

Gabrielle Beck

EDUCATION

- **Johns Hopkins** Baltimore, MD
PhD Computer Science *Sept 2018 - Present*
Advisor: Matthew Green
- **University of Michigan** Ann Arbor, MI
Bachelor of Science, with Distinction *Sept. 2014 - April 2018*

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)

WORKING EXPERIENCE

- **Trail of Bits** Remote
Software Assurance Intern *May 2021- Present*
- **Microsoft** Redmond, WA
Software Engineering Intern *May 2018 - July 2018*
- **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 public key infrastructure.
- **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.

TALKS/POSTERS

- Beck, Gabrielle. Garcia, Ponce J Kevin. Shu, Tao. Physical Layer Security: Spoofing Link Signatures. Poster presented at: MID-Michigan Symposium for Undergraduate Research Experiences; Jul 27 2016; East Lansing, MI.
- **Automating the Development of Chosen Ciphertext Attacks.** 29th USENIX Security Symposium, Aug. 2020

PUBLICATIONS

- 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**. 39th IEEE Symposium on Security and Privacy (Oakland 2018), San Francisco, CA. May 21-23,2018.
- Gabrielle Beck*, Maximilian Zinkus*, Matthew Green. **Automating the Development of Chosen Ciphertext Attacks**. 29th USENIX Security Symposium. Aug 12-14, 2020.
- Gabrielle Beck, Aarushi Goel, Abhishek Jain, Gabriel Kaptchuk. **Order-C Secure Multiparty Computation for Highly Repetitive Circuits**. EUROCRYPT 2021.†
- Gabrielle Beck, Julia Len, Ian Miers, Matthew Green. **Fuzzy Message Detection**. ACM CCS 2021.

★ - the authors contributed equally to the work

† - the authors are listed alphabetically rather than by contribution

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 2020)

AWARDS

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