Yuncong Hu

Assistant Professor at Shanghai Jiao Tong University

Personal Information

EMAIL: yuncong_hu@berkeley.edu
HOMEPAGE: huyuncong.com
GITHUB: @huyuncong

Research Interests

I am broadly interested in systems security and applied cryptography. My current research focuses on secure decentralized systems and zero-knowledge proofs.

Education

2017-2022 Doctor of Philosophy in Computer Science, UC Berkeley
Advisors: Prof. Raluca Ada Popa and Prof. Alessandro Chiesa
Thesis: Decentralized Ledgers: Design and Applications

2017-2020 Master of Science in Computer Science, UC Berkeley
Advisors: Prof. Raluca Ada Popa and Prof. Alessandro Chiesa
Thesis: Broadcast Encryption with Fine-grained Delegation and its Application to IoT

2013-2017 Bachelor in Computer Science, Shanghai Jiao Tong University (SJTU), China
ACM Honored Class, Zhiyuan College

Selected Publications

- *A Succinct Range Proof for Polynomial-based Vector Commitment*
  Rui Gao, Zhiguo Wan, *Yuncong Hu (corresponding author)*, Huaqun Wang
  CCS 2024 (31th ACM Conference on Computer and Communications Security)
- *VPNNT: A Verifiable and Privacy-Preserving Neural Network Training Framework*
  Haohua Duan, Zedong Peng, Liyao Xiang, *Yuncong Hu*, Bo Li
  TDSC 2024 (IEEE Transactions on Dependable and Secure Computing)
- *Hadamard Product Argument from Lagrange-Based Univariate Polynomials*
  Jie Xie, *Yuncong Hu (corresponding author)*, Yu Yu
  ACISP 2024 (29th Australasian Conference on Information Security and Privacy)
- *Gemini: Elastic SNARKs for Diverse Environments*
  (alphabetical order) Jonathan Bootle, Alessandro Chiesa, *Yuncong Hu* and Michele Orrù
  Eurocrypt 2022 (41st Annual International Conference on the Theory and Applications of Cryptographic Techniques)
- *Non-Interactive Differentially Anonymous Router*
  (alphabetical order) Benedikt Bünz, *Yuncong Hu*, Shin'ichiro Matsuo and Elaine Shi
  Cryptology ePrint Archive 2021
- *Merkle^2: A Low-Latency Transparency Log System*
  Yuncong Hu, Kian Hooshmand, Harika Kalidhindi, Seung Jin Yang, Raluca Ada Popa
  S&P 2021 (42nd IEEE Symposium on Security and Privacy)
- *Marlin: Preprocessing zkSNARKs with Universal and Updatable SRS*
  (alphabetical order) Alessandro Chiesa, *Yuncong Hu*, Mary Maller, Pratyush Mishra, Noah Vesely, and Nicholas P. Ward
  Eurocrypt 2020 (39th Annual International Conference on the Theory and Applications of Cryptographic Techniques)

- *Ghostor: Toward a Secure Data-Sharing System from Decentralized Trust*
  Yuncong Hu, Sam Kumar, and Raluca Ada Popa
  NSDI 2020 (17th USENIX Symposium on Networked Systems Design and Implementation)
- *JEDI: Many-to-Many End-to-End Encryption and Key Delegation for IoT*
  Sam Kumar, *Yuncong Hu*, Michael P Andersen, Raluca Ada Popa, and David E. Culler
  USENIX Security 2019 (28th USENIX Security Symposium)

Open Source Projects

- Merkle^2: A Low-Latency Transparency Log System (S&P 2021)
  - A Go library that implements a low-latency transparency log system and a new authenticated data structure. Our system can support 100x more users than prior state-of-the-art key transparency systems.
- Arkworks: An Ecosystem for Developing and Programming with zkSNARKs
  - A modular, coherent Rust ecosystem that provides a low-cost abstraction for developing and programming with zkSNARKs. Our ecosystem has been used in several blockchain companies (such as Aleo) for building applications with zkSNARKs.
  - The Marlin library implements a preprocessing zkSNARK for R1CS with universal and updatable SRS and is publised at Eurocrypt 2020.
  - The Gemini library implements an elastic zkSNARK for R1CS and is publised at Eurocrypt 2022.
- JEDI: Many-to-Many End-to-End Encryption and Key Delegation for IoT (USENIX Security 2019)
  - A Golang library that implements a secure many-to-many messaging protocol with decentralized key delegations for IoT devices. Our library has been used in a decentralized authorization framework that has been running for more than 2 years, with more than 800 IoT devices.

Selected Talks

- **Gemini: Elastic SNARKs for Diverse Environments**
  - ChinaCrypt 2023
  - CMU Cylab Crypto Seminar 2022
- **Merkle^2: A Low-Latency Transparency Log System**
  - RISELab Retreat Summer 2021
  - S&P 2021 (42nd IEEE Symposium on Security and Privacy)
- **Marlin: Preprocessing zkSNARKs with Universal and Updatable SRS**
  - Eurocrypt 2020 (39th Annual International Conference on the Theory and Applications of Cryptographic Techniques)
- **Ghostor: Toward a Secure Data-Sharing System from Decentralized Trust**
  - RISELab Retreat Winter 2020, Summer 2019, Winter 2019, Summer 2018.
  - Microsoft Research Redmond Cryptography Colloquium 2020.
- **JEDI: Many-to-Many End-to-End Encryption and Key Delegation for IoT**

  - RISELab Retreat Summer 2019, Summer 2018, Winter 2018.
  - Stanford Secure Internet of Things Project 2018.

Selected Scholarships, Grants, and Awards

- Science Fund Program for Excellent Young Scientists (Overseas), 2023
- Shanghai Overseas High-level Young Talents, 2023
- ExploreX Research Grant, Shanghai Jiao Tong University, 2022
- Berkeley Graduate Division Conference Travel Grant, University of California, Berkeley, 2020
- Hui-Chun Chin and Tsung-Dao Lee Chinese Undergraduate Research Endowment Receiver, Shanghai Jiao Tong University, 2017
- Boot Camp Project Grand Prize Winners (top 1), IC3-Ethereum Crypto Boot Camp and Workshop, 2016
  - Blog and Report
- International Collegiate Programming Contest (ACM-ICPC) Asia Regional
  - 10th Place in Taichung site, 2014
  - Gold Medal in Hangzhou site, 2013

Service

Program Committee	Asiacrypt 2023, USENIX Security 2024

Work Experience

Summer 2021	Research intern at NTT Research Lab, advised by Prof. Elaine Shi and Prof. Shin'ichiro Matsuo
Fall 2016	Research intern at Cornell University, advised by Prof. Elaine Shi

Teaching

Spring 2024	Introduction to Blockchains, Shanghai Jiao Tong University
Fall 2023	Introduction to Cryptography, Shanghai Jiao Tong University