# ANDREW KWONG

ankwong@umich.edu https://andrewkwong.org

## EDUCATION

**University of Michigan**

Ph.D. in Computer Science & Engineering — *Expected Spring 2023*
Masters in Computer Science & Engineering — *December 2018*
*Advisor: Daniel Genkin*

**University of California, Santa Cruz (UCSC)**

B.A. in Mathematics — *June 2016*
B.S. in Computer Science — *June 2016*
*Advisors: Ethan Miller and Darrell Long*

## AWARDS

– CCS Best Paper Award Honorable Mention 2022
– Intel Bug Bounty Award 2020
– 1st Place in Michigan CSE Honors Competition ("Best Student Research in Department") 2019
– NSF Graduate Research Fellowship Program – Honorable Mention 2018
– Highest Honors in the Major: Mathematics 2016
– Highest Honors in the Major: Computer Science 2016
– 1st Place in Symantec Capture the Flag Hacking Competition 2015
– 1st Place in National Cyber League CTF 2015
– 1st Place UCSC Hackathon for Pebble Applications 2015
– UCSC Merit Scholarship 2012

## PUBLICATIONS

### Conference Publications

1. **Checking Passwords on Leaky Computers: A Side-Channel Analysis of Chrome's Password Leak Detection Protocol**
Andrew Kwong, Walter Wang, Jason Kim, Jonathan Berger, Daniel Genkin, Eyal Ronen, Hovav Shacham, Riad Wahby, Yuval Yarom
Accepted with Shepherd at *USENIX Security Symposium* (**USENIX Security**), 2023.
(Acceptance Rate: TBD)

2. **When Frodo Flips: End-to-End Key Recovery on Frodokem via Rowhammer**
Michael Fahr*, Hunter Kippen*, Andrew Kwong*, Thinh Dang, Jacob Lichtinger, Dana Dachman-Soled, Daniel Genkin, Alex Nelson, Ray Perlner, Arkady Yerukhimovich, Daniel Apon
*ACM Conference on Computer and Communications Security* (**CCS**), 2022.
(22.4% Acceptance Rate)
**Best Paper Award Honorable Mention**
*Students listed in alphabetical order

3. **Spechammer: Combining Spectre and Rowhammer for New Speculative Attacks**
Youssef Tobah, Andrew Kwong, Ingab Kang, Daniel Genkin, Kang G. Shin
*IEEE Symposium on Security and Privacy* (**IEEE S&P**), 2022.
(14.6% Acceptance Rate)

4. **CacheOut: Leaking Data on Intel CPUs via Cache Evictions**
   Stephan van Schaik, Marina Minkin, Andrew Kwong, Daniel Genkin, Yuval Yarom
   *IEEE Symposium on Security and Privacy* (**IEEE S&P**), 2021.
   (12.0% Acceptance Rate)

5. **RAMBleed: Reading Bits in Memory Without Accessing Them**
   Andrew Kwong, Daniel Genkin, Daniel Gruss, Yuval Yarom
   *IEEE Symposium on Security and Privacy* (**IEEE S&P**), 2020.
   (12.3% Acceptance Rate)

6. **Pseudorandom Black Swans: Cache Attacks on CTR_DRBG**
   Shaanan Cohney, Andrew Kwong, Shahar Paz, Daniel Genkin, Nadia Heninger, Eyal Ronen, Yuval Yarom
   *IEEE Symposium on Security and Privacy* (**IEEE S&P**), 2020.
   (12.3% Acceptance Rate)

7. **Hard Drive of Hearing: Disks that Listen to Conversations**
   Andrew Kwong, Wenyuan Xu, Kevin Fu
   *IEEE Symposium on Security and Privacy* (**IEEE S&P**), 2019.
   (11.7% Acceptance Rate)

8. **Blue Note: How Intentional Acoustic Interference Damages Availability and Integrity in Hard Drives and Operating Systems**
   Connor Bolton, Sara Rampazzi, Chaohao Li, Andrew Kwong, Wenyuan Xu, Kevin Fu
   *IEEE Symposium on Security and Privacy* (**IEEE S&P**), 2018.
   (11.5% Acceptance Rate)

### Preprints

9. **SGAxe: How SGX Fails in Practice**
   Stephan Van Schaik, Andrew Kwong, Daniel Genkin, and Yuval Yarom
   https://sgaxe.com, 2020.

## SELECT TALKS

- **When Frodo Flips: End-to-End Key Recovery on Frodokem via Rowhammer**
  Paper Presentation at *ACM Conference on Computer and Communications Security* (**CCS**), 2022.
- **CacheOut and SGAxe: How SGX Fails in Practice**
  At *Real World Cryptography Symposium 2021* (**RWC**), 2021.
- **RAMBleed: Reading Bits in Memory Without Accessing Them**
  Paper Presentation at *IEEE Symposium on Security and Privacy* (**IEEE S&P**), 2020.
- **Hard Drive of Hearing: Disks that Listen to Conversations**
  Paper Presentation at *IEEE Symposium on Security and Privacy* (**IEEE S&P**), 2019.

## REFEREED POSTERS

- **Blue Note - How Intentional Acoustic Interference Damages Availability and Integrity in Hard Disk Drives and Operating Systems**
  Connor Bolton, Sara Rampazzi, Chaohao Li, Andrew Kwong, Wenyuan Xu, Kevin Fu
  *IEEE Symposium on Security and Privacy* (**IEEE S&P**), 2018.
- **Why do You Trust Sensors? Analog Cybersecurity Attack Demos**
  Andrew Kwong, Connor Bolton, Timothy Trippel, Kevin Fu
  *IEEE International Symposium on Hardware Oriented Security and Trust* (**HOST**), 2017.

## TEACHING EXPERIENCE AND OUTREACH

**University of Michigan** September 2018 - December 2018
*EECS 388 Graduate Student Instructor* *Ann Arbor, MI*

- Lectured to 360 students on binary exploitation topics (return-oriented-programming, heap feng shui, stack smashing, fuzzing, etc.) and taught students to use IDA Pro

**University of Michigan** January 2018 - April 2018
*EECS 588 Graduate Student Instructor* *Ann Arbor, MI*

- Led discussions on both recent and foundational papers in computer security
- Designed a project from scratch that required students to extract an RSA key from the ATmega328 micro controller by measuring its power consumption

**University of Michigan** September 2017 - December 2017
*Michigan Engineering Lunch & Lab Graduate Student Mentoring Program* *Ann Arbor, MI*

- Mentored three undergraduate students on how to pursue graduate education

**University of California, Santa Cruz** 2014-2016
*Security Santa Cruz President* *Santa Cruz, CA*

- I was the president and founder of the UCSC Computer Security team, whose primary function is to compete in Capture the Flag hacking competitions.
- Taught and worked alongside students to solve problems in cryptography, binary exploitation, forensics, and web security

## SERVICE

### External Reviewer

- ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT) (2020)
- Usenix Security Symposium (2021, 2022)
- IEEE Symposium on Security and Privacy (2018, 2019, 2020)
- ACM Computer and Communications Security Conference (2019)

## POSITIONS

**University of Michigan** July 2016 - Present
*Graduate Student Research Assistant* *Ann Arbor, MI*

**University of California, Santa Cruz** December 2014 - June 2016
*Undergraduate Research Assistant* *Santa Cruz, CA*

- Affiliation: Storage Systems Research Center

**Symantec** June 2015 - September 2015
*Security, Technology and Response Intern* *Culver City, CA*

- Analyzed and developed tools for reverse engineering malware