

Gabriel Kaptchuk

<https://kaptchuk.com>

gabriel@kaptchuk.com

Affiliations

Assistant Professor Department of Computer Science University of Maryland, College Park, MD	2024—
Research Assistant Professor Department of Computer Science Boston University, Boston, MA	2020—Present
Civic Technology Fellow Faculty of Computing and Data Science Boston University, Boston, MA	2020—2022
Visiting Scholar Hariri Institute for Computing Boston University, Boston MA	2019—2020

Education

Johns Hopkins University , Baltimore, MD <i>PhD, Computer Science</i> Advisors: Prof. Matthew Green and Prof. Aviel Rubin <i>Dissertation Title: New Applications of Public Ledgers</i>	2015—2020
Johns Hopkins University , Baltimore, MD <i>Masters of Science, Computer Science</i>	2015—2018
Johns Hopkins University , Baltimore, MD <i>Bachelor of Science, Computer Science and Electrical Engineering</i> <i>Minor in Mathematics</i>	2011—2015

Publications

Following the norm in mathematics and theoretical computer science, authors are listed alphabetically by default. Publications in which authors are listed by contribution are marked with a star.

Peer-Reviewed Conference Publications

- Scalable Multiparty Garbling**
Gabrielle Beck, Aarushi Goel, Aditya Hegde, Abhishek Jain, Zhengzhong Jin, and GABRIEL KAPTCHUK
ACM CCS 2023. November 2023
- What Are the Chances? Explaining the Epsilon Parameter in Differential Privacy***
Priyanka Nanayakkara, Mary Anne Smart, Rachel Cummings, GABRIEL KAPTCHUK, and Elissa M. Redmiles
USENIX Security 2023. August 2023

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

Aarushi Goel, Mathias Hall-Andersen, [GABRIEL KAPTCHUK](#), and Nicholas Spooner
EUROCRYPT 2023, Part II. April 2023

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

Aarushi Goel, Matthew Green, Mathias Hall-Andersen, and [GABRIEL KAPTCHUK](#)
EUROCRYPT 2022, Part II. May / June 2022

Fluid MPC: Secure Multiparty Computation with Dynamic Participants

Arka Rai Choudhuri, Aarushi Goel, Matthew Green, Abhishek Jain, and [GABRIEL KAPTCHUK](#)
CRYPTO 2021, Part II. August 2021

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

Rachel Cummings, [GABRIEL KAPTCHUK](#), and Elissa M. Redmiles
ACM CCS 2021. November 2021
Best Paper Runner-Up

Meteor: Cryptographically Secure Steganography for Realistic Distributions*

[GABRIEL KAPTCHUK](#), Tushar M. Jois, Matthew Green, and Aviel D. Rubin
ACM CCS 2021. November 2021

Order-C Secure Multiparty Computation for Highly Repetitive Circuits

Gabrielle Beck, Aarushi Goel, Abhishek Jain, and [GABRIEL KAPTCHUK](#)
EUROCRYPT 2021, Part II. October 2021

Abuse Resistant Law Enforcement Access Systems

Matthew Green, [GABRIEL KAPTCHUK](#), and Gijs Van Laer
EUROCRYPT 2021, Part III. October 2021

Improving Signal’s Sealed Sender*

Ian Martiny, [GABRIEL KAPTCHUK](#), Adam J. Aviv, Daniel S. Roche, and Eric Wustrow
NDSS 2021. February 2021

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

[GABRIEL KAPTCHUK](#), Matthew Green, and Ian Miers
NDSS 2019. February 2019

Fairness in an Unfair World: Fair Multiparty Computation from Public Bulletin Boards

Arka Rai Choudhuri, Matthew Green, Abhishek Jain, [GABRIEL KAPTCHUK](#), and Ian Miers
ACM CCS 2017. October / November 2017

Outsourcing Medical Dataset Analysis: A Possible Solution*

[GABRIEL KAPTCHUK](#), Matthew Green, and Aviel D. Rubin
FC 2017. April 2017

Dancing on the Lip of the Volcano: Chosen Ciphertext Attacks on Apple iMessage

Christina Garman, Matthew Green, [GABRIEL KAPTCHUK](#), Ian Miers, and Michael Rushanan
USENIX Security 2016. August 2016

A Practical Implementation of a Multi-Device Split Application for Protecting Online Poker*

[GABRIEL KAPTCHUK](#) and Aviel Rubin
Annual Security Conference. April 2016

Peer-Reviewed Journal Publications

Safer Digital Intimacy for Sex Workers and Beyond: A Technical Research Agenda

Vaughn Hamilton, [GABRIEL KAPTCHUK](#), Allison McDonald, and Elissa M. Redmiles
IEEE Security & Privacy Magazine, 2023

