Christina Garman

clg@cs.purdue.edu
https://www.cs.purdue.edu/homes/clg/

Research Interests

My research seeks to develop, build and deploy privacy enhancing technologies across a variety of spaces. Fundamentally I focus on building systems that offer privacy in addition to performance, as well as understanding and developing the cryptographic tools required to construct them. My work takes a full stack approach, necessitating understanding not just the cryptography itself, but also the systems stack that utilizes it, across different abstraction layers and deployment scenarios.

Education

2011–2017 **Ph.D., Computer Science**, *Johns Hopkins University*, *Baltimore, MD*
- Thesis: *Securing Deployed Cryptography Systems*
- Advisor: Matthew D. Green

2011–2013 **MSE, Computer Science**, *Johns Hopkins University*, *Baltimore, MD*

2007–2011 **BS, Computer Science and Engineering; BA, Mathematics; Minor, Physics, *magna cum laude***, *Bucknell University*, *Lewisburg, PA*

Experience

Jan 2018–Present **Assistant Professor**, *Purdue University*, *West Lafayette, IN*

Aug 2017–Dec 2017 **Postdoctoral Researcher**, *University of Maryland*, *College Park, MD*
Postdoctoral researcher with Dave Levin

May 2015–Aug 2015 **Graduate Research Intern**, *Intel Labs*, Hillsboro, OR
Graduate research intern with Jesse Walker and Mic Bowman

May 2014–Aug 2014 **Visiting Academic**, *Royal Holloway, University of London*, Egham, UK
Visiting academic with Kenneth Paterson

2011–2017 **Research Assistant**, *Johns Hopkins University*, *Baltimore, MD*
Research Assistant with Matthew D. Green

Publications

Conference

[24] Jalen Chuang, Alex Seto, Nicolas Berrios, Stephan van Schaik, Christina Garman, Daniel Genkin. "TEE.fail: Breaking Trusted Execution Environments via DDR5 Memory Bus Interposition". To Appear in IEEE Security and Privacy (S&P) 2026. (18 pages) [Student authors contribution order, lead faculty author at the end]

[23] Alex Seto, Oytun Kuday Duran, Samy Amer, Jalen Chuang, Stephan van Schaik, Daniel Genkin, Christina Garman. "WireTap: Breaking Server SGX via DRAM Bus Interposition". In ACM Conference on Computer and Communications Security (CCS) 2025. **DISTINGUISHED PAPER AWARD** (16 pages) [Student authors contribution order, lead faculty author at the end]

[22] Nureddin Kamadan, Walter Wang, Stephan van Schaik, Christina Garman, Daniel Genkin, Yuval Yarom. "ECC.fail: Mounting Rowhammer Attacks on DDR4 Servers with ECC Memory". In USENIX Security 2025. (Acceptance rate 17.1% (407/2385), 20 pages, passed Artifacts Available evaluation)

[21] Arushi Arora, Christina Garman. "Improving the Performance and Security of Tor's Onion Services". Accepted to The Privacy Enhancing Technologies Symposium (PETS) 2025. (22 pages) [Artifact Badges Available and Functional Awarded]

[20] Yongming Fan, Priyam Biswas, Christina Garman. "R+R: A Systematic Study of Cryptographic Function Identification Approaches in Binaries". In the Annual Computer Security Applications Conference (ACSAC) 2024. (Acceptance rate 19.7% (83/421), 17 pages)

[19] Hosein Yavarzadeh, Archit Agarwal, Max Christman, Christina Garman, Daniel Genkin, Andrew Kwong, Daniel Moghimi, Mohammadkazem Taram, Deian Stefan, Dean Tullsen. "High-Resolution Control-Flow Attacks with Conditional Branch Predictor". In ASPLOS 2024. (15 pages)

[18] Stephan van Schaik, Alex Seto, Thomas Yurek, Adam Batori, Bader AlBassam, Daniel Genkin, Andrew Miller, Eyal Ronen, Yuval Yarom, Christina Garman. "SoK: SGX.Fail: How Stuff Get eXposed". In IEEE Security and Privacy (Oakland), 2024. (20 pages) [Authors contribution order, lead faculty author at the end]

[17] Yongming Fan, Yuquan Xu, Christina Garman. "SNARKProbe: An Automated Security Analysis Framework for zkSNARK Implementations". In Applied Cryptography and Network Security (ACNS), 2024. (30 pages)

[16] Michael Rosenberg, Jacob White, Christina Garman, Ian Miers. "`zk-creds`: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure". In IEEE Symposium on Security and Privacy (Oakland), 2023. (19 pages) [Authors alphabetical by student then alphabetical by professors]

[15] Arushi Arora, Raj Karra, Dave Levin, Christina Garman. "Provably Avoiding Geographic Regions for Tor's Onion Services." In Financial Cryptography and Data Security, 2023. (17 pages) [lead faculty author]

[14] Alexander Master, Christina Garman. "A Worldwide View of Nation-state Internet Censorship". In Free and Open Communications on the Internet, 2023. (21 pages)

