160 Malone Hall
3400 North Charles Street
Baltimore, MD 21218
☎ 585.301.6949
✉ cgarman@cs.jhu.edu
https://cs.jhu.edu/~cgarman

Christina Garman

Education

2011–2017 **Ph.D., Computer Science**, *Johns Hopkins University*, *Baltimore, MD.*
- Research interests in practical and applied cryptography and privacy
- Advised by Dr. 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.*

Publications

2016 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**

2016 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.

2016 Christina Garman, Matthew Green, Ian Miers. "Accountable Privacy for Decentralized Anonymous Payments". In Financial Cryptography and Data Security, 2016.

2015 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.

2015 Christina Garman, Kenneth G Paterson, Thyla van der Merwe. "Attacks Only Get Better: Password Recovery Attacks Against RC4 in TLS". In USENIX Security, 2015.

2014 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.

2014 Christina Garman, Matthew Green, Ian Miers, Aviel Rubin. "Rational Zero: Economic Security for Zerocoin with Everlasting Anonymity". In Workshop on Bitcoin Research, 2014.

2014 Christina Garman, Matthew Green, Ian Miers. "Decentralized Anonymous Credentials". In Network and Distributed System Security Symposium (NDSS), 2014.

2013 Ian Miers, Christina Garman, Matthew Green, Aviel Rubin. "Zerocoin: Anonymous Distributed E-Cash from Bitcoin". In IEEE Symposium on Security and Privacy (Oakland), 2013.

2013 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.

2009 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.

Experience

Work

2018 **Assistant Professor, Purdue University**, West Lafayette, IN.

Fall, 2017 **Postdoctoral Researcher, University of Maryland**, College Park, MD.
- Working with Dr. David Levin

Summer, 2015 **Graduate Research Intern, Intel Labs**, Hillsboro, OR.
- Cryptography intern working on algorithms and protocols for cryptocurrency designs and implementing proof-of-concepts
- Worked with Dr. Jesse Walker and Dr. Mic Bowman

Summer, 2014 **Visiting Academic, Royal Holloway, University of London**, Egham, UK.
- Password recovery attacks against RC4 in TLS
- Worked with Dr. Kenneth Paterson

Teaching

Fall, 2015 **Security and Privacy in Computing, Student Instructor**, *Johns Hopkins University*.
Lectured, helped develop syllabus, created course assignments and exams, and provided help for students

Fall, 2012 **Practical Cryptographic Systems TA**, *Johns Hopkins University*.
Created course projects on the security of practical cryptographic systems, graded projects, and provided help for students

Fall, 2011 **Security and Privacy TA**, *Johns Hopkins University*.
Graded projects and exams and provided help for students

2010–2011 **Calculus Help Sessions TA**, *Bucknell University*.
Assisted in running help sessions and worked with students on calculus questions and homework

2010-2011 **Biomimetic Materials TA**, *Bucknell University*.
Graded homework assignments and helped develop demonstrations

Fall, 2009 **Exploring Engineering, Computer Science seminar, TA**, *Bucknell University*.
Graded labs and homework assignments, assisted the professor in classes and labs

Service (Community)

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 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 Program Committee Member**.

2016 **IEEE Security and Privacy Student Program Committee Member**.

2015-2016 **She++ Student Collaborator**.

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

2015 **Workshop on Bitcoin Research Program Committee Member**.

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

Service (University)

Spring, 2013–Spring, 2017 **Graduate Representative Organization, Social Chair**, *Johns Hopkins University*.
Organization to promote graduate student interests and improve graduate student welfare and life on campus. Elected officer of the Executive Board. Co-manage a budget of approximately $45,000 to organize social events for graduate students throughout the year.

Fall, 2012–Spring, 2017 **Computer Science Department, Happy Hour Czar**, *Johns Hopkins University*.
Co-organize and run a weekly/bi-weekly social hour for computer science graduate students

Research

2016 **Johns Hopkins University**, Baltimore, MD.
- Analyzed the security of Apple's iMessage secure messaging protocol and discovered and implemented new attacks on it

2015 **Royal Holloway, University of London**, Egham, UK.
- New attacks against RC4 in TLS focused on recovering user passwords (`http://www.isg.rhul.ac.uk/tls/RC4mustdie.html`)

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–present **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–Present **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`)

Fall, 2010 **Bucknell University Presidential Fellowship**, Lewisburg, PA.
- Work on correlation identification in three-qubit quantum registers
- Advised by Dr. Michael Frey

Summer, 2010 **Department of Energy Research Assistantship**, Lewisburg, PA.
- Research into forecasting of computer network conditions using Gaussian Process Regression
- Advised by Dr. Michael Frey

2009–2010 **Bucknell University Presidential Fellowship**, Lewisburg, PA.
- Investigated numbers through the use of computational analysis
- Research into idempotents in $M_2(\mathbb{R})$, characterizations of them, mappings into $\mathbb{R}^3$, and polynomial connections between them
- Advised by Dr. Julien Giol

2007–2010 **Bucknell University Presidential Fellowship**, Lewisburg, PA.
- Biomimetics research
- Development of a research protocol for the study of the composition and deformation of various silks
- Advised by Dr. Donna Ebenstein

Invited Talks

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

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

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

August, 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.*

Professional Societies

2016–Present International Financial Cryptography Association (IFCA)

2015–Present USENIX

2012–Present International Association for Cryptologic Research (IACR)

2013–2014 Institute of Electrical and Electronics Engineers (IEEE)

2007–2011 Society of Women Engineers (SWE)

2009–2011 Association for Computing Machinery (ACM)

Awards and Honors

2016 ACM CCS Best Paper Award

2016 Recipient of CRYPTO Student Stipend

2016 Recipient of Financial Cryptography Student Stipend

2015 Recipient of CRYPTO Student Stipend

2015 Recipient of USENIX Security Symposium Grant for Women

2015 Inducted into Upsilon Pi Epsilon Computer Science Honor Society

2015 Recipient of Real World Cryptography Student Stipend

2014 Recipient of Financial Cryptography Student Stipend

2012 Recipient of CRYPTO Student Stipend

2007–2011 Dean's List

Recipient of Society of Women Engineers Dorothy M. and Earl S. Hoffman scholarship

Recipient of Bucknell University Presidential Fellowship

2011 Recipient of Bucknell University Computer Science Departmental Achievement Award

Inducted into Pi Mu Epsilon Mathematics Honor Society

2010 Inducted into Sigma Pi Sigma Physics Honor Society

2009 3rd place in the local ACM Programming contest (22nd overall in the Mid-Atlantic Region)
Inducted into Tau Beta Pi Engineering Honor Society

2008 Inducted into Alpha Lambda Delta Honor Society
Presidential Award for Distinguished Academic Achievement
Patriot League Scholar Athlete