. Arezoo Rajabi*, Rakesh Bobba, Mike Rosulek, Charles V. Wright, Wu-Chi Feng. *On the (Im)Practicality of Adversarial Perturbation for Image Privacy.* In *Privacy Enhancing Technologies Symposium (PETS).* 2021.

C51. Gayathri Garimella*, Payman Mohassel, Mike Rosulek, Saeed Sadeghian, Jaspal Singh*. *Private Set Operations from Oblivious Switching.* In *International Conference on Practice and Theory of Public-Key Cryptography (PKC).* 2021.

C52. Gayathri Garimella*, Benny Pinkas, Mike Rosulek, Ni Trieu, Avishay Yanai. *Oblivious Key-Value Stores and Amplification for Private Set Intersection.* In *CRYPTO: Advances in Cryptology.* 2021.

★ C53. Mike Rosulek and Lawrence Roy*. *Three Halves Make a Whole? Beating the Half-Gates Lower Bound for Garbled Circuits.* In *CRYPTO: Advances in Cryptology.* 2021. **(best paper honorable mention)**

C54. Ian McQuoid*, Mike Rosulek, Lawrence Roy*. *Batching Base Oblivious Transfers.* In *ASIACRYPT: Advances in Cryptology.* 2021.

C55. Mike Rosulek, Ni Trieu. *Compact and Malicious Private Set Intersection for Small Sets.* In *ACM Conference on Computer and Communications Security (CCS).* 2021.

C56. Tommy Hollenberg*, Mike Rosulek, Lawrence Roy*. *A Complete Characterization of Security for Linicrypt Block Cipher Modes.* In *IEEE Computer Security Foundations Symposium (CSF).* 2022.

C57. Lawrence Roy*, Stanislav Lyakhov*, Yeongjin Jang, Mike Rosulek. *Practical Privacy-Preserving Authentication for SSH.* In *USENIX Security.* 2022.

C58. Tyler Beauregard*, Janabel Xia*, Mike Rosulek. *Finding One Common Item, Privately.* In *Conference on Security and Cryptography for Networks (SCN).* 2022.

C59. Gayathri Garimella*, Mike Rosulek, Jaspal Singh*. *Structure-Aware Private Set Intersection, with Applications to Fuzzy Matching.* In *CRYPTO: Advances in Cryptology.* 2022.

C60. Ian McQuoid*, Mike Rosulek, Jiayu Xu. *How to Obfuscate MPC Inputs.* In *TCC: Theory of Cryptography Conference.* 2022.

C61. Hannah Davis, Christopher Patton, Mike Rosulek, Phillipp Schoppmann. *Verifiable Distributed Aggregation Functions.* In *Privacy Enhancing Technologies Symposium (PETS).* 2023.

C62. Gayathri Garimella*, Mike Rosulek, Jaspal Singh*. *Malicious Secure, Structure-Aware Private Set Intersection.* In *CRYPTO: Advances in Cryptology.* 2023.

C63. Ian McQuoid, Mike Rosulek, Jiayu Xu. *How to Tolerate Typos in Strong Asymmetric PAKE.* In *CRYPTO: Advances in Cryptology.* 2025.

C64. Jake Januzelli*, Mike Rosulek, Lawrence Roy. *Lower Bounds for Garbled Circuits from Shannon-Type Information Inequalities.* In *CRYPTO: Advances in Cryptology.* 2025.

C65. David Richardson*, Mike Rosulek, Jiayu Xu. *Conditionally Input-Revealing 2PC and Fuzzy Password-Authenticated Key Exchange.* In *EUROCRYPT: International Cryptology Conference.* 2026.

C66. Junxin Liu*, Peihan Miao, Mike Rosulek, Xinyi Shi, Jifeng Wang. *Updatable Private Set Intersection from Symmetric-Key Techniques.* In *EUROCRYPT: International Cryptology Conference.* 2026.

Journal articles:

J1. Manoj Prabhakaran and Mike Rosulek. *Reconciling Non-Malleability with Homomorphic Encryption. Journal of Cryptology* 30(3), p601-671. 2017.