[13] Yuyan Bao, Kirshanthan Sundararajah, Raghav Malik, Qianchuan Ye, Christopher Wagner, Fei Wang, Mohammad Hassan Ameri, Donghang Lu, Alexander Seto, Benjamin Delaware, Roopsha Samanta, Aniket Kate, Christina Garman, Jeremiah Blocki, Pierre-David Letourneau, Benoit Meister, Jonathan Springer, Tiark Rompf, Milind Kulkarni. "HACCLE: Metaprogramming for Secure Multi-Party Computation". In ACM SIGPLAN International Conference on Generative Programming: Concepts & Experiences (GPCE), 2021. (Acceptance rate 50% (16/32), 14 pages)

[12] Michael Reininger, Arushi Arora, Stephen Herwig, Nicholas Francino, Jayson Hurst, Christina Garman, Dave Levin. "Bento: Safely Bringing Network Function Virtualization to Tor". In ACM SIGCOMM, 2021. (Acceptance rate 22.8% (55/241), 15 pages, passed Artifact Evaluation) [Authors contribution-ordered for student, alphabetical for professors]

[11] Stephen Herwig, Christina Garman, Dave Levin. "Achieving Keyless CDNs with Conclaves". In USENIX Security, 2020. (Acceptance rate 16.1% (157/977), 17 pages, passed Artifact Evaluation) [Student first author then alphabetical for professors]

[10] Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Cohney, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla, Hovav Shacham. "A Systematic Analysis of the Juniper Dual EC Incident". In ACM Conference on Computer and Communications Security (CCS), 2016. **BEST PAPER AWARD** (Acceptance rate 16.5% (137/831), 14 pages)

[9] Christina Garman, Matthew Green, Gabriel Kaptchuk, Ian Miers, Michael Rushanan. "Dancing on the Lip of the Volcano: Chosen Ciphertext Attacks on Apple iMessage". In USENIX Security, 2016. (Acceptance rate 15.6% (72/463), 19 pages)

[8] Christina Garman, Matthew Green, Ian Miers. "Accountable Privacy for Decentralized Anonymous Payments". In Financial Cryptography and Data Security, 2016. (Acceptance rate 26% (36/139), 18 pages (extended version, 28 pages))

[7] Joseph A. Akinyele, Christina Garman, Susan Hohenberger. "Automating Fast and Secure Translations from Type-I to Type-III Pairing Schemes". In ACM Conference on Computer and Communications Security (CCS), 2015. (Acceptance rate 19.8% (128/646), 12 pages (extended version, 34 pages))

[6] Christina Garman, Kenneth G Paterson, Thyla van der Merwe. "Attacks Only Get Better: Password Recovery Attacks Against RC4 in TLS". In USENIX Security, 2015. (Acceptance rate 15.7% (67/426), 17 pages)

[5] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza. "Zerocash: Practical Decentralized Anonymous E-Cash from Bitcoin". In IEEE Symposium on Security and Privacy (Oakland), 2014. **IEEE S&P TEST OF TIME AWARD** (Acceptance rate 13.2% (44/334), 16 pages (extended version, 56 pages))

[4] Christina Garman, Matthew Green, Ian Miers, Aviel Rubin. "Rational Zero: Economic Security for Zerocoin with Everlasting Anonymity". In Workshop on Bitcoin Research, 2014. (15 pages)

[3] Christina Garman, Matthew Green, Ian Miers. "Decentralized Anonymous Credentials". In Network and Distributed System Security Symposium (NDSS), 2014. (Acceptance rate 18.6% (55/295), 15 pages (extended version, 21 pages))

[2] Ian Miers, Christina Garman, Matthew Green, Aviel Rubin. "Zerocoin: Anonymous Distributed E-Cash from Bitcoin". In IEEE Symposium on Security and Privacy (Oakland), 2013. (Acceptance rate 12.1% (38/315), 15 pages)

[1] Garman C*, Bindert N*, Sunkara A*, Paliulis L, Ebenstein DM. "Deformation Mapping in Micro- and Nanoscale Fibers". In: N Tamura, editor. Probing Mechanics at Nanoscale Dimensions, (Mater. Res. Soc. Symp. Proc. 1185), 2009.

Journal

[3] Arushi Arora, Christina Garman. "Analysis of software bill of materials tools". In Cyber Security: A Peer-Reviewed Journal, 2023. (22 pages)

[2] Arushi Arora, Virginia Wright, Christina Garman. "Strengthening the Security of Operational Technology: Understanding Contemporary Bill of Materials". In (JCIP) The Journal of Critical Infrastructure Policy, 2022. (25 pages)

[1] Joseph A. Akinyele, Christina Garman, Ian Miers, Matthew W. Pagano, Michael Rushanan, Matthew Green, Aviel D. Rubin. "Charm: A Framework for Rapidly Prototyping Cryptosystems". In Journal of Cryptographic Engineering, 2013. (18 pages)

Poster

[2] Arushi Arora, Sai Raj Karra, Dave Levin and Christina Garman. "Improving the Performance and Security of Tor's Onion Services". In Network and Distributed System Security Symposium (NDSS), 2022. **BEST POSTER PRESENTATION AWARD** (Acceptance rate unknown)

[1] Michael Reininger, Arushi Arora, Stephen Herwig, Nicholas Francino, Christina Garman, Dave Levin. "Bento: Bringing Network Function Virtualization to Tor". In ACM Conference on Computer and Communications Security (CCS), 2020. (Acceptance rate unknown, 3 pages)

Magazine

[1] Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Cohney, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla, Hovav Shacham. "Where did I leave my keys?: lessons from the Juniper Dual EC incident". In Communications of the ACM, 2018. (Invited, 8 pages)

