

# Shaokai Lin

shaokai@berkeley.edu | <https://shaokai.co>

Last updated August 2020

## Education

---

### University of California, Berkeley

*Ph.D. in Computer Science*

Berkeley, CA

June 2020 - Present

- Advisors: Prof. Edward Lee and Prof. Sanjit Seshia

### Columbia University

*BS in Computer Science*

New York, NY

Sept. 2017 - May 2020

## Presentations

---

- **Shaokai Lin**, Zichuan Wang, Lior Horesh. (2019). *Communication over Continuous Quantum Secure Dialogue using Einstein-Podolsky-Rosen States*. Poster presented at QIP 2020.

## Research Experiences

---

### **Scivik: compositional verification of blockchain smart contracts**

*Research Assistant for Prof. Ronghui Gu at Columbia University*

New York, NY

Sept. 2019 - Jan. 2020

- Led a team of 5 students in developing an automated formal verification framework for Ethereum smart contracts, which focused on functional correctness, usability, and reduction of false-positive test results
- Implemented a parser, a translator, and a proof manager using OCaml and Why3 to parse, translate, and solve SMT proof obligations generated from smart contracts' intermediate representation named Yul
- Designed and built a security pattern checker in Why3 to enforce security pattern matching, which detects unsecure patterns in smart contracts and reveals additional vulnerabilities

### **Armor: secure partitioning of C programs with on-demand memory management**

*Research Assistant for Prof. Stephen Edwards at Columbia University*

New York, NY

Sept. 2019 - Dec. 2019

- Designed and built a Clang extension using LibTooling to partition C programs and generate multiple partition executables for different machine environments
- Developed a virtual memory layer to store and synchronize data shared by partitions labeled as “secure” or “unsecure”; designed a metadata table for tracking metadata of a C pointer (dirty bits, memory bounds, permissions, etc.) to enable on-demand cross-boundary data provision
- Produced an LLVM pass to conduct source code transformation by replacing C memory management functions (e.g. malloc, memcpy, etc.) with memory management functions tailored for the virtual memory layer

### **Continuous quantum secure dialogue (CQSD) protocol**

*Research Assistant for Prof. Lior Horesh at Columbia University*

New York, NY

May 2019 - Nov. 2019

- Developed the Continuous Quantum Secure Dialogue protocol (CQSD), a quantum communication protocol which enables the continuity of qubit state exchange between two parties through a secure quantum channel
- Conducted security analysis on the CQSD protocol and compared its security performance against previous generations of quantum communication protocols; analyzed the efficiency and performance of these communication protocols under noisy environments
- Experimented with the CQSD protocol using the Qiskit framework on a 15-qubit IBMQ quantum computer

### **Serverlessnet: IoT network prototyping with serverless architecture**

*Research Assistant for Prof. Henning Schulzrinne at Columbia University*

New York, NY

Feb. 2019 - May 2019

- Designed and implemented Serverlessnet (<https://serverless-net.github.io/serverlessnet/>), an Internet of Things (IoT) network prototyping tool with the integration of serverless architecture to demonstrate the improved energy efficiency and resilience of a serverless-enabled IoT network

- Built a simulation environment using Mininet, Docker; implemented a serverless module using Apache OpenWhisk; created an HTTP request relay using Flask
- Benchmarked the performance of serverless-enabled IoT network using Serverlessnet by running different network topologies including one-to-one and one-to-many relationships between switches and actuators

## Work Experiences

---

### CertiK

New York, NY

*Software Engineering Intern, Department of Engineering*

May 2019 - Aug. 2019

- Researched into and developed formal verification techniques to verify the VM-level logical correctness of blockchain smart contracts; discussed formal verification solutions with clients and how to integrate formal verification into their blockchain platforms
- Designed and implemented an automated formal verification engine using Python and Microsoft Z3 to analyze smart contracts against specifications, generate SMT proof tasks, and output security reports
- Implemented the gas model in the CertiK Chain virtual machine (CVM) using Golang, Hyperledger Burrow, and Cosmos SDK

### BitRights.io: Digital Content Registration and Licensing Platform

New York, NY

*Co-Founder and CTO*

Feb. 2018 - Feb. 2019

- Co-founded a digital content licensing startup that enables media organizations and digital content creators to streamline the digital content licensing process using the blockchain technology
- Designed and built a scalable, cost-effective data persistence infrastructure using InterPlanetary File System (IPFS) and the Stellar blockchain
- Built a REST API with Node.js, Express, MongoDB, and Stellar SDK; implemented microservices architecture using RabbitMQ; deployed server and IPFS nodes using AWS EC2 and Elastic Load Balancer
- Accepted into NYC Media Lab Combine program; secured funding from the NYC Economic Development Corporation and Columbia School of Engineering and Applied Sciences

## Honors & Awards

---

- Dean's List (top 20%) 2016 - 2019
- 2nd Place, Akraino 5G MEC Hackathon (Project: Smart City Emergency Traffic Control) 2019
- SEAS cFUND Ignition Grants, Columbia School of Engineering and Applied Sciences 2018
- NYC Media Lab Combine Grant, NYC Media Lab 2018

## Media Coverage

---

- "Blockchain, Beyond the Hype," *Columbia Engineering Magazine*, Columbia University, May 2019.
- "NYC Media Lab Combine launches 11 new startups," *Combine*, May 2018.

## Technical Skills

---

*Programming Languages:* Python, C/C++, Coq, OCaml, Java, Javascript, LaTeX