Unpublished preprints available online:

U1. Arash Afshar, Payman Mohassel, Mike Rosulek. *Efficient Maliciously Secure Two Party Computation for Mixed Programs.* ePrint Archive 2017. https://ia.cr/2017/062

U2. Marshall Ball, Brent Carmer, Tal Malkin, Mike Rosulek, Nichole Shimanski. *Garbled Neural Networks are Practical.* ePrint Archive 2019. https://ia.cr/2019/338

U3. David Richardson*, Mike Rosulek, Jiayu Xu. *Fuzzy PSI via Oblivious Protocol Routing.* ePrint Archive 2024. https://ia.cr/2024/1642

PhD dissertation:

D1. Mike Rosulek. *The Structure of Secure Multi-Party Computation.* Department of Computer Science, University of Illinois. Urbana, Illinois. 2009.

Articles written for general audiences:

GA1. Mike Rosulek. *Secure Your Data and Compute on it Too!* In *XRDS: Crossroads, The ACM Magazine for Students.* Vol. 21, No. 3, pp36-41. Spring 2015. http://xrds.acm.org/article.cfm?aid=2730910

SOFTWARE PROJECTS

SW1. Brent Carmer* and Mike Rosulek. *Vamonos: a browser-based framework for advanced algorithm visualization.* http://rosulek.github.io/vamonos

TECHNICAL PRESENTATIONS

Invited talks:

T1. *Reconciling Non-malleability with Homomorphic Encryption.*

- ▷ Bell Labs ECT seminar. Murray Hill, NJ. November 2008.
- ▷ University of Montana computer science seminar. Missoula, MT. December 2008.
- ▷ Montana State University computer science seminar. Bozeman, MT. April 4, 2011.
- ▷ University of Maryland cryptography seminar (substantially revised from above). College Park, MD. January 16, 2012.

T2. *The (nearly) All-or-Nothing Nature of Universally Composable Security.* Columbia University cryptography seminar. New York, NY. June 6, 2011.

T3. *Must You Know the Code of f to Securely Compute f?* University of Illinois CS theory seminar. Urbana, IL. April 3, 2012.

T4. *Getting More out of Secure Computation.*

- ▷ Oregon State University EECS colloquium. Corvallis, OR. November 2013.
- ▷ Intel seminar. Hillsboro, OR. February 2014.

T5. *From Circuits to RAM Programs in Malicious 2PC.*

- ▷ Microsoft Research seminar. Redmond, WA. August 2014.
- ▷ University of Maryland cybersecurity seminar. College Park, MD. September 2014.
- ▷ Columbia University cryptography seminar. New York, NY. September 2014.

T6. *A Crash Course in Garbled Circuit Optimizations.*

- ▷ Oregon State University number theory seminar. Corvallis, OR. November 2014.
- ▷ Oregon Crypto Interest Group. Portland, OR. November 2014.

T7. *A Brief History of Practical Garbled Circuit Optimizations.* Securing Computation workshop. Simons Institute, UC Berkeley. June 2015.

T8. *Towards Optimal Garbled Circuit Constructions.* Allerton Conference on Communication, Control & Computing. University of Illinois, October 2015.

T9. *Secure Computation with Sublinear Cost.* DIMACS/Columbia Data Science Institute Workshop on Cryptography for Big Data. New York, NY, December 2015.

T10. *Faster Malicious 2PC with Online/Offline Dual Execution.*

- ▷ Cryptography Seminar, Aarhus University, Denmark. March 2016.
- ▷ Microsoft Research Seminar, Redmond, WA. May 2016.

T11. *New Results for Garbled Arithmetic and High Fan-In Computations.*

- ▷ Indiana University Computer Science colloquium. Bloomington, IN. October 2016.
- ▷ Workshop on Theory and Practice of Multiparty Computation (TPMPC). Bristol, UK. March 2017.
- ▷ Reed College Math/CS seminar. Portland, OR. November 2017.

