# Christina Garman

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

## Research Interests

My research interests focus on practical and applied cryptography, namely the design and analysis of real world cryptographic systems. I aim to make it easier to design and securely deploy new and complex cryptographic systems while preventing insecurities from occurring in such systems. While this currently involves a large amount of manual work, my goal is to instrument many of these processes through the use of cryptographic automation, including automating the discovery of cryptographic vulnerabilities and building tools to aid in the deployment of complex cryptography.

## 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.*

## Research 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

[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)

[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. (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

[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

[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

[1] 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)

### Thesis

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

## Teaching

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

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

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

Fall 2020–Present **Organizing Committee, GREPSEC (Underrepresented Groups in Security Research)**, *A workshop for women and members of underrepresented groups interested in computer security research. Held in cooperation with USENIX and is supported by NSF.*

Fall, 2019–Spr 2020 **Chair of the Midwest Security Workshop**, *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

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

### External Engagement

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.

## University Service

### Department

Fall, 2019–Present **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

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

Jan 2019–Present **b01lers Faculty Advisor**, *Purdue University*.

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

### Undergraduate Engagement

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.

## Invited Talks

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

Oct 2020 **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

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

2017–2019 **University of Maryland**, College Park, MD.
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" (`https://github.com/smherwig/phoenix`)

2014–2015 **Johns Hopkins University**, Baltimore, MD.
AutoGroup+: a cryptographic tool for securely and automatically converting Type-I to Type-III pairing schemes (`https://github.com/JHUISI/auto-tools`)

2014–2017 **Johns Hopkins University**, Baltimore, MD.
Zerocash: a privacy-preserving decentralized anonymous payment system (`http://zerocash-project.org`)

2012–2014 **Johns Hopkins University**, Baltimore, MD.
Zerocoin: a cryptographic extension to Bitcoin that augments the protocol to allow for fully anonymous currency transactions (`http://zerocoin.org`)

2011–2018 **Johns Hopkins University**, Baltimore, MD.
Charm: a cryptographic library written in Python to facilitate intuitive, modular, and reusable development and analysis of cryptographic schemes and protocols (`http://charm-crypto.com`)

## Grants

2020–2021 **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*, co-PI with Jeremiah Blocki, Benjamin Delaware, Aniket Kate, Milind Kulkarni, Hemanta Maji, Tiark Rompf, and Roopsha Samanta.

2018–2021 **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.

## Students

### Ph.D. Students

| | |
|---|---|
| Fall 2020–Present | Yongming Fan. |
| Spring 2020–Present | Arushi Arora. |
| 2018–Present | Alex Seto. |
| Fall 2019–Fall 2020 | Priyam Biswas (co-advised with Mathias Payer), *Successfully defended and graduated in Fall 2020.* |
| Spring 2019 | Eman Abdel-Muhdi Abu Ishgair (ECE). |

### Masters Students

| | |
|---|---|
| Spring 2020 | Arushi Arora |
| Spr 2019–Spr 2020 | Patrick Cunningham |

### Undergraduate Students

| | |
|---|---|
| Sum 2020–Present | Devansh Panirwala |
| Sum 2020–Present | Varun Shah |
| Sum 2020 | Zheying Lu |
| Sum 2020 | Shravan Suravarjjala |
| Sum 2020 | Sehajbir Randhawa |
| Sum 2020 | Nikhilendra Rathore |
| Sum 2020 | Sonia Rista (NSF REU) |

### Prelim Committees

| | |
|---|---|
| 2019 | Priyam Biswas |
| 2018 | Kyriakos Ispoglou |

### Graduate Advisory Committees

Boakye Dankwa

Peiyuan Liu

Alexander Block

Wuwei Zhang

Easwar Vivek Mangipudi

### External Thesis Committees

| | |
|---|---|
| Fall 2019–Present | Stephen Herwig, University of Maryland |

### Independent Research Projects

| | |
|---|---|
| Fall 2020 | Yongming Fan, CS 699 |
| Fall 2020 | Devansh Panirwala, CS 490 |
| Spr 2019–Fall 2020 | Boakye Dankwa, CS 699 |
| Fall 2019 | Shivam Bajpayi, CS 490 |

## Awards and Honors

| | |
|---|---|
| 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