Ganyuan Cao

E-mail: ganyuan.cao@epfl.ch

Site: ganyuancao.github.io

Phone: +86 131-2676-8780

Education

- **M.Sc Informatique** — Lausanne, Switzerland
  École polytechnique fédérale de Lausanne - EPFL — *Expected 2021 - 2023*
  - Concentration: Cybersecurity
- **B.Sc Computer Science** — Tempe, AZ, USA
  Arizona State University — *2016 - 2020*
  - Concentration: Cybersecurity
  - Minor/Certificate : Cryptology
  - Honors: Summa Cum Laude (GPA: 3.83/4.0)

Experience

- *Independent Research* — July 2020 - Now
  - Author a book about Cryptography including content of Number Theory, Abstract Algebra, and Elliptic Curves. (link to the current version of the book)
  - Work on a proposal that utilizes efficient Zero-knowledge Proof system in distributed environment via secure outsourcing computation.
- *Research Assistant* — Fall 2017 - Fall 2018
  Laboratory of Security Engineering for Future Computing(**SEFCOM**), Arizona State University
  - Work on algorithms and protocols to increase the Proof-of-Work blockchain mining efficiency while persevering the original security features.
  - Evaluate performance of different blockchain consensus protocols including Proof-of-Work, Proof-of-Stake, and Byzantine Fault Tolerance protocols.

Publications

1. Xue, Tengfei, Yuyu Yuan, Zahir Ahmed, Krishna Moniz, **Ganyuan Cao**, and Cong Wang. ”Proof of Contribution: A Modification of Proof of Work to Increase Mining Efficiency.” In 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), pp. 636-644. IEEE, 2018. (link to paper)
2. **Cao,Ganyuan**. ”Estafette : A Parallelized Block Generation Protocol to increase scalability of cryptocurrencies”. In 2018 Arizona State University CryptoRally poster session. (link to poster)
3. **Cao,Ganyuan**. ”Computational Problems in Designing Asymmetric Cryptosystems”. 2019. Arizona State University, Bachelor’s Research Paper. (link to paper)

Awards

Dean's List Fall 2016 - Spring 2018, Spring 2019 - Spring 2020
Ir.A Fulton School of Engineering, Arizona State University

Skills & Endorsements

- *Relevant Knowledge:* Cryptography, Blockchain, Abstract Algebra, Elliptic Curves
- *Programming Languages:* Python, C/C++, Java, Soldity
- *Mathematical Computation:* Wolfram Mathematica, Pari/GP
- *OS & Framework:* Linux, Docker
- *Text Editing:* LaTeX, Markdown

Certificates

1. Bitcoin and Cryptocurrency Technologies → Coursera
2. Blockchain → Coursera (link to certificate)
3. Cryptography I → Coursera (link to certificate)
4. Cryptography and Information Theory → Coursera (link to certificate)
5. Cyber Attack Countermeasures → Coursera (link to certificate)