T12. *Linicrypt: A Model For Practical Cryptography.* Charles River Crypto Day. Boston, MA. December 2016.

T13. *Garbled circuits for secure computation.* Invited tutorial at Indocrypt 2017. Chennai, India. December 2017.

T14. Invited lecturer for *crypt@b-it*, a 5-day summer school on cryptography hosted at Bonn University, Germany. Contributed 15 hours of lecture and tutorial sessions on practical secure two-party computation techniques. July 2018.

T15. *A Brief Overview of Private Set Intersection.*

- ▷ Invited keynote speaker, ProvSec 2020. November 2021.
- ▷ Invited speaker, NIST Special Topics on Privacy and Public Auditability, April 2021.
- ▷ Invited speaker, Protocol Labs seminar, October 2022.

T16. *Practical Privacy-Preserving Authentication for SSH.* NIST cryptography reading group. August 2022.

T17. *Private set intersection on sets with known structure.* Bay Area Crypto Day. April 2024.

T18. *Spotlight on Private Set Intersection for Small Sets.* NIST Workshop on Privacy-Enhancing Cryptography. September 2024.

Contributed conference & workshop presentations:

P1. *Rerandomizable RCCA Encryption.* International Cryptology Conference (CRYPTO 2007). Santa Barbara, CA. August 2007.

P2. *Cryptographic Complexity of Multi-Party Computation Problems.* International Cryptology Conference (CRYPTO 2008). Santa Barbara, CA. August 2008.

P3. *Homomorphic Encryption with CCA Security.* International Colloquium on Automata, Languages and Programming (ICALP 2008). Reykjavik, Iceland. July 2008.

P4. *Reconciling Non-malleability with Homomorphic Encryption.* Crypto in the Clouds workshop. MIT. August, 2009.

P5. *Attribute-Based Signatures.* RSA Conference, Cryptographers' Track (CT-RSA 2011). San Francisco, CA. February 18, 2011.

P6. *Must You Know the Code of f to Securely Compute f?* International Cryptology Conference (CRYPTO 2012). Santa Barbara, CA. August 20, 2012.

P7. *Universal Composability from Essentially Any Trusted Setup.* International Cryptology Conference (CRYPTO 2012). Santa Barbara, CA. August 21, 2012.

P8. *FleXOR: Flexible Garbling of XOR Gates that Beats Free XOR.*

- ▷ Workshop on Applied Multi-Party Computation. Redmond, WA. February 20, 2014.
- ▷ Workshop on Theory & Practice of Multiparty Computation (TPMPC). Aarhus, Denmark. May 2014.
- ▷ International Cryptology Conference (CRYPTO 2014). Santa Barbara, CA. August 2014.

P9. *Richer Efficiency/Security Tradeoffs in 2PC.* Theory of Cryptography Conference (TCC 2015). Warsaw, Poland. March 23, 2015.

P10. *Improvements for Gate-Hiding Garbled Circuits.* International Conference on Cryptology in India (Indocrypt 2017). Chennai, India. December 11, 2017.

P11. *Garbled neural networks are practical.* Privacy preserving machine learning (PPML) workshop at ACM CCS 2019. London, UK. November 15, 2019.

P12. *PSI from PaXoS: Fast, Malicious Private Set Intersection.* International Cryptology Conference (Eurocrypt). Virtual. March 12, 2020.

P13. *Compact and Malicious Private Set Intersection for Small Sets.* In ACM Conference on Computer and Communications Security (CCS). November 15, 2021.

P14. *Structure-Aware Private Set Intersection.* In Workshop on Theory & Practice of Multiparty Computation (TPMPC). Aarhus, Denmark. June 2022.

P15. *Practical Privacy-Preserving Authentication for SSH.* In Usenix Security. Boston, MA. August 2022.