Technical Report

[12] Jalen Chuang, Alex Seto, Nicolas Berrios, Stephan van Schaik, Christina Garman, Daniel Genkin. "TEE.fail: Breaking Trusted Execution Environments via DDR5 Memory Bus Interposition". `tee.fail`. (22 pages)

[11] Alex Seto, Oytun Kuday Duran, Samy Amer, Jalen Chuang, Stephan van Schaik, Daniel Genkin, Christina Garman. "WireTap: Breaking Server SGX via DRAM Bus Interposition". `wiretap.fail`. (17 pages)

[10] Stephan van Schaik, Alex Seto, Thomas Yurek, Adam Batori, Bader AlBassam, Daniel Genkin, Andrew Miller, Eyal Ronen, Yuval Yarom, Christina Garman. "SoK: SGX.Fail: How Stuff Get eXposed". `sgx.fail`. (28 pages)

[9] Michael Rosenberg, Jacob White, Christina Garman, Ian Miers. "`zk-creds`: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure". Cryptology ePrint Archive, Paper 2022/878. (43 pages) [Authors alphabetical for students and then alphabetical for professors]

[8] Alexander R. Block, Christina Garman. "Honest Majority Multi-Prover Interactive Arguments". Cryptology ePrint Archive, Paper 2022/557. (36 pages)

[7] Yuyan Bao, Kirshanthan Sundararajah, Raghav Malik, Qianchuan Ye, Christopher Wagner, Fei Wang, Mohammad Hassan Ameri, Donghang Lu, Alexander Seto, Benjamin Delaware, Roopsha Samanta, Aniket Kate, Christina Garman, Jeremiah Blocki, Pierre-David Letourneau, Benoit Meister, Jonathan Springer, Tiark Rompf, Milind Kulkarni. "HACCLE: An Ecosystem for Building Secure Multi-Party Computations". arXiv:2009.01489. (19 pages)

[6] Alexander Master, Christina Garman. "A WireGuard Exploration". CERIAS Technical Reports. (4 pages)

[5] Stephen Checkoway, Shaanan Cohney, Christina Garman, Matthew Green, Nadia Heninger, Jacob Maskiewicz, Eric Rescorla, Hovav Shacham, Ralf-Philipp Weinmann. "A Systematic Analysis of the Juniper Dual EC Incident". Cryptology ePrint Archive, Paper 2016/376. (14 pages)

[4] Christina Garman, Matthew Green, Ian Miers. "Accountable Privacy for Decentralized Anonymous Payments". Cryptology ePrint Archive, Paper 2016/061. (28 pages)

[3] Joseph A. Akinyele, Christina Garman, Susan Hohenberger. "Automating Fast and Secure Translations from Type-I to Type-III Pairing Schemes". Cryptology ePrint Archive, Paper 2015/290. (34 pages)

[2] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza. "Zerocash: Practical Decentralized Anonymous E-Cash from Bitcoin". Cryptology ePrint Archive, Paper 2014/349. (56 pages)

[1] Christina Garman, Matthew Green, Ian Miers. "Decentralized Anonymous Credentials". Cryptology ePrint Archive, Paper 2013/622. (21 pages)

Thesis

2017 Christina Garman, "Securing Deployed Cryptographic Systems", Ph.D. Thesis

Teaching

Fall, 2025 **CS 526: Information Security**, *Purdue University*, Enrollment: TBA

Fall, 2024 **CS 526: Information Security**, *Purdue University*, Enrollment: 53

Spring, 2024 **CS 426: Computer Security**, *Purdue University*, Enrollment: 83

Spring, 2024 **CS 490: MITRE Embedded CTF**, *Purdue University*, Enrollment: 12

Fall, 2023 **CS 526: Information Security**, *Purdue University*, Enrollment: 82

Fall, 2023 **CS 526: Information Security (Online)**, *Purdue University*, Enrollment: 5

Fall, 2022 **CS 526: Information Security**, *Purdue University*, Enrollment: 102

Spring, 2022 **CS 426: Computer Security**, *Purdue University*, Enrollment: 68

Fall, 2021 **CS 526: Information Security**, *Purdue University*, Enrollment: 59

Spring, 2021 **CS 590: Practical and Applied Cryptography**, *Purdue University*, Enrollment: 9

Fall, 2020 **CS 526: Information Security**, *Purdue University*, Enrollment: 44

Spring, 2020 **CS 526: Information Security – Online Course Development**, *Purdue University*, Enrollment: N/A
Developed a high quality online course at the department's request for the ISCP program.

Fall, 2019 **CS 526: Information Security**, *Purdue University*, Enrollment: 40

Fall, 2019 **CS 591: CERIAS Security Seminar**, *Purdue University*, Enrollment: 22

Fall, 2018 **CS 590: Practical and Applied Cryptography**, *Purdue University*, Enrollment: 8

Fall, 2018 **CS 526: Information Security**, *Purdue University*, Enrollment: 43 (On Campus), 4 (Online)

Spring, 2018 **CS 526: Information Security**, *Purdue University*, Enrollment: 24

Professional Service

Conference Leadership/Organization

2025-2026 **Associate Chair**, *IEEE Security and Privacy 2026*
One of sixteen associate chairs invited to help the two chairs with the logistics and running of all parts of the organization and review process for IEEE Security and Privacy 2026.