SocIoTy: Practical Cryptography in Smart Home Contexts*

Tushar Jois, Gabrielle Beck, Sofia Belikovetsky, Joseph Carrigan, Alishah Chator, Logan Kostick, Maximilian Zinkus, [GABRIEL KAPTCHUK](#), and Avi Rubin
PoPETs, 2024(1), January 2024

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

Rachel Cummings, [GABRIEL KAPTCHUK](#), and Elissa M. Redmiles

Journal of Privacy and Confidentiality, 13(1), August 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

PoPETs, 2023(1), January 2023

Efficient Set Membership Proofs using MPC-in-the-Head

Aarushi Goel, Matthew Green, Mathias Hall-Andersen, and [GABRIEL KAPTCHUK](#)

PoPETs, 2022(2), April 2022

How Good is Good Enough? Quantifying the Impact of Benefits, Accuracy, and Privacy on Willingness to Adopt COVID-19 Decision Aids*

[GABRIEL KAPTCHUK](#), Daniel G. Goldstein, Eszter Hargittai, Jake M. Hofman, and Elissa M. Redmiles

ACM Journal on Digital Threats: Research and Practice, 3(3), March 2022

Peer-Reviewed Workshop and Non-Archival Publications

Models Matter: Setting Accurate Privacy Expectations for Local and Central Differential Privacy

Priyanka Nanayakkara, Mary Anne Smart, Rachel Cummings, [GABRIEL KAPTCHUK](#), and Elissa M. Redmiles*

Theory and Practice of Differential Privacy Workshop Series (TPDP). September 2023

Models Matter: Setting Accurate Privacy Expectations for Local and Central Differential Privacy

Priyanka Nanayakkara, Mary Anne Smart, Rachel Cummings, [GABRIEL KAPTCHUK](#), and Elissa M. Redmiles*

Theory and Practice of Differential Privacy Workshop Series (TPDP). September 2023

Designing Safer Systems for Digital Intimacy

Vaughn Hamilton, [GABRIEL KAPTCHUK](#), Allison McDonald, and Elissa M. Redmiles

IEEE Workshop on Security for Harassment Online, Protections, and Empowerment (SecHOPE). May 2023

Improving Education on Differential Privacy Protections

Priyanka Nanayakkara, Mary Anne Smart, Rachel Cummings, [GABRIEL KAPTCHUK](#), and Elissa M. Redmiles*

Privacy Interventions and Education (PIE). April 2023

Improving Education on Differential Privacy Protections

Priyanka Nanayakkara, Mary Anne Smart, Rachel Cummings, [GABRIEL KAPTCHUK](#), and Elissa M. Redmiles*

Theory and Practice of Differential Privacy Workshop Series (TPDP). September 2022

Designing for Trust and Truth in Digital Intimacy

Vaughn Hamilton, [GABRIEL KAPTCHUK](#), Allison McDonald, and Elissa M. Redmiles

Proceedings of the 2022 Truth and Trust Online Conference (TTO). October 2022

Improving Education on Differential Privacy Protections

Priyanka Nanayakkara, Mary Anne Smart, Rachel Cummings, [GABRIEL KAPTCHUK](#), and Elissa M. Redmiles*

Annual Symposium on Applications of Contextual Integrity. September 2022

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

Rachel Cummings, [GABRIEL KAPTCHUK](#), and Elissa M. Redmiles

Theory and Practice of Differential Privacy Workshop Series (TPDP). September 2021

Public Preprints

Dora: Processor Expressiveness is (Nearly) Free in Zero-Knowledge for RAM Programs

Aarushi Goel, Mathias Hall-Andersen, and [GABRIEL KAPTCHUK](#)

Cryptology ePrint Archive, Paper 2023/1749, <https://eprint.iacr.org/2023/1749>

Pulsar: Secure Steganography through Diffusion Models*

Tushar M. Jois, Gabrielle Beck, and [GABRIEL KAPTCHUK](#)

Cryptology ePrint Archive, Paper 2023/1758, <https://eprint.iacr.org/2023/1758>

Public Comments on Government Calls

Comment on “NIST SP 800-226: Guidelines for Evaluating Differential Privacy Guarantees”

Rachel Cummings, Shlomi Hod, [GABRIEL KAPTCHUK](#), Priyanka Nanayakkara, Jayshree Sarathy, and Jeremy Seeman

2024, [Link to Comment](#).

Request for Information (RFI) on Advancing Privacy Enhancing Technologies

Ran Canetti, Gabe Kaptchuk, Leonid Reyzin, Adam Smith, and Mayank Varia

2022, [Link to Comment](#).