FUNDING

External research funding (my share $1.97M):

- *Getting the Most out of Secure Multi-Party Computation.* Role: **Sole PI**. National Science Foundation, Faculty Early Career Development (CAREER) Program. CCF-1149647. March 2012 – March 2017. $492,588 + $4,750 REU supplement (Summer 2013)
- *Private Set Intersection: Fast, Fuzzy, and Strongly Secure.* Role: **Sole PI**. Google Faculty Research Awards. February 2016. $47,667.
- *TWC: Small: Finding Optimality in Practical Cryptography.* Role: **Sole PI**. National Science Foundation, Secure and Trustworthy Cyberspace (SaTC) program. CCF-1617197. August 2016 – September 2019. $500,000 + $8,000 REU supplement (Summer 2017).
- Visa Research Faculty Award (unsolicited). Role: **Sole PI**. September 2017. $37,500.
- *PASCAL: Programming Architecture for Secure Cryptographic AppLications.* Role **Co-PI** (PI of OSU subcontract; lead institution IBM Research). Intelligence Advanced Research Projects Activity (IARPA). June 2019 – August 2020. OSU share $151,122.
- *Next-generation private record linkage.* Role: **Sole PI**. Facebook "Role of applied cryptography in a privacy-focused ecosystem" award. May 2020. $58,013.
- *Authenticated Video Using Self-Healing Encryption.* Role: **Co-PI** (PI Camille Palmer @OSU). Department of Energy, subcontracted through PNNL. January 2022. $356,000 (my share $178,000).
- *SaTC: CORE: Small: New Approaches for Fuzzy Private Set Intersection.* Role: **PI**. National Science Foundation, Secure and Trustworthy Cyberspace (SaTC) program. CNS-2150726. June 2022 – May 2025. $500,000.

Internal and external educational funding (my share $154k):

- *REU Site: Mathematics and Theoretical Computer Science at Oregon State University.* Role: **Co-PI** (PI Holly Swisher @OSU). National Science Foundation, Research Experiences for Undergraduates (REU) program. DMS-1757995. September 2018 – August 2021. $288,249 (my share $144,124).
- *Open Oregon State* open textbook initiative. $10,000 award to produce an open-access textbook in cryptography. (reference [B4] above)

ADVISING

Current students:

- Alice Murphy
- Junxin Liu
- David Richardson (co-advised with Jiayu Xu)
- Aditya Damodhar Dhanapal (co-advised with Jiayu Xu)

Graduate students advised:

- ▷ Perry Hooker: CS MS (University of Montana). Graduated Spring 2012. Thesis topic: *Functional Encryption as Mediated Obfuscation.*
- ▷ Zhangxiang Hu: CS MS. Graduated June 2015. Thesis topic: *Random Access Machine in Secure Multi-Party Computation.*
- ▷ Morgan Shirley: CS MS. Graduated Spring 2017. Thesis topic: *On the Structure of Unconditional UC Hybrid Protocols.*
- ▷ Peter Rindal: CS PhD. Graduated Summer 2018. Thesis topic: *Keeping your Friends Secret: Improving the Security, Efficiency and Usability of Private Set Intersection.*
- ▷ Brent Carmer: CS PhD. Graduated Summer 2018. Thesis topic: *Optimizing Cryptographic Obfuscation.*
- ▷ Tommy Hollenberg: CS MS. Graduated Spring 2019.
- ▷ Naimisha Saireddy: CS MS. Graduated Spring 2019.
- ▷ Ni Trieu: CS PhD. Graduated Winter 2020. Thesis topic: *Efficient Private Matching for Private Databases.*
- ▷ Lawrence Roy: CS PhD. Graduated Fall 2022. Thesis topic: *Communication-Efficient Secure Two-Party Computation From Minicrypt and OT.*
- ▷ Gayathri Garimella: CS PhD. Graduated Spring 2023. Thesis topic: *Communication-efficient Private Set and Database Operations.*
- ▷ Jaspal Singh: CS PhD. Graduated Summer 2023. Thesis topic: *New constructions and applications for Homomorphic Secret Sharing and Function Secret Sharing.*
- ▷ Ian McQuoid: CS PhD. Graduated Summer 2023. Thesis topic: *Characterizing Server Compromise: Resilience Models, Instantiations, and Impossibilities.*
- ▷ Jake Januzelli: CS MS (co-advised with Jiayu Xu): Graduated Spring 2025. Thesis topic: *A Complete Characterization of One-More Assumptions In the Algebraic Group Model.*
- ▷ Naman Kumar: CS MS (co-advised with Jiayu Xu): Graduated Spring 2025. Thesis topic: *New Directions in Multi-Party Computation from LPN.*