2025 **Mentoring Co-Chair**, *USENIX Security*

2024-2025 **Associate Chair**, *IEEE Security and Privacy 2025*
One of ten associate chairs invited to help the two chairs with the logistics and running of all parts of the organization and review process for IEEE Security and Privacy 2025.

2024-2025 **Program Chair**, *Financial Cryptography and Data Security 2025*

2024 **Chair of the Midwest Security Workshop**
Held at Purdue University in Fall 2024

2024 **Mentoring Co-Chair**, *USENIX Security*
Helped to co-organize a mentoring event for students/junior folks in computer security and privacy at USENIX Security.

2023-2024 **Co-Organizer**, *NSF SaTC Aspiring PI Workshop 2024*
The purpose of this workshop is to provide individuals who have never received a SaTC award with tips and tools for navigating the NSF's proposal review process, with a focus on SaTC's goals. The workshop also focuses on broadening participation in SaTC and mentoring PIs that might otherwise not have access to such resources. Had 83 attendees.

2023-2024 **General Chair**, *Financial Cryptography and Data Security 2024*

Fall 2023 **Co-organizer of the (Mini) Midwest Security Workshop**

2022-2023 **Vice Chair**, *USENIX Security*
One of five vice chairs invited to help the two chairs with the logistics and running of all parts of the organization and review process for USENIX Security 2023.

Fall, 2022–Fall, 2023 **Organizing Committee, GREPSEC VI (Underrepresented Groups in Security Research)**
Helped to organize a workshop for early-stage graduate students in computer security and privacy, focusing on underrepresented populations. Held in cooperation with USENIX and supported by NSF and other external sponsors. Had 44 student attendees.

August, 2021 **Virtual Environment Chair**, *USENIX Security*
Designed, built, and managed a Gather space to facilitate social interactions, meet-ups, and general collaborative activities during USENIX Security.

Fall, 2020–Fall, 2021 **Organizing Committee, GREPSEC V (Underrepresented Groups in Security Research)**
Helped to organize a workshop for early-stage graduate students in computer security and privacy, focusing on underrepresented populations. Held in cooperation with USENIX and supported by NSF and other external sponsors. Had 43 student attendees.

Fall, 2019–Spr 2020 **Chair of the Midwest Security Workshop**, *Was to be hosted at Purdue in Fall 2020 (postponed due to Covid19)*

Summer, 2019 **Lightning Talks Chair**, *USENIX Security*

Spring, 2019 **Co-organizer of the Midwest Security Workshop**

Spring, 2018 **Co-organizer of the Midwest Security Workshop**
Day long workshop to bring together researchers in computer security and privacy from across the Midwest with over 200 registered attendees.

Program Committees

2026 ACM Conference on Computer and Communications Security (CCS) Program Committee Member

2026 International Conference on Financial Cryptography and Data Security Program Committee Member

2026 Real World Cryptography (RWC) Program Committee Member

2025 USENIX Security Program Committee Member

2025 Privacy Enhancing Technologies (PETS) Program Committee Member

2025 Real World Cryptography (RWC) Program Committee Member

2024 IEEE Security and Privacy Program Committee Member

2024 Privacy Enhancing Technologies (PETS) Program Committee Member

2024 Real World Cryptography (RWC) Program Committee Member

2023 International Conference on Financial Cryptography and Data Security Program Committee Member

2023 NDSS Program Committee Member

2023 Privacy Enhancing Technologies (PETS) Senior Program Committee Member

2023 The Science of Blockchain Conference (SBC) Program Committee Member

2022 International Conference on Financial Cryptography and Data Security Program Committee Member

2022 Privacy Enhancing Technologies (PETS) Program Committee Member

2022 USENIX Security Program Committee Member

2021 USENIX Workshop on Offensive Technologies (WOOT) Program Committee Member

2021 USENIX Security Program Committee Member

2021 International Conference on Financial Cryptography and Data Security Program Committee Member

2020 NDSS Program Committee Member

2020 International Conference on Financial Cryptography and Data Security Program Committee Member

2020 IEEE Security and Privacy Program Committee Member

2019 Eurocrypt Program Committee Member

2019 International Conference on Financial Cryptography and Data Security Program Committee Member

2019 NDSS Program Committee Member

2019 IEEE Security & Privacy on the Blockchain (IEEE S&B)

2019 ACM Advances in Financial Technologies (AFT)

2018 ACM Conference on Computer and Communications Security (CCS) Program Committee Member

2018 CRYPTO Program Committee Member

2018 Workshop on Bitcoin Research (International Conference on Financial Cryptography and Data Security) Program Committee Member

2018 International Conference on Financial Cryptography and Data Security Program Committee Member

2018 Proceedings on Privacy Enhancing Technologies (PoPETs 2018.2) Reviewer

2017 Workshop on Bitcoin Research (International Conference on Financial Cryptography and Data Security) Program Committee Member

2017 Proceedings on Privacy Enhancing Technologies (PoPETs 2017.4) Reviewer

2016 World Wide Web Conference (WWW) Security and Privacy Track Program Committee Member

2016 Workshop on Bitcoin Research (International Conference on Financial Cryptography and Data Security) Program Committee Member

