Gabriel Kaptchuk

gabriel@kaptchuk.com
9 Hall st, Somerville MA, 02144
www.kaptchuk.com
+1-617-480-4717

ACADEMIC APPOINTMENTS

Fall 2020 – Present

Research Assistant Professor

Department of Computer Science , Boston University, Boston MA
- Civic Tech Fellow at BU Faculty of Computing & Data Science
- Research Scientist at Hariri Institute for Computing
- Supported by CRA as Computing Innovation Fellow

Fall 2019 – Spring 2020

Visiting Scholar

Hariri Institute for Computing, Boston University, Boston MA

EDUCATION

2015 — 2020

Ph.D. in Computer Science

The Johns Hopkins University, Whiting School of Engineering
- Advisors: Professor Matthew Green and Professor Avi Rubin
- Dissertation: "New Applications of Public Ledgers"

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 (with honors) and Electrical Engineering
- Minor in Mathematics

PUBLICATIONS

(Authors listed alphabetically by default. Publications ordered by contribution marked with *)

EUROCRYPT 2023

Speed-Stacking: Fast Sublinear Zero-Knowledge Proofs for Disjunctions

Aarushi Goel, Mathias Hall-Anderson, Gabriel Kaptchuk, and Nicholas Spooner

PoPETS 2023

Efficient Proofs of Software Exploitability for Real-world Processors

Matthew Green, Mathias Hall-Andersen, Eric Hennenfent, Gabriel Kaptchuk, Benjamin Perez, and Gijs Van Laer

EUROCRYPT 2022

Stacking Sigmas: A General Framework to Compose Σ-Protocols for Disjunctions

Aarushi Goel, Matthew Green, Mathias Hall-Anderson, and Gabriel Kaptchuk

PoPETS 2022

Efficient Set Membership using MPC-in-the-Head

Aarushi Goel, Matthew Green, Mathias Hall-Anderson, and Gabriel Kaptchuk

ACM DTRAP Special Edition on COVID-19

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

CRYPTO 2021

Fluid MPC: Secure Multiparty Computation with Dynamic Participants

Arka Rai Choudhuri, Aarushi Goel, Matthew Green, Abhishek Jain, and Gabriel Kaptchuk

ACM CCS 2021

"I need a better description": An Investigation Into User Expectations For Differential Privacy

Rachel Cummings, Gabriel Kaptchuk, and Elissa M. Redmiles
(Best Paper Runner-up)

ACM CCS 2021 Meteor: Cryptographically Secure Steganography for Realistic Distributions*
Gabriel Kaptchuk, Tushar Jois, Matthew Green, and Aviel D. Rubin

EUROCRYPT 2021 Order-C Secure Multiparty Computation for Highly Repetitive Circuits
Gabrielle Beck, Aarushi Goel, Abhishek Jain, and Gabriel Kaptchuk

EUROCRYPT 2021 Abuse Resistant Law Enforcement Access
Matthew Green, Gabriel Kaptchuk, and Gijs Van Laer

NDSS 2021 Improving Signal's Sealed Sender*
Ian Martiny, Gabriel Kaptchuk, Adam Aviv, Daniel Rosche, and Eric Wustrow

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.

CURRENT SUBMISSIONS

Submitted 2022 What are the Chances? Explaining the Epsilon Parameter in Differential Privacy*
Priyanka Nanayakkara, Mary Anne Smart, Rachel Cummings, Gabriel Kaptchuk, and Elissa M. Redmiles

Submitted 2022 Safe Digital Intimacy: A Research Agenda
Vaughn Hamilton, Gabriel Kaptchuk, Allison McDonald, and Elissa M. Redmiles

Submitted 2022 SocIoTy: Building At-Home Cryptography from IoT Devices*
Tushar M. Jois, Gabrielle Beck, Sofia Belikovetsky, Joseph Carrigan, Alishah Chator, Gabriel Kaptchuk, Logan Kostick, Maximilian Zinkus, and Aviel Rubin