Undergraduate research (REU) advising:

- ▷ Amzi Jeffs: Summer 2013. (U Montana; resulted in publication at TCC 2013)
- ▷ Jessica Covington & Megan Golbek: Summer 2015.
- ▷ Morgan Shirley: Summer 2016. (Resulted in publication at TCC 2018)
- ▷ Josh Gerstein & Anna Raichev: Summer 2017.
- ▷ Ian McQuoid & Trevor Swope: Summer 2017 – Summer 2019. (Resulted in publication at TCC 2019)
- ▷ Justin Bloom & Lalita Devadas: Summer 2019.
- ▷ Jo O'Harrow: AY 2020–21.
- ▷ Ryan Little: AY 2020–21.
- ▷ Tyler Beauregard & Janabel Xia: Summer 2021. (Resulted in publication at SCN 2022)

TEACHING

Courses taught at Oregon State University (► = new course approval):

- ▷ CS 321: *Theory of Computation.* Fall 2016 (109 students), Fall 2017 (146 students). Fall 2021 (90 students).
- ▷ CS 420/520: *Graph Algorithms.* Winter 2025 (37 students).
- ► CS 427: *Cryptography.* Fall 2013 (22 students, as CS419/519), Winter 2015 (25 students, as CS419), Winter 2016 (12 students), Winter 2017 (46 students), Winter 2018 (46 students), Winter 2019 (57 students), Fall 2020 (hybrid section: 5 students), Winter 2020 (online section + on-campus section: 99 students total), Winter 2021 (67 students), Winter 2022 (65 students), Winter 2025 (56 students).
- ▷ CS 517: *Computational Complexity.* Spring 2015 (16 students), Spring 2016 (14 students), Spring 2017 (25 students), Spring 2018 (28 students), Spring 2019 (21 students), Spring 2020 (37 students), Spring 2021 (36 students), Spring 2022 (24 students), Spring 2024.
- ▷ CS 505: *Graduate Writing Seminar.* Spring 2022 (10 students).
- ▷ CS 5x9: *Special Topics in Cryptography.* Winter 2014 (15 students; 2 enrolled from U Oregon), Fall 2015 (9 students), Spring 2024 (5 students).
- ▷ CS/ECE 478: *Network Security.* Spring 2014 (33 students), Spring 2019 (52 students).
- ▷ CS 578: *Graduate Cybersecurity.* Winter 2024.

Courses taught at University of Montana (► = new course approval):

- ▷ CSCI 232: *Data Structures.* Fall 2012 (34 students).
- ▷ CSCI 332: *Design & Analysis of Algorithms.* Fall 2009 (13 students), Fall 2010 (14 students), Fall 2011 (17 students), Spring 2013 (34 students).
- ▷ CSCI 361: *Computer Architecture.* Spring 2013 (33 students).
- ▷ CSCI 488: *Networking.* Fall 2009 (16 students).
- ► CSCI 473/573: *Cryptography.* Fall 2009 (10 students), Spring 2011 (23 students, 11 remote), Spring 2012 (17 students, 13 remote).
  - Offered concurrently at Montana State University via live videoconference, Spring 2011 & 2012.
- ► CSCI 476/576: *Theory of Computation.* Fall 2011 (9 students).
- ▷ CSCI 531: *Advanced Algorithms.* Fall 2010 (6 students), Fall 2012 (7 students).

Other activities:

- ▷ Fellow of the University of Montana's "Pedagogy Project," Fall 2011 – Spring 2013.
  - Contributor to article: Tobin Miller Shearer. *A Pleasing Observation.* In *Chronicle of Higher Education.* March 6, 2012. http://chronicle.com/article/A-Pleasing-Observation/131074/
- ▷ Completed *College Teaching* course (EOL 585) at University of Illinois, Spring 2007.