2016 IEEE Security and Privacy Student Program Committee Member

2015 USENIX Workshop on Offensive Technologies (WOOT) Program Committee Member

2015 Workshop on Bitcoin Research (International Conference on Financial Cryptography and Data Security) Program Committee Member

2012–2016 Subreviews for PKC 2012, USENIX 2012, FC 2014, USENIX 2014, CCS 2014, FC 2015, USENIX 2015, USENIX 2016, CRYPTO 2016

Editorial Boards/Journals

2025 Member of the Editorial Board of the Proceedings on Privacy Enhancing Technologies (PoPETs)

2024 ACM Transactions on Privacy and Security (TOPS) Reviewer

2024 Member of the Editorial Board of the Proceedings on Privacy Enhancing Technologies (PoPETs)

2023 Science Reviewer

2023 IEEE Transactions on Mobile Computing (TMC) Reviewer

2023 Member of the Editorial Board of the Proceedings on Privacy Enhancing Technologies (PoPETs)

2022 Member of the Editorial Board of the Proceedings on Privacy Enhancing Technologies (PoPETs)

2021 IEEE Transactions on Software Engineering (TSE) Reviewer

NSF Panels

2024 NSF SaTC Panelist

2022 NSF SaTC Panelist

DOE Reviews

2025 DOE External Reviewer

Steering Committee Member

2025–present International Financial Cryptography Association (IFCA)

2018–present Midwest Security Workshop

External Engagement

Summer 2024 **USENIX Mentoring Event at USENIX Security 2024**, *Co-organizer*
Helped to co-organize a mentoring event for students/junior folks in computer security and privacy. Held in cooperation with USENIX.

Fall 2022–Present **Bucknell University Engineering Alumni Association Board of Directors Member**
The BEAA's mission is to promote the general well-being of Bucknell University's College of Engineering by developing among alumni an active and enduring interest and involvement in the affairs of the University. Tasks of a board member include mentoring of undergraduate students, engagement in curriculum development, and work with college administration.

Summer 2022 **USENIX/GREPSEC Mentoring Event at USENIX Security 2022**, *Co-organizer*
Helped to co-organize a mentoring event for students/junior folks in computer security and privacy, focusing on members of underrepresented populations. Held in cooperation with USENIX and GREPSEC.

2020 **Individualized Cybersecurity Research Mentoring (iMentor) Workshop**, *Selection committee and student mentor*
iMentor focuses on attracting, mentoring, and career advising early-stage graduate students from underrepresented communities who want to pursue a career in computer security. Mentors were assigned a student to meet with, advise, and guide through their first attendance at ACM CCS.

2019 **Bucknell University Department of Computer Science ABET Advisory Board**
Review the program curriculum and advise the program on the establishment, review, and revision of its program educational objectives as well as provide advisement on current and future aspects of the technical fields for which the graduates are being prepared.

Fall 2017 **John Deere SecureCAN Project**
Helped develop technologies for John Deere that improve the security of the CAN protocol by specifying mechanisms to provide an enhanced level of confidence that its network communications (packets) are tamper-evident and authentic.

Sum 2012–Sum 2015 **Bucknell University Engineering Alumni Association Board of Directors Member**
The BEAA's mission is to promote the general well-being of Bucknell University's College of Engineering by developing among alumni an active and enduring interest and involvement in the affairs of the University. Tasks of a board member include mentoring of undergraduate students, engagement in curriculum development, and work with college administration.

Industry Engagement/Talks

Sep 2025 Talk given to Crane through CERIAS

Nov 2023 Talk given to MITRE through CERIAS

March 2023 Talk given to Los Alamos National Labs through CERIAS

Oct 2022 Talk given to ManTech through CERIAS

Jun 2022 Talk given to Google through CERIAS

Oct 2019 Talk given to visitors from University of Tsukuba through CS

March 2019 Talk on "Securing Deployed Cryptographic Systems" given at the Citi Global Information Security Conference

University Service

Department

Fall, 2024–present **Cybersecurity (ISCY) Program**, *Purdue University*

Spr, 2024 **Purdue Online Professor of Practice Search Committee**, *Purdue University*

Fall, 2023–Spr, 2024 **Colloquium Committee**, *Purdue University*

Fall, 2022–Spr, 2024 **Cybersecurity (ISCY) Program**, *Purdue University*

Spring 2023 **Cybersecurity (ISCY) Admissions**, *Purdue University*

Fall, 2021 **Honors Research Advisor (CS397)**, *Purdue University*

Fall, 2019–Spr, 2021 **Graduate Admissions Committee**, *Purdue University*

Fall, 2019 **Founding Member of the Purdue University Center for Programming Principles and Software Systems (PURPL Center)**, *Purdue University*

Fall, 2018–Spr, 2019 **(Security) Hiring Committee**, *Purdue University*

Spring, 2018 **Graduate Admissions Committee**, *Purdue University*

University

Spring, 2022 **Astronaut Scholarship Selection Committee**, *Purdue University*
Reviewed University-wide applications for the national undergraduate Astronaut Scholarship and selected the top candidates from Purdue

Fall, 2020 **Barry M. Goldwater Scholarship Selection Committee**, *Purdue University*

Fall, 2019 **Barry M. Goldwater Scholarship Selection Committee**, *Purdue University*
Reviewed University-wide applications for the national undergraduate Goldwater scholarship and selected the top candidates from Purdue to send to the national competition

