

EDUCATION

---

- **Johns Hopkins** Baltimore, MD  
*PhD Computer Science* *Sept 2018 - May 2024*  
*Thesis: Towards Efficient Metadata-Hiding Cryptography*  
*Advisor: Matthew Green*
- **University of Michigan** Ann Arbor, MI  
*Bachelor of Science, with Distinction* *Sept. 2014 - April 2018*

PUBLICATIONS

---

- Tushar Jois, Gabrielle Beck, and Gabriel Kaptchuk. **Pulsar: Secure Steganography through Diffusion Models**. ACM CCS 2024.
- Harry Eldridge, Gabrielle Beck, Matthew Green, Nadia Heninger, and Abhishek Jain. **Abuse-Resistant Location Tracking: Balancing Privacy and Safety in the Offline Finding Ecosystem**. 33<sup>rd</sup> USENIX Security Symposium. Aug 14-16, 2024.
- Tushar Jois, Gabrielle Beck, Sofia Belikovetsky, Joseph Carrigan, Alishah Chator, Logan Kostick, Maximilian Zinkus, Gabriel Kaptchuk. **SocIoTy: Practical Cryptography in Smart Home Contexts**. PETS 2024.
- Gabrielle Beck, Aarushi Goel, Aditya Hegde, Abhishek Jain, Zhengzhong Jin, Gabriel Kaptchuk. **Scalable Multiparty Garbling**. ACM CCS 2023. †
- Gabrielle Beck, Arka Rai Choudhuri, Matthew Green, Abhishek Jain, Pratyush Ranjan Tiwari. **Time-Deniable Signatures**. PETS 2023.†
- Gabrielle Beck, Julia Len, Ian Miers, Matthew Green. **Fuzzy Message Detection**. ACM CCS 2021.
- Gabrielle Beck, Aarushi Goel, Abhishek Jain, Gabriel Kaptchuk. **Order-C Secure Multiparty Computation for Highly Repetitive Circuits**. EUROCRYPT 2021.†
- Gabrielle Beck\*, Maximilian Zinkus\*, Matthew Green. **Automating the Development of Chosen Ciphertext Attacks**. 29<sup>th</sup> USENIX Security Symposium. Aug 12-14, 2020.
- Deepak Kumar, Zhengping Wang, Matthew Hyder, Joseph Dickinson, Michael Bailey, Gabrielle Beck, David Adrian, Zakir Durumeric, J. Alex Halderman. **Tracking Certificate Misissuance in the Wild**. 39<sup>th</sup> IEEE Symposium on Security and Privacy (Oakland 2018), San Francisco, CA. May 21-23,2018.

★ - the authors contributed equally to the work

† - the authors are listed alphabetically rather than by contribution

TALKS

---

- **Who tracks the trackers? Balancing privacy and stalker detection for Apple's Airtags**. RWC, Mar. 2024
- **Fuzzy Message Detection**. ACM CCS, Nov. 2021
- **Order-C Secure Multiparty Computation for Highly Repetitive Circuits**. TCC, Nov. 2021
- **Automating the Development of Chosen Ciphertext Attacks**. 29<sup>th</sup> USENIX Security Symposium, Aug. 2020

## TEACHING EXPERIENCE

---

- **Johns Hopkins** Baltimore, MD  
*(Graduate) Teaching Assistant* Spring 2020/ Fall 2020
  - **Courses:** Practical Cryptographic Systems (EN.601.445), Information Theory (EN.520.447)
- **Johns Hopkins CTY Program** Lancaster and Carlisle, PA  
*Teaching Assistant* June 2019 - Aug 2019
  - **Assisting Students:** Assisted in helping students one-on-one with basic computing concepts and algorithms (ie fast exponentiation) and the cracking of classical ciphers
  - **Teaching Students:** Taught high school students (approximately 15-45 people) about a variety of modern topics in cryptography, including simplified AES and Zero Knowledge Proofs and mathematical topics like modular arithmetic, conjugations and permutations
- **University of Michigan** Ann Arbor, MI  
*Instructional Aide* Winter 2016 - Spring 2018
  - **Courses:** Discrete Math (EECS 203), Intro to Computer Security (EECS 388)

## WORK EXPERIENCE

---

- **Self-Employed** Remote  
*Cryptography Consultant* Feb 2024 - present
  - **Bolt Labs:** Doing spec writing for a new product, interfacing with engineers, reading academic papers, and looking over Github PRs for cryptographic code.
- **Trail of Bits** Remote  
*Software Assurance Intern* May 2021- Aug 2021
  - **Assurance:** Shadowed and helped with client engagements by doing code review, running automated security analysis tools, matching technical white papers to code, and communicating findings with clients in writing and through video calls
  - **Research:** Helped develop static analysis tools for common API misuse and construct an example exploit in C for a ZK project
- **Microsoft** Redmond, WA  
*Software Engineering Intern* May 2018 - July 2018
  - **Web Development:** Worked on a One Drive team doing work on the representation of customer feedback on a product to engineers. Mostly worked on creating an SPA written in javascript using D3.
- **University of Michigan** Ann Arbor, MI  
*Research Assistant* April 2017 - Aug 2017
  - **Developing a visual representation of the PKI:** Worked on integrating an interactive webpage into a currently existing website, using CSS, javascript and the graphing API D3 to represent trust relationships among CAs
  - **Researching Certificate Authorities:** Did research on Certificate Authorities, the x509 standard, baseline requirements and their failures, and other details pertaining to CAs and the web PKI.
- **Oakland University** Rochester, MI  
*Student Researcher* Summer 2016
  - **Researching Attacks on Physical Layer Security:** Read papers and watched seminars relating to security in general while also going into depth in the area of physical layer security and methods for extracting secret keys for cryptographic operations from a channel between a transmitter and receiver.
  - **Developing Attacks:** Used Machine Learning via Matlab's statistical learning package to attempt to predict channel impulse responses, using measurements taken from surrounding receivers to a given transmitter.

## IN SERVICE TO ACADEMIC INSTITUTIONS/COMMUNITY

---

- Member of Graduate Student Council for the Computer Science Department at Hopkins (recorded seminars 2018, organized a portion of the new PhD student orientation for 2020-2021)
- PC Committee member: FC (2023), CCS (2024), RWC (2025)

## FELLOWSHIPS/AWARDS

---

- Johns Hopkins Computer Science Department Fellowship (2018-2019)