Op-eds and Public Media

People want data privacy but don’t always know what they’re getting

Rachel Cummings, [GABRIEL KAPTCHUK](#), and Elissa M. Redmiles

Business Insider, Houston Chronicle, The Conversation, and other national media outlets. October 2020

The Success of Contact Tracing Doesn’t Just Depend on Privacy*

Elissa M. Redmiles, [GABRIEL KAPTCHUK](#), and Eszter Hargittai

Wired. May 2020

Talks

Public-Facing Presentation

What Are the Consequences of Backdoors for Online Privacy?

Panel Discussion hosted by Center for Data Innovation. April 2023

Conference Presentations

The Good, The Bad, and The Ugly—Lessons from an MPC for Social Good Deployment

Real World Crypto Symposium. March 2024

Efficient Proofs of Software Exploitability for Real-world Processors

Privacy Enhancing Technologies Symposium. January 2023

Designing for Trust and Truth in Digital Intimacy

2022 Truth and Trust Online Conference (TTO). October 2022

Efficient Set Membership Proofs using MPC-in-the-Head

Privacy Enhancing Technologies Symposium. April 2022

Commit Acts of Steganography—Before it’s too late

Real World Crypto Symposium. April 2022

Abuse Resistant Law Enforcement Access Systems

TCC Special In-Person Workshop. November 2021

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

ACM CCS 2021. November 2021

Meteor: Cryptographically Secure Steganography for Realistic Distributions

ACM CCS 2021. November 2021

Abuse Resistant Law Enforcement Access Systems

EUROCRYPT 2021, Part II. October 2021

Order-C Secure Multiparty Computation for Highly Repetitive Circuits

EUROCRYPT 2021, Part II. October 2021

Giving State to the Stateless: Augmenting Trustworthy Computation with Ledgers

NDSS 2019. February 2019

The Hill We Must Die On: Cryptographers and Congress

Real World Crypto Symposium. January 2019

Fairness in an Unfair World: Fair Multiparty Computation from Public Bulletin Boards

ACM CCS 2017. October / November 2017

Outsourcing Medical Dataset Analysis: A Possible Solution

FC 2017. April 2017

A Practical Implementation of a Multi-Device Split Application for Protecting Online Poker

Annual Security Conference. April 2016

Workshop Presentations

Analyzing Cryptography in Context: The Case Study of Apple's CSAM Scanning Proposal

Cryptographic Applications Workshop (CAW). May 2024

The Good, The Bad, and The Ugly — Lessons from an MPC for Social Good Deployment

Re-Imagining Cryptography and Privacy (ReCAP) Workshop. April 2024

Meteor, Pulsar, and Beyond: Steganography for the Machine Learning Age

Anonymity Day at Brown University. April 2024

Panel—What to know getting started in Usable Security

Panel Discussion at Annual Boston Security Usability Research Day (ABSURD). April 2024