Other

Fall 2023–Present **Organizer of the Crypto Reading Group**, *Purdue University*
Attendance of roughly 25 students and professors each week

Jan 2019–Present **b01lers Faculty Advisor/co-Advisor**, *Purdue University*

Fall, 2018–Present **Computer Science Women's Network (CSWN) Faculty Advisor**, *Purdue University*

Undergraduate Engagement

Spring, 2025 **Seminar Talk, CS 197 Freshman Honors Seminar**, *Purdue University*

Spring, 2024 **Seminar Talk, CS 197 Freshman Honors Seminar**, *Purdue University*

Jan 2024 **BoilerMake XI Judge**, *Purdue University*
Faculty judge for Purdue's largest (completely undergraduate run) hackathon with over 500 students and 80+ projects.

Spring, 2023 **Seminar Talk, CS 197 Freshman Honors Seminar**, *Purdue University*

Fall, 2022 **Seminar Talk, CS 397 Honors Seminar**, *Purdue University*

Fall, 2021 **Seminar Talk, CS 397 Honors Seminar**, *Purdue University*

Fall, 2020 **Seminar Talk, CS 397 Honors Seminar**, *Purdue University*

Fall, 2018 **Seminar Talk, CS 197 Freshman Honors Seminar**, *Purdue University*

2015-2016 **She++ Student Collaborator**
Selected by She++, a nonprofit organization working to empower underrepresented groups in technology, to work to increase and celebrate diversity in technical fields by organizing at least three events in the community that promote diversity in computer science.

Other Student Engagement

Fall, 2024 **Panelist/Speaker, Research Job Search Seminar**, *Purdue University*
Panelist/speaker for the first CS department Research Job Search Seminar.

Spring, 2024 **Panelist, CSWN Event**, *Purdue University*
Panelist at the CSWN (Computer Science Womens Network) event "Women In Tech Panel Day".

Fall, 2022 **Facilitator and discussion leader, WISP Event**, *Purdue University*
Facilitator and discussion leader at the WISP (Women in Science Programs) event "Getting the most out of Conferences: Travel Funds, Preparation, and Networking".

Invited Talks

March 2024 **Invited Talk: "`zk-creds`: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure"**, *Real World Cryptography (RWC)*

July 2024 **`zk-creds`: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure**, *Bertinoro Seminar: Cryptography in the Blockchain Era*

July 2024 **Invited to Bertinoro Seminar: Cryptography in the Blockchain Era**, *Bertinoro (Forlì-Cesena), Italy*

May 2023 **Invited to Bertinoro Seminar: Cryptography in the Blockchain Era – Cancelled due to flooding**, *Bertinoro (Forlì-Cesena), Italy*

March 2023 **Invited Talk: "SGX.Fail: How Secrets Get eXtracted"**, *Real World Cryptography (RWC)*

March 2023 **Invited Panelist: Bucknell Engineering Women in Tech/Entrepreneurship**, *Bucknell University*

Nov 2021 **Invited Talk: "Bento: Safely Bringing Network Function Virtualization to Tor"**, *Penn State*

June 2021 **Invited Keynote: "Privacy, Identity, and Access Control"**, *ACM Symposium on Access Control Models and Technologies (SACMAT)*

Dec 2020 **Invited to Dagstuhl Seminar: 20491 Security of Decentralized Financial Technologies – Cancelled due to Covid19**, *Schloss Dagstuhl*

Oct 2020 **Invited Panelist: Security and Privacy Issues for Next-G Networks' Infrastructure**, *NSF NextG Security Workshop*

Aug 2020 **Cryptographic Automation**, *PurPL Retreat, Purdue University*

March 2019 **Securing Deployed Cryptographic Systems**, *Citi Global Information Security Conference*

Nov 2018 **Attendee at Dagstuhl Seminar: 18461 Blockchain Security at Scale**, *Schloss Dagstuhl*

Oct 2018 **Securing Deployed Cryptographic Systems**, *Bucknell University*

March 2018 **Guest Lecture, Privacy Enhancing Technologies Graduate Course**, *University of Illinois, Urbana-Champaign*

Aug 2018 **An Analysis of Apple iMessage**, *Workshop on Attacks in Cryptography, CRYPTO 2018*

Feb 2017 **Securing Deployed Cryptographic Systems**, *University of Iowa Computing Conference*

Nov 2016 **Zerocash and Other Techniques**, *Workshop on privacy, data sharing, and distributed ledgers, Intel Labs*

Jul 2016 **Cryptography: How to Keep a Secret**, *Engineering Innovation Program, Johns Hopkins University*

Jun 2014 **Zerocoin and Zerocash: Anonymous Distributed E-Cash and Decentralized Anonymous Payments from Bitcoin**, *ISG Research Seminar, Royal Holloway, University of London*

Aug 2010 **Gaussian Process Regression Forecasting of Computer Network Conditions**, *Bucknell University Physics REU*

Poster Sessions

2024 **`zk-creds`: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure**, *CERIAS Security Symposium*

2023 **Investigating Nation-state Internet Censorship Methods**, *CERIAS Security Symposium*

2020 **Bento: Bringing Network Function Virtualization to Tor**, *CERIAS Security Symposium*

2015 **Password Recovery Attacks Against RC4 in TLS**, *Real World Cryptography Poster Session*

