

Gabriel Kaptchuk ✉ gabriel@kaptchuk.com

🌐 www.kaptchuk.com

📍 (Contact Me For Address)

📞 (Contact Me For Phone Number)

EDUCATION

2015 – 2020 **Ph.D. in Computer Science**
The Johns Hopkins University, Whiting School of Engineering

- Co-advised by Professor Avi Rubin and Professor Matthew Green
- Specializing in applied cryptography

2015 – 2018 **Master of Science in Computer Science**
The Johns Hopkins University, Whiting School of Engineering

2011 – 2015 **Bachelor of Science**
The Johns Hopkins University, Whiting School of Engineering

- Double Major in Computer Science (Honors) and Electrical Engineering
- Minor in Mathematics

ACADEMIC APPOINTMENT

Fall 2020 – Present **Research Assistant Professor**
Department of Computer Science, Boston University, Boston MA
Affiliations with Hariri Institute and Center for Data Science

Fall 2019 – Spring 2020 **Visiting Scholar**
Hariri Institute, Boston University, Boston MA

INDUSTRY EXPERIENCE

Fall 2019 – Present **Cryptographic Engineer**
Bolt Labs Inc, Baltimore MD

- Deploying the first payment channel protocol for anonymous payment networks
- Helped design and develop initial prototype

Summer 2018 **Cryptography Fellow**
Senator Ron Wyden's Personal Office, United States Senate, Washington DC

- Funded as a summer fellow by Tech Congress
- Assisted in identifying and addressing policy issues related to information security
- Met with leaders from industry, military, NIST, and NSA
- Developed and refined legislation related to information security

Summer 2017 **Research Intern**
Intel Labs, Portland OR

- Designed new applications for Intel Software Guard Extension (SGX)
- Helped clarify vision for Intel SGX, including future updates and features

2015 – 2018 **Research Scientist**
Harbor Labs, Baltimore MD

- Advised legal team and edited expert witness testimony for patent litigation
- Performed security reviews and penetration test of widely deployed medical devices
- Analyzed cryptographic protocols being deployed in novel security applications

Summer 2013, 2014 **DevOps Intern**
Onshape, Boston MA

- Interned with team developing leading, cloud-based, computer aided 3D design product
- Assisted in development of cloud architecture and automated testing framework
- Modeled release-time computational requirements for product
- Implemented matchmaking algorithms for routing internal traffic

2013 – 2014 **Technical Lead**

Procia, Baltimore MD

- Led technical team for student-founded company developing automated cancer diagnostic system
- Developed computer vision and machine learning algorithms for system back-end

Johns Hopkins Undergraduate Admissions

- Spring 2015 • Senior Undergraduate Admissions Intern
Fall 2012 – Spring 2015 • Tour Guide

PUBLICATIONS

Submitted 2020 **Towards Global Scale MPC with Applications to Privacy Preserving Machine Learning**
Gabrielle Beck, Aarushi Goel, Abhishek Jain, and Gabriel Kaptchuk

Submitted 2020 **Abuse Resistant Law Enforcement Access**
Matthew Green, Gabriel Kaptchuk, and Gijis Van Laer

Submitted 2020 **Meteor: Cryptographically Secure Steganography for Realistic Distributions**
Tushar Jois, Gabriel Kaptchuk, Matthew Green, and Aviel Rubin

Submitted 2020 **Improving Signal's Sealed Sender**
Gabriel Kaptchuk, Ian Martiny, Adam Aviv, Daniel Rosche, and Eric Wustrow

Submitted 2020 **How good is good enough for COVID19 apps? The influence of benefits, accuracy, and privacy on willingness to adopt**
Gabriel Kaptchuk, Daniel G. Goldstein, Eszter Hargittai, Jake Hofman, and Elissa M. Redmiles

Submitted 2020 **Fluid MPC: Secure Multiparty Computation with Dynamic Participants.**
Arka Rai Choudhuri, Aarushi Goel, Matthew Green, Abhishek Jain, and Gabriel Kaptchuk

NDSS 2019 **Giving State to the Stateless: Augmenting Trustworthy Computation with Ledgers**
Gabriel Kaptchuk, Ian Miers, and Matthew Green

ACM CCS 2017 **Fairness in an Unfair World: Fair Multiparty Computation from Public Bulletin Boards**
Arka Rai Choudhuri, Matthew Green, Abhishek Jain, Gabriel Kaptchuk, and Ian Miers

Financial Cryptography 2017 **Outsourcing Medical Dataset Analysis: A Possible Solution**
Gabriel Kaptchuk, Matthew Green, and Aviel D. Rubin

USENIX Security 2016 **Dancing on the Lip of the Volcano: Chosen Ciphertext Attacks on Apple iMessage**
Christina Garman, Matthew Green, Gabriel Kaptchuk, Ian Miers, and Michael Rushanan

Annual Security Conference 2016 **A Practical Implementation of a Multi-Device Split Application for Protecting Online Poker**
Gabriel Kaptchuk and Aviel D. Rubin.

