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
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: <u>Kevin Liao</u>	2018
Inductive Reverse Engineering of Web Applications Fulton Undergraduate Research Initiative, $3,000 PI: <u>Kevin Liao</u>, Advisor: Adam Doupé	2016

Publications

* = alphabetical authorship

Manuscripts In Submission

SoK: Computer-Aided Cryptography
Manuel Barbosa, Gilles Barthe, Karthik Bhargavan, Bruno Blanchet, Cas Cremers, <u>Kevin Liao</u>*, Bryan Parno

Refereed Conferences

A Probabilistic Separation Logic
Gilles Barthe, Justin Hsu, <u>Kevin Liao</u>*
Symposium on Principles of Programming Languages (POPL), Jan. 2020

ILC: A Calculus for Composable, Computational Cryptography
<u>Kevin Liao</u>, 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
<u>Kevin Liao</u>, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn
Symposium on Electronic Crime Research (eCrime), Jun. 2016

Refereed Workshops

Incentivizing Blockchain Forks via Whale Transactions
<u>Kevin Liao</u> 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 <u>Kevin Liao</u>
Book chapter in *Cybercrime Through an Interdisciplinary Lens* ed. by Thomas J. Holt, Dec. 2016

Experience

University of Porto (FCUP)	Porto, Portugal
Visiting Researcher	Feb. 2020–Present
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–Present
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
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