2010 **Gaussian Process Regression Forecasting of Computer Network Conditions**, *Bucknell Engineering Alumni Society (BEAA) Poster Session, Bucknell University*

Gaussian Process Regression Forecasting of Computer Network Conditions, *Sigma Xi Poster Session, Bucknell University*

2009 **A Strain Gauge Force Sensor-Based Method for Material Characterization of Natural Microscale Fibers**, *National Biomedical Engineering Society (BMES) Meeting*

Strain Mapping in Microscale Natural Fibers, *Bucknell Engineering Alumni Society (BEAA) Poster Session, Bucknell University*

2008 **Strain Mapping in Microscale Natural Fibers**, *Kalman Symposium, Bucknell University*

Strain Mapping in Microscale Natural Fibers, *Materials Research Society Symposium*

Software

2025–Present **ECC.fail**, `https://doi.org/10.5281/zenodo.15579424`
End-to-end code for performing Rowhammer attacks on DDR4 with ECC enabled, ECC matrices and data scrambling strings for Intel's Skylake and Cascade Lake platforms, and code for profiling DIMMs.

2024–Present **CryptoBinary**, `https://github.com/BARC-Purdue/CryptoBinary`
A comprehensive testing and evaluation framework for comparing existing and future work in the field of cryptographic algorithm detection and identification in binary applications, as well as the results of an extensive replication and reproduction study.

2023–Present `SNARKProbe`, `https://github.com/BARC-Purdue/SNARKProbe`
An automated security analysis framework for zkSNARKs that can scan R1CS-based libraries and applications to detect various issues, such as edge case crashing, cryptographic operation errors, and/or inconsistencies with protocol descriptions.

2022–Present `zk-creds`, `https://github.com/rozbb/zkcreds-rs`
A cryptographic library for designing anonymous credential systems in a flexible, issuer-agnostic, and efficient manner using general-purpose zero-knowledge proofs.

2020–Present **Bento**, `http://bento.cs.umd.edu/`
An architecture for adding programmable "middleboxes" to the Tor anonymity network.

2017–2020 **Phoenix**, `https://github.com/smherwig/phoenix`
An extension of the Graphene libOS for Intel SGX hardware enclaves which introduces a new architectural primitive called conclaves: containers of enclaves as well as a "keyless CDN".

2014–2015 **AutoGroup+**, `https://github.com/JHUISI/auto-tools`
A cryptographic tool for securely and automatically converting Type-I to Type-III pairing schemes.

2014–2017 **Zerocash**, `http://zerocash-project.org`
A privacy-preserving decentralized anonymous payment system.

2012–2014 **Zerocoin**, `http://zerocoin.org`
A cryptographic extension to Bitcoin that augments the protocol to allow for fully anonymous currency transactions.

2011–2018 **Charm**, `http://charm-crypto.com`
A cryptographic library written in Python to facilitate intuitive, modular, and reusable development and analysis of cryptographic schemes and protocols.

Grants

2024–2025 **Purdue University Ross-Lynn Research Scholar Grant, "Exploring Extensions of a New Paradigm in Anonymous Credentials"**, *Total: $41,700*

2024–2025 **NSF, "Collaborative Research: Conference: 2024 Aspiring PIs in Secure and Trustworthy Cyberspace"**, *Share: $25,773, Total: $173,792*

2022–2023 **INL (Idaho National Lab), "Privacy-Preserving Digital Bill of Materials"**, *Total: $82,214*

2021–2026 **NSF, "CAREER: Removing the Human Element: Securing Deployed Cryptographic Systems through the use of Cryptographic Automation"**, *Total: $499,342*

2020–2022 **NSF REU Supplement, "SaTC: CORE: Small: Collaborative: Building Sophisticated Services with Programmable Anonymity Networks"**, *Total: $16,000*

2019–2020 **IARPA, "HACCLE: High Assurance Compositional Cryptography: Languages and Environments"**, *Share: $103,645, Total: $1,439,393.94, (entire program cancelled by IARPA after one year)*, co-PI with Jeremiah Blocki, Benjamin Delaware, Aniket Kate, Milind Kulkarni, Hemanta Maji, Tiark Rompf, and Roopsha Samanta

2018–2022 **NSF, "SaTC: CORE: Small: Collaborative: Building Sophisticated Services with Programmable Anonymity Networks"**, *Share: $249,988, Total: $499,988*, With David Levin at the University of Maryland

Gifts

Nov 2024 **Zama**
Zama is an open source cryptography company building state-of-the-art FHE solutions for blockchain and AI. `https://www.zama.ai/`

Students

Ph.D. Students

Spring 2022–Present **Jacob White**

Fall 2020–Present **Yongming Fan**

Fall 2018–Present	**Alex Seto**
Spring 2019	Eman Abdel-Muhdi Abu Ishgair (ECE) Switched to a different area of research.

