Kevin Liao

kevliao@mit.edu ⧉ │ www.kevliao.com ⧉

Research Interests

Cryptography, systems security, formal verification

Education

Ph.D. in EECS, Massachusetts Institute of Technology   Sep. 2020–Present
Advisors: Henry Corrigan-Gibbs, Nickolai Zeldovich

M.S. in Computer Science, University of Illinois at Urbana-Champaign   Aug. 2017–May 2019
Advisor: Andrew Miller

B.S. in Computer Science with Honors, Arizona State University   Aug. 2013–May 2017
Advisor: Adam Doupé

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   2018
Facebook, $50,000
PI: Andrew Miller, Co-PI: Kevin Liao

Inductive Reverse Engineering of Web Applications   2016
Fulton Undergraduate Research Initiative, $3,000
PI: Kevin Liao, Advisor: Adam Doupé

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

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   Cambridge, MA, USA
Research Assistant   Sep. 2020–Present
Advisors: Henry Corrigan-Gibbs, Nickolai Zeldovich

University of Porto (FCUP)   Porto, Portugal
Visiting Researcher   Feb. 2020–May 2020
Advisor: Gilles Barthe, Host: Manuel Barbosa

Max Planck Institute for Software Systems   Saarbrücken, Germany
Visiting Researcher   Aug. 2019–Dec. 2019
Advisor: Gilles Barthe

Max Planck Institute for Security & Privacy   Bochum, Germany
Researcher   Aug. 2019–Sep. 2020
Advisor: Gilles Barthe

University of Illinois at Urbana-Champaign   Urbana, IL, USA
Research Assistant   Aug. 2017–Aug. 2019
Advisor: Andrew Miller

Arizona State University   Tempe, AZ, USA
Research Assistant   May 2017–Aug. 2017
Advisor: Adam Doupé

University of Maryland   College Park, MD, USA
Research Intern   Jun. 2016–Aug. 2016
Advisor: Jonathan Katz

Arizona State University   Tempe, AZ, USA
Undergraduate Research Assistant   Mar. 2015–May 2017
Advisors: Gail-Joon Ahn, Adam Doupé, Ziming Zhao

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   Spring 2017
CSE240: Introduction to Programming Languages   Fall 2016
CSE110: Introduction to Programming   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)	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

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 (USENIX) 2019
Future Generation Computer Systems (FGCS) 2018
Conference on Computer and Communications Security (CCS) 2017

Community

First Gen Scientists	Tempe, AZ, USA
Curriculum developer	Fall 2016