Submitted 2022 Scalable Multiparty Garbling
Gabrielle Beck, Aarushi Goel, Aditya Hegde, Abhishek Jain, Zhengzhong Jin, and Gabriel Kaptchuk

Submitted 2022 Expanded journal version of "I need a better description": An Investigation Into User Expectations For Differential Privacy
Rachel Cummings, Gabriel Kaptchuk, and Elissa M. Redmiles

Submitted 2020 zkChannels: Fast, Unlinkable Payments for Any Blockchain using 2PC
J. Ayo Akinyele, Matthew Green, Marcella Hastings, Gabriel Kaptchuk, Ian Miers, Darius E. Parvin, Colleen M. Swanson, and Gijs Van Laer

CONFERENCE PRESENTATIONS

Future of Computer Research 2022 Early Career Researchers Roundtable

Trust and Truth Online 2022 Designing for Trust in Digital Intimacy

PoPETs 2022 Efficient Set Membership using MPC-in-the-Head

Real World Cryptography 2022 Commit Acts of Steganography—Before it's too late

TCC 2021 Special In-Person Workshop Abuse Resistant Law Enforcement Access Systems

Eurocrypt 2021 Order-C Secure Multiparty Computation For Highly Repetitive Circuits

Eurocrypt 2021 Abuse Resistant Law Enforcement Access Systems

ACM CCS 2021 Meteor: Cryptographically Secure Steganography for Realistic Distributions

ACM CCS 2021 "I need a better description": An Investigation Into User Expectations For Differential Privacy

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

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

INVITED PRESENTATIONS

Fall 2022 Disjunctive Zero-knowledge
Boston Computation Club

Fall 2022 Speed Stacking: Fast Sublinear Zero-Knowledge Proofs for Disjunctions
DARPA SIEVE PI Meeting

Spring 2022 Weaving Social Accountability into Cryptographic Systems
Charles River Area Crypto Day

Fall 2021 Stacking Sigmas: Framework to Compose Σ-Protocols for Disjunctions
DARPA SIEVE PI Meeting

Fall 2021 Abuse Resistant Law Enforcement Access Systems
- Invited talk at Max Plank Institute for Software Systems
- Invited talk at Cornell Security Seminar
- DARPA SIEVE PI Meeting

Fall 2021 "I need a better description": An Investigation Into User Expectations For Differential Privacy
- Invited talk at George Washington University
- Invited talk at Brave

Spring 2021 NIZKPoK For Disjunctions
BUSec Seminar

Fall 2019 The Hill We Must Die On: Cryptographers and Congress
Boston University Cyber Alliance

Fall 2017 Blockchain Technology Beyond Cryptocurrencies
- Invited talk at US Naval Academy
- Guest Lecture at Hagerstown Community College (Hagerstown, MD)

TEACHING

Spring 2022 (BU) — Network Security
- Enrollment of ≈ 60 students.
- Overall Course Quality Rating: 4.3/5. Overall Instructor Rating: 4.5/5
- Course syllabus available here and course reviews available here .

Spring 2022 (BU) — Confronting Surveillance: Living In Data Science's Gaze
- Enrollment of 15 students
- Each week, we bring in a different speak to talk about a different aspect of surveillance
- Course syllabus available here (Course reviews not collected for seminar courses).

Spring 2022 (BU) — Law and Algorithms (Co-taught with Andy Sellers and Ran Canetti)
- Enrollment of 15 computer science students and 10 law students
- Course covers a wide array of the ways that law and algorithms interact with each other, focusing on Transparency, Fairness, Bias, Trust, and Privacy.
- Overall Course Quality Rating: 4.2/5. Overall Instructor Rating: 4.6/5
- Course website available here and course reviews available here .

Spring 2021 (BU) — Network Security
- Enrollment of 50 students during a hybrid teaching semester.
- Course had to be completely revamped due to creation of new lower-level course that covered much of the previously covered material.
- Overall Course Quality Rating: 4.84/5. Overall Instructor Rating: 4.88/5
- Course syllabus available here and course reviews available here .