Invited Presentations

Disjunctive Zero-knowledge

Boston Computation Club. November 2022

Speed Stacking: Fast Sublinear Zero-Knowledge Proofs for Disjunctions

DARPA SIEVE PI Meeting. October 2022

Speed Stacking: Fast Sublinear Zero-Knowledge Proofs for Disjunctions

Symposium on the Future of Computing Research. October 2022

Stacking Sigmas: Framework to Compose Σ -Protocols for Disjunctions

DARPA SIEVE PI Meeting. April 2022

Weaving Social Accountability into Cryptographic Systems

Charles River Area Crypto Day. March 2022

Abuse Resistant Law Enforcement Access Systems

Cornell Tech Security Seminar. November 2021

Abuse Resistant Law Enforcement Access Systems

DARPA SIEVE PI Meeting. October 2021

Abuse Resistant Law Enforcement Access Systems

Cornell Tech Security Seminar. November 2021

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

George Washington University Security Seminar. September 2021

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

Invited Talk at Brave. September 2021

Disjunctive Zero-knowledge

Boston Computation Club. November 2022

The Hill We Must Die On: Cryptographers and Congress

Boston University Cyber Alliance. December 2019

Blockchain Technology Beyond Cryptocurrencies

US Naval Academy Seminar. October 2017

Teaching and Mentorship

CS 558: Network Security Department of Computer Science, Boston University <i>Links to Course Reviews:</i> SP23 , SP22 , and SP1	SP23, SP22, SP21
DS 457/657, JD 673: Law and Algorithms Faculty of Computing and Data Science & School of Law, Boston University <i>Co-taught with Prof. Andrew Sellers, Prof. Ran Canetti, and Prof. Mayank Varia</i> <i>Links to Course Reviews:</i> SP23 and SP22 .	SP23, SP22
DS 199: Confronting Surveillance Faculty of Computing and Data Science, Boston University <i>No course reviews collected for seminar course.</i>	SP22
EN 601.414/614: Computer Network Fundamentals Department of Computer Science, Johns Hopkins University <i>Co-taught with Prof. Aviel Rubin</i> <i>Links to Course Reviews:</i> Section 1 and Section 2	SP20
EN 601.226.21: Data Structures Department of Computer Science, Johns Hopkins University <i>Co-taught with Prof. Joanne Selinski</i> <i>Links to Course Reviews:</i> Sum19	Sum19
EN 500.111: HEART—Introduction to Computer Security and Applied Cryptography Whiting School of Engineering, Johns Hopkins University <i>Links to Course Reviews:</i> F18 Section 1 , F18 Section 2 , and F19 Section 1	F19, F18
Course Support Experience Guest Lecturer for EN 601.414/614 Computer Network Fundamentals, Johns Hopkins University Head Teaching Assistant for EN 601.445/645 Practical Cryptographic Systems, Johns Hopkins University Course Assistant for EN 601.433/633 Introduction to Algorithms, Johns Hopkins University Course Assistant for EN 601.271 Automata and Computation Theory, Johns Hopkins University	SP17, Sp16 SP15 F14 F14
Dissertation Committees Tushar M. Jois (Johns Hopkins University), 2023 Rawane Issa (Boston University), 2022	

Work Experience

horizontl , London, United Kingdom <i>Technical Advisor</i>	2021—Present
Bolt Labs Inc , Baltimore, MD <i>Cryptographer</i>	2019—2023
Senator Ron Wyden’s Personal Office, US Senate , Washington, DC <i>Cryptography Fellow</i>	Summer 2018
Intel Labs , Portland, OR <i>Research Intern</i>	Summer 2017
Onshape , Boston, MA <i>DevOps Intern</i>	Summer 2013, Summer 2014
Proscia , Baltimore, MD <i>Technical Lead</i>	2013—2014

Service

Area Chair

ACM Conference on Fairness, Accountability, and Transparency (FACcT) 2023

Guest Editor

ACM Journal on Digital Threats: Research and Practice (DTRAP) 2022

Program Committee Member

USENIX Security Symposium 2024,2023,2021

USENIX Security Symposium Distinguished Reviewer Award 2023

IEEE Symposium on Security and Privacy (IEEE S&P) 2023

ACM Conference on Computer and Communications Security (ACM CCM) 2023,2022

IACR Theory of Cryptography Conference (TCC) 2022

Financial Cryptography 2021

Workshop on Technology and Consumer Protection (ConPro) 2022

External Reviewer

IACR Asiacrypt 2023

IACR ITCS 2022

USENIX Security Symposium 2022,2019,2016

IEEE International Conference on Distributed Computing Systems (ICDCS) 2021

IACR Eurocrypt 2020

ACM Conference on Computer and Communications Security (ACM CCM) 2019

Financial Cryptography 2019,2015

Departmental Service

Graduate Award Committee, Department of Computer Science, Boston University 2022

External Department Head Search Committee, Department of Computer Science, Johns Hopkins University 2018

Science Graduate Student Council, Department of Computer Science, Johns Hopkins University 2018—2020

Curriculum Committee (non-voting), Department of Computer Science, Johns Hopkins University 2016—2020

Workshop Organizer

PETs in the Public Interest 2023,2022

Funding

[NSF] “Secure Censor-resistant Overlay Resilient Networks”, 2022—2023

Award Information: Convergence Accelerator Track G, Number 49100422C0024

PIs: Qinqing Zhang (Peraton Labs), Gabriel Kaptchuk (Boston University), Ufuk Topcu (University of Texas at Austin), and Hongyi Wu (University of Arizona)

Total Funding: \$750,000.00

[DARPA] “Guarding Against User Misperceptions of Differential Privacy”, 2021—2024

Award Information: Sub-awardee on Prof. Rachel Cummings’ Young Faculty Award, Number W911NF-21-1-0371

Team: Rachel Cummings (Columbia University), Gabriel Kaptchuk (Boston University), and Elissa M. Redmiles (MPI for Software Systems)

Total Funding: \$495,346.00

[NSF & CRA] Computing Innovation Fellowship, 2020—2023

Award Information: Award Number #2030859

PIs: Gabriel Kaptchuk (Boston University)

Total Funding: \$150,000.00

Smaller Awards

[Schmidt Futures] Workshop on PETs and the Future of Governance, <i>Total Funding:</i> \$25,000	2021-2022
[BU CAR] Research and Policy Team, <i>Total Funding:</i> \$26,000	2021-2022
[BU CDS] Civic Technology Fellow, <i>Total Funding:</i> \$10,000	2020-2022
[Tech Congress] Summer Fellow, <i>Total Funding:</i> \$4,000	2018