

Kevin Liao

kevliao@mit.edu | www.kevliao.com

Research Interests

Cryptography, systems security, formal verification

Education

Ph.D. in EECS, Massachusetts Institute of Technology Advisors: Henry Corrigan-Gibbs, Nickolai Zeldovich	Sep. 2020–Present
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: Kevin Liao	2018
Inductive Reverse Engineering of Web Applications Fulton Undergraduate Research Initiative, \$3,000 PI: Kevin Liao , Advisor: Adam Doupé	2016

Publications

* = alphabetical authorship

Manuscripts In Submission

High-Assurance Cryptography in the Spectre Era

Gilles Barthe, Sunjay Cauligi, Benjamin Gregoire, Adrien Koutsos, [Kevin Liao](#)*, Tiago Oliveira, Swarn Priya, Tamara Rezk, Peter Schwabe

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

Logging to the Danger Zone: In-Memory Attacks and Defenses on System Auditing Frameworks

Riccardo Paccagnella, [Kevin Liao](#), Dave (Jing) Tian, Adam Bates
ACM Conference on Computer and Communications Security (CCS), Nov. 2020

A Probabilistic Separation Logic

Gilles Barthe, Justin Hsu, [Kevin Liao](#)*
ACM SIGPLAN Symposium on Principles of Programming Languages (POPL), Jan. 2020

ILC: A Calculus for Composable, Computational Cryptography

[Kevin Liao](#), Matthew A. Hammer, and Andrew Miller
ACM SIGPLAN 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

APWG 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

[Massachusetts Institute of Technology](#)

Research Assistant

Advisors: Henry Corrigan-Gibbs, Nickolai Zeldovich

Cambridge, MA, USA

Sep. 2020–Present

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

Visiting Researcher

Advisor: Gilles Barthe, Host: Manuel Barbosa

Porto, Portugal

Feb. 2020–May 2020

[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–Sep. 2020

[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

Talks

[SoK: Computer-Aided Cryptography](#)

Symposium on Security and Privacy (Oakland) (San Francisco, CA, USA)

May 2021

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)	Sep. 2019
Conference on Programming Language Design and Implementation (Phoenix, AZ, USA)	Jun. 2019
Formal Methods Seminar at UIUC (Urbana, IL, USA)	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](#)

USENIX Security Symposium 2021

Symposium on Operating Systems Design and Implementation (OSDI) 2021

Conference on Programming Language Design and Implementation (PLDI) 2020

[External Reviewer](#)

Computer Communications 2019

Computers & Security 2019

[Subreviewer](#)

USENIX Security Symposium 2019

Future Generation Computer Systems (FGCS) 2018

Conference on Computer and Communications Security (CCS) 2017

Mentoring & Outreach

MIT Graduate Application Assistance Program (GAAP)	Fall 2020
Mentor	
UIUC Promoting Undergraduate Research in Engineering (PURE)	Fall 2018
Mentor	
First Gen Scientists	Fall 2016
Curriculum developer	