Spring 2020 (JHU) — 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
- Overall Course Quality Rating: 4.46/5. Overall Instructor Rating: 4.52/5
- Course reviews available for Section 1 and Section 2 .

Summer 2019 (JHU) — 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.
- Overall Course Quality Rating: 4.33/5. Overall Instructor Rating: 4.47/5
- Course reviews available here .

Fall 2018 (JHU) and Fall 2019 (JHU) — HEART - Introduction to Computer Security and Applied Cryptography
- 1 credit pass/fail course exposing freshman engineering students to high-level research ideas
- 10 week course. Fall 2018 two sections (total of 23 students) and Fall 2019 one section (9 students)
- F19 Ratings: Overall Course Quality Rating: 4.69/5. Overall Instructor Rating: 4.96/5
- F18 Ratings: Overall Course Quality Rating: 4.75/5. Overall Instructor Rating: 4.78/5
- Course reviews available for F18 Section 1 , F18 Section 2 , and F19 Section 1 .

Spring 2016 (JHU) and Spring 2017 (JHU) — 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 (JHU) — Head Teaching Assistant for Practical Cryptographic Systems
- Received a rating of 3.8/5 from student course reviews

Fall 2014 (JHU) — Course Assistant for Introduction to Algorithms

Spring 2014 (JHU) — Course Assistant for Automata and Computation Theory

PROFESSIONAL SERVICE

Workshop Organizer
PETs in the Public Interest (October 22)

Area Chair
FAccT 2023 (Area: Privacy and Security)

Program Committee Member
TCC 2022, USENIX 2023, IEEE S&P 2023, ACMCCS 2022, ConPro 2022, USENIX 2021, Financial Cryptography 2021

Guest Editor
ACM DTRAP Special Issue on COVID19

External Reviewer
ITCS 2022, USENIX 2022, TCC 2021, ICDCS 2021, Eurocrypt 2020, ACM HEALTH, ACM-CCS 2019, USENIX 2019, Financial Cryptography 2019, FOCI 2018, USENIX 2016, Financial Cryptography 2015

Fall 2022 Member of Boston University's Computer Science Graduate Award Committee

Fall 2018 Member of External Department Head Search Committee

Fall 2018 – Summer 2020 Member of Computer Science Graduate Student Council

Fall 2016 – Summer 2020 Member of Computer Science Curriculum Committee (non-voting)

INDUSTRY EXPERIENCE

2021 – Present **Technical Advisor**
horizontl, London UK

Fall 2019 – Present **Cryptographer**
Bolt Labs Inc, Baltimore MD

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

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

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

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

2013 – 2014 **Technical Lead**
Procia, Baltimore MD

FUNDING AND AWARDS

Fall 2022 – Fall 2023 NSF — NSF Convergence Track G "Secure Censor-resistant Overlay Resilient Networks"
$750,000

Fall 2022 – Fall 2027 NSF — Sub-awardee on NSF Frontiers Grant "Securing the Future of Computing for Marginalized and Vulnerable Populations"

Fall 2021 – Fall 2024 DARPA — Sub-awardee on Rachel Cummings' Young Faculty Award
Total Funding - $495,346.00
Personal Funding - 13% (max. allowable amount)

Fall 2021 – Fall 2022 Schmidt Futures — Workshop on Privacy Technologies and the Future of Governance
$25,000

Fall 2021 – Fall 2022 Boston University's Center for Antiracist Research — Research and Policy Team
$26,000

Fall 2020 – Fall 2022 CRA and CCC — Computing Innovation Fellow
$150,000

Fall 2020 – Fall 2022 BU CDS — Civic Tech Fellow
$10,000

Summer 2018 Tech Congress — Summer Fellow
$4,000

ACM CCS 2021 Best Paper Runner-up: "I need a better description": An Investigation Into User Expectations For Differential Privacy

Fall 2020 GYSS2020 Attendee

2018 NDSEG Finalist