PRESENTATIONS

December 2019 **The Hill We Must Die On: Cryptographers and Congress**
Invited talk at Boston University Cyber Alliance

NDSS 2019 **Giving State to the Stateless: Augmenting Trustworthy Computation with Ledgers**

Real World Cryptography 2019 **The Hill We Must Die On: Cryptographers and Congress**
Joint presentation with Shaanan Cohney

- Fall 2017* **Blockchain Technology Beyond Cryptocurrencies**
- Invited talk at US Naval Academy
 - Guest Lecture at Hagerstown Community College (Hagerstown, MD) covering new research on blockchains for non-cryptocurrency applications

ACM CCS 2017 **Fairness in an Unfair World: Fair Multiparty Computation from Public Bulletin Boards**

Financial Cryptography 2017 **Outsourcing Medical Dataset Analysis: A Possible Solution**

Annual Security Conference 2016 **A Practical Implementation of a Multi-Device Split Application for Protecting Online Poker**

TEACHING

Spring 2020 **Computer Networks**

- Teaching one section with 60 seats. Second section taught by Prof Avi Rubin. Divided by topics and each lectured to both sections during our topics.
- Semester transitioned to online learning due to COVID-19
- Course reviews available for [Section 1](#) and [Section 2](#).

Summer 2019 **Data Structures**

- 19 students attending a four week term covering full Data Structures curriculum (normally a 13 week term).
- Course had 13 hours of lecture per week. Workload included 8 programming assignments, 2 midterm exams, and a final exam.
- Course reviews available [here](#).
- Course received a 4.33/5.00 in "Course Quality" category
 - School Average: 4.06/5.00. Department Average: 3.75/5.00.
- Course received a 4.47/5.00 in "Instructor Teaching Effectiveness" category
 - School Average: 4.13/5.00. Department Average: 3.97/5.00.

Fall 2018 **HEART - Introduction to Computer Security and Applied Cryptography**

Fall 2019

- 1 credit pass/fail course targeted at freshman engineering students
- Goal of the course was to expose students to high-level research ideas in field
- 10 week course. Fall 2018 two sections (total of 23 students) and Fall 2019 one section (9 students)
- Course reviews available for [F18 Section 1](#), [F18 Section 2](#), and [F19 Section 1](#).
- F18 Course received 4.69/5.00 rating in "Course Quality" category
 - School Average: 4.06/5.00. Department Average: 3.75/5.00.
- F18 Course received 4.96/5.00 rating in "Instructor Teaching Effectiveness" category
 - School Average: 4.13/5.00. Department Average: 3.97/5.00.

Spring 2016, Spring 2017 **Guest Lecturer for Computer Network Fundamentals**

- Lecture entitled "Networking Tools Practicum" covered the tools required to explore and diagnose problems with computer networks

Spring 2015 **Head Teaching Assistant for Practical Cryptographic Systems**

- Received a rating of 3.8/5 from student course reviews

Fall 2014 **Course Assistant for Introduction to Algorithms**

Spring 2014 **Course Assistant for Automata and Computation Theory**

PROFESSIONAL SERVICE

Fall 2018 **Member of External Department Head Search Committee**

- Interviewed candidates and advocated for PhD student perspectives

Fall 2018 – Present **Member of Computer Science Graduate Student Council**
Fall 2018, Fall 2019

- Developed, organized, and facilitated incoming PhD student orientation
- Contained multiple sessions, including Baltimore life, academic advice, and advisor-advisee relationships

Fall 2016 – Present **Member of Computer Science Curriculum Committee**

- First and only student representative on curriculum committee

Program Committee Member

Financial Cryptography 2021

External Reviewer

Eurocrypt 2020, ACM HEALTH, ACMCCS 2019, USENIX 2019, Financial Cryptography 2019, FOCI 2018, USENIX 2016, Financial Cryptography 2015

AWARDS AND FUNDING

Fall 2020 – Fall 2022 **CRA and CCC Computing Innovation Fellow**

Summer 2018 **Tech Congress Summer Fellow**

2018 **NDSEG Finalist**