Ph.D. Graduates

Spring 2020–Spring 2024	**Arushi Arora**, *Successfully passed Prelim in Spring 2023, defended in Spring 2024. Now at Oracle.* Thesis focused on building programmable anonymity networks and using these for security and privacy improvements for Tor. Also lead projects on privacy preserving bill of materials.
Fall 2019–Fall 2020	Priyam Biswas (co-advised with Mathias Payer), *Successfully defended and graduated in Fall 2020*

Masters Students

Fall 2024–present	Saurav Chittal
Fall 2022–Spr 2023	Walt Weiffenbach
Sum 2021–Spr 2022	Jacob White
Spring 2020	Arushi Arora
Spr 2019–Spr 2020	Patrick Cunningham

Undergraduate Students

Spring 2025	Mikk Sanborn
Sum 2024	Xinyi Guan
Spring 2024	Kevin Jones
Spring 2024	Alexandre C. Moraes
Spring 2024	Trey Rosenfeldt
Spring 2024	Chase Thompson
Spring 2024	Ga Hyun (Emily) Song
Sum 2022–Spr 2023	Yuquan Xu – now a Masters student at Georgia Tech
Spr 2022–Spr 2023	Arnav Gupta
Fall 2021–Spr 2023	Jinen Setpal
Spring 2022	Connor Cai
Spring 2022	Benton Rupp
Spring 2022	Drew Hatfield
Spring 2022	SangWon Kim
Fall 2021–Spr 2022	Nikolas Damalas (Supported on startup)
Fall 2021–Spr 2022	Walt Weiffenbach – became a Masters student at Purdue University
Fall 2021–Spr 2022	Vidur Gupta
Sum 2020–Spr 2022	Raj Karra
Sum 2020–Fall 2021	Varun Shah (Supported on startup: Summer 2020–Fall 2021)
Sum 2021	Kanti Bharat (NSF REU support)
Sum 2020–Spr 2021	Devansh Panirwala (Supported on NSF grant: Summer 2020)

Sum 2020 Sonia Rista (NSF REU support)

Sum 2020 Sehajbir Randhawa (Supported on NSF grant)

Sum 2020 Nikhilendra Rathore (Supported on NSF grant)

Sum 2020 Zheying Lu (Supported on startup) – became a Masters student at Columbia University

Sum 2020 Shravan Suravarjjala

Thesis Committees

2025 Abdullah Imran (successfully defended Spring 2025)

2025 Zeyu Lei (successfully defended Spring 2025)

2024 Muhammad Ibrahim (successfully defended Fall 2024)

2024 Boakye Dankwa (successfully defended Summer 2024)

2024 Peiyuan Liu (successfully defended Spring 2024)

2023 Alexander Master (successfully defended Summer 2023)

2022 Alexander Block (successfully defended Summer 2022)

2022 Easwar Vivek Mangipudi (successfully defended Summer 2022)

2022 Derrick McKee (successfully defended Spring 2022)

2020 Priyam Biswas (successfully defended Fall 2020)

Prelim Committees

2025 Zhongtang Luo

2024 Zeyu Lei

2024 Abdullah Imran

2023 Muhammad Ibrahim

2023 Boakye Dankwa

2022 Alexander Master

2022 Qianchuan Ye

2021 Alexander Block

2021 Easwar Vivek Mangipudi

2019 Priyam Biswas

2018 Kyriakos Ispoglou

Graduate Advisory Committees

Milad Esrafilian Najafabadi

Wuwei Zhang

External Thesis Committees

Fall 2019–Sum 2021 Stephen Herwig, University of Maryland (successfully defended in July 2021) – Now an Assistant Professor at The College of William and Mary

Independent Research Projects

Spring 2025 Mikk Sanborn, CS 497 ("Post-Quantum Anonymous Credentials and zk-creds")

Summer 2024	Xinyi Guan, CS 490 ("Tor Security Research")
Fall 2022	Arnav Gupta, CS 490 ("Tor Security Research")
Fall 2022	Mason Lovett, CS 699
Summer 2022	Ryan Hennessee, CS 590 ("Web App Security Principles")
Summer 2022	Ryan Hennessee, CS 590 ("CTF Applied Security")
Spring 2022	Walt Weiffenbach, CS 497 ("Anonymous Credentials for Tor Middleboxes")
Spring 2022	Arnav Gupta, CS 490 ("Tor Security Research")
Fall 2021	Jacob White, CS 590 ("Decentralized Anonymous Creds")
Fall 2021	Raj Karra, CS 490 ("Decentralized App Encryption")
Fall 2021	Vidur Gupta, CS 490 ("Decentralized App Encryption")
Fall 2021	Walt Weiffenbach, CS 490 ("Programmable Tor Middleboxes")
Summer 2021	Raj Karra, CS 490 ("Improving Onion Services")
Fall 2020	Yongming Fan, CS 699
Fall 2020	Devansh Panirwala, CS 490 ("Detecting Crypto In Binaries")
Spr 2019–Fall 2020	Boakye Dankwa, CS 699
Fall 2019	Shivam Bajpayi, CS 490 ("Zero Knowledge Proofs")

Awards and Honors

2025	ACM CCS Distinguished Paper Award
2025	IEEE Security and Privacy Distinguished Associate Chair Award
2025	USENIX Security Notable Reviewer Award
2024	IEEE Security and Privacy Test of Time Award
2024	PETS Outstanding Reviewer Recognition
2022	NDSS Best Poster Presentation Award
2019	Purdue University Seeds for Success Award
2018	Recipient of Google EMEA Women in Tech Travel and Conference Grant Award
2017	Internet Society and the Internet Research Task Force Applied Networking Research Prize
2017	Recipient of ACM CyberW Travel Grant
2016	ACM CCS Best Paper Award