

# Kevin Liao

[kevliao@mit.edu](mailto:kevliao@mit.edu) | [www.kevliao.com](http://www.kevliao.com)

## Research Interests

Cryptography, systems security, formal verification

## Education

Ph.D. in EECS, Massachusetts Institute of Technology	Sep. 2020
M.S. in Computer Science, University of Illinois at Urbana-Champaign Advisor: Andrew Miller	Aug. 2017–May 2019
B.S. in Computer Science with Honors, Arizona State University Advisor: Adam Doupé	Aug. 2013–May 2017

## Honors & Awards

DFINITY scholarship	2019
National Science Foundation Graduate Research Fellowship	2017
Outstanding Undergraduate in Computer Science, Arizona State University	2017
Moeur Award, Arizona State University	2017

## Research Funding

SaUCy: Modular Testing and Verification for Distributed Cryptography Facebook, \$50,000 PI: Andrew Miller, Co-PI: <a href="#">Kevin Liao</a>	2018
Inductive Reverse Engineering of Web Applications Fulton Undergraduate Research Initiative, \$3,000 PI: <a href="#">Kevin Liao</a> , Advisor: Adam Doupé	2016

## Publications

\* = alphabetical authorship

### Refereed Conferences

- [SoK: Computer-Aided Cryptography](#)  
Manuel Barbosa, Gilles Barthe, Karthik Bhargavan, Bruno Blanchet, Cas Cremers, [Kevin Liao](#)\*, Bryan Parno  
IEEE Symposium on Security and Privacy (Oakland), May 2021
- [A Probabilistic Separation Logic](#)  
Gilles Barthe, Justin Hsu, [Kevin Liao](#)\*  
Symposium on Principles of Programming Languages (POPL), Jan. 2020
- [ILC: A Calculus for Composable, Computational Cryptography](#)  
[Kevin Liao](#), Matthew A. Hammer, and Andrew Miller  
Conference on Programming Language Design and Implementation (PLDI), Jun. 2019
- [Behind Closed Doors: Measurement and Analysis of CryptoLocker Ransoms in Bitcoin](#)  
[Kevin Liao](#), Ziming Zhao, Adam Doupé, and Gail-Joon Ahn  
Symposium on Electronic Crime Research (eCrime), Jun. 2016

### Refereed Workshops

- [Incentivizing Blockchain Forks via Whale Transactions](#)  
[Kevin Liao](#) and Jonathan Katz  
Workshop on Bitcoin and Blockchain Research (BITCOIN), Apr. 2017

## Books & Chapters

[Ransomware and Cryptocurrency: Partners in Crime](#)

Gail-Joon Ahn, Adam Doupé, Ziming Zhao, and [Kevin Liao](#)

Book chapter in *Cybercrime Through an Interdisciplinary Lens* ed. by Thomas J. Holt, Dec. 2016

## Experience

[University of Porto \(FCUP\)](#)

Visiting Researcher

Advisor: Gilles Barthe, Host: Manuel Barbosa

Porto, Portugal

Feb. 2020–Present

[Max Planck Institute for Software Systems](#)

Visiting Researcher

Advisor: Gilles Barthe

Saarbrücken, Germany

Aug. 2019–Dec. 2019

[Max Planck Institute for Security & Privacy](#)

Researcher

Advisor: Gilles Barthe

Bochum, Germany

Aug. 2019–Present

[University of Illinois at Urbana-Champaign](#)

Research Assistant

Advisor: Andrew Miller

Urbana, IL, USA

Aug. 2017–Aug. 2019

[Arizona State University](#)

Research Assistant

Advisor: Adam Doupé

Tempe, AZ, USA

May 2017–Aug. 2017

[University of Maryland](#)

Research Intern

Advisor: Jonathan Katz

College Park, MD, USA

Jun. 2016–Aug. 2016

[Arizona State University](#)

Undergraduate Research Assistant

Advisors: Gail-Joon Ahn, Adam Doupé, Ziming Zhao

Tempe, AZ, USA

Mar. 2015–May 2017

## Teaching

[Teaching Assistant](#), University of Illinois at Urbana-Champaign

CS498: Applied Cryptography

Fall 2018

[Undergraduate Teaching Assistant](#), Arizona State University

CSE220: Programming for Computer Engineering

CSE240: Introduction to Programming Languages

CSE110: Introduction to Programming

Spring 2017

Fall 2016

Fall 2014

## Advising & Mentoring

Dhruv Bohra, Eunice Zhou (UIUC)

Fall 2018

## Talks

[A Probabilistic Separation Logic](#)

Symposium on Principles of Programming Languages (New Orleans, LA, USA)

Jan. 2020

[ILC: A Calculus for Composable, Computational Cryptography](#)

Prosecco Seminar at INRIA Paris (Paris, France)

Conference on Programming Language Design and Implementation (Phoenix, AZ, USA)

Formal Methods Seminar at UIUC (Urbana, IL, USA)

Sep. 2019

Jun. 2019

Apr. 2019

[Incentivizing Blockchain Forks via Whale Transactions](#)

Workshop on Bitcoin and Blockchain Research (Sliema, Malta)

Apr. 2017

[Measurement and Analysis of CryptoLocker Ransoms in Bitcoin](#)

Symposium on Electronic Crime Research (Toronto, Canada)

Jun. 2016

## Service

### External

#### [Program Committee](#)

International Conference on Blockchain and Cryptocurrency (ICBC) 2019, 2020

#### [Artifact Evaluation Committee](#)

Programming Language Design and Implementation (PLDI) 2020

#### [External Reviewer](#)

Computer Communications 2019

Computers & Security 2019

#### [Subreviewer](#)

USENIX Security Symposium (USENIX) 2019

Future Generation Computer Systems (FGCS) 2018

Conference on Computer and Communications Security (CCS) 2017

### Community

#### [First Gen Scientists](#)

Curriculum developer

Tempe, AZ, USA  
Fall 2016