SERVICE

Service to the department/university at Oregon State University:

- EECS faculty search committees:
  - tenure-stream cybersecurity: AY 2013-14, AY 2018-19, AY 2019-20
  - instructor: AY 2017-18, 2019-20.
  - Associate Head of Online Programs: **chair** AY 2021-22.
  - tenure-stream broad CS: AY 2020-21, **chair** AY 2023-24, **chair** AY 2024-25.
- College of Engineering NSF CAREER proposal workshop panelist. Winter & Spring 2014.
- EECS cybersecurity initiative task force. Spring 2014.
- Faculty sponsor for EECS student security club. Spring 2014 – 2018.
- EECS undergraduate CS curriculum committee. AY 2014-17; **chair** AY 2018-20.
- EECS ABET accreditation committee. AY 2019-20.

Service to the department/university at University of Montana:

- Faculty advisor for department Student Evaluation Committee (committee of students who evaluate faculty teaching for annual reviews). Fall 2010, Fall 2011, Fall 2012.
- Coordinated overhaul of CS department website, deployed January 2011.
- Director, Montana State Science Fair. 558 students (grades 6-12) attended this 2-day event. Spring 2011.
- Faculty senate representative. Spring 2011 – Spring 2013
- Coach for ACM programming competition team. Summer 2011.
- Department TA coordinator. Fall 2012 – Spring 2013.
- ACM club faculty advisor. Fall 2011 – Spring 2013.
- Math department faculty hiring committee. Spring 2013.

Service to the profession:

- Communications secretary of the International Association for Cryptologic Research (IACR): 2014 – 2019.
- Associate editor: ACM Transactions on Privacy and Security (TOPS): 2020 – 2024.
- Award selection committees:
  - RSA Award for Excellence in Mathematics: 2022 – 2025.
  - IACR Test-of-Time Award: 2025 – 2026.
- Steering committees:
  - Theory & Practice of Multiparty Computation (TPMPC) Workshop: May 2017 – present.

- Conference for Failed Approaches and Insightful Losses in Cryptology (CFAIL): 2020 – present.
- Cryptographers' Track at RSA Conference (CT-RSA): 2022 – 2025.

▷ Co-organizer, Simons Institute workshop on Secure Computation, August 2025.

▷ Program committee memberships:

PKC 2011	Crypto 2018	Crypto 2021
TCC 2012	TCC 2018	CFAIL 2021
TCC 2014	IEEE S&P 2019	PETS 2022 (**senior PC** member)
Eurocrypt 2014	CCS 2019 (**area chair**)	CT-RSA 2022
ACNS 2015	CCSW 2019	SCN 2022
PETS 2015	Indocrypt 2019	CT-RSA 2023 (**program chair**)
PETS 2016	Crypto 2020	CFAIL 2024
Crypto 2016	SCN 2020	RWC 2025
CCS 2017	Indocrypt 2020	TPMPC 2025
Indocrypt 2017	CFAIL 2020	Crypto 2025 (**area chair**)
Eurocrypt 2018	RWC 2021	Crypto 2026 (**program co-chair**)

AWARDS

▷ Outstanding Sophomore in Computer Science, Iowa State University, 2001.

▷ Top 2% of Class Award, Iowa State University, 2000 – 2003.

▷ CRA Outstanding Undergraduate Award, honorable mention, 2003.

▷ List of Teachers Ranked as Excellent by Their Students, University of Illinois. For CS 273: *Introduction to Theory of Computation.* Summer 2008. (Overall teacher effectiveness rated 4.5/5.0 by students.)

▷ Oregon State University College of Engineering Engelbrecht Young Faculty Award, Fall 2019.

▷ Best paper honorable mention (for [C53]), Crypto 2021.

▷ Oregon State University College of Engineering Graduate Mentoring Award, Fall 2022.