Fangke Li

ACM Honor Class, SJTU
Email: lifangke@sjtu.edu.cn
Website: venillalemon.github.io

EDUCATION

Shanghai Jiao Tong University *September 2022 – June 2027 (expected)*
B.Eng. in Computer Science, ACM Honor Class *GPA: 4.08 (Rank: 3/27)*

RESEARCH INTERESTS

- Applied cryptography
- Cryptographic hard problems and computational complexity
- AI-based cryptanalysis

PUBLICATIONS AND MANUSCRIPTS

- **Triptych: Scalable Threshold ML-DSA with Low Online Communication**.
  Fangke Li, Hanlin Liu, Xiao Wang, Kang Yang, Yu Yu, Wenhao Zhang.
  Under submission to IEEE S&P 2027.
- **Fair Exchange of Computation**.
  Dung Bui, **Fangke Li**, Hanlin Liu, Xiao Wang.
  Under submission to IEEE S&P 2027.

RESEARCH EXPERIENCE

Northwestern University *July 2026 – Present*
Student Intern, working under the guidance of Prof. Xiao Wang

- Designed and implemented a threshold signing protocol for ML-DSA (see Triptych under Projects).

Shanghai Jiao Tong University *July 2025 – Present*
Lattice Cryptography Lab, working under the guidance of Prof. Shi Bai and Prof. Yu Yu

- Investigated reductions among lattice problems, including LWE, the Dihedral Coset Problem (DCP) and their variants.
- Analyzed classical combinatorial algorithms (BKW- and Wagner-style) for the Short Integer Solution (SIS) problem.

RELEVANT COURSEWORK

- **Cryptography and theory:** Modern Cryptography, Computational Complexity, Algorithm Design & Analysis, Topics in Advanced Algorithms
- **Mathematics:** Mathematical Logic, Algebra, Probability Theory, Combinatorics, Harmonic Analysis

PROJECTS

Triptych *July 2026 – November 2026*
Threshold signing protocol for ML-DSA (FIPS 204), research project with Prof. Xiao Wang

- Proposed a threshold signing protocol that combines preprocessing with a small garbled circuit, producing standard ML-DSA signatures.
- Implemented the protocol in C++ on top of the **EMP toolkit**.

Online Judger for the Rx* Compiler Course *October 2025*

- Built a online judger using Docker sandbox, Flask, MySQL, and Redis for student compilers during TA work.

PROVE *May 2025 – June 2025*

- Formally verified a first-order logic theorem prover in **Coq**, using structural induction, separation logic and monads.

Mx* Compiler *August 2024 – March 2025*

- Built a compiler from a C-like language to RV32I assembly, with graph-coloring register allocation and incremental, multi-threaded builds.

BurningCPU *November 2024*

- Implemented a RISC-V CPU with Tomasulo's algorithm in **Verilog**, supporting out-of-order execution, register renaming and speculative execution.

HONORS AND AWARDS

Honorable Mention in S.-T. Yau Mathematics Contest *2024*
Applied & Computational Mathematics

- Ranked 20th among about 300 participants.

National Scholarship, Ministry of Education of China (Top 10%) *2024*

Ruiyuan-Hongshan Scholarship, SJTU (Top 15%) *2025*

TEACHING EXPERIENCE

C++ Programming, Teaching Assistant *September 2024 – January 2025*

Data Structures, Teaching Assistant *February 2025 – June 2025*

Compiler Design and Implementation, Teaching Assistant *August 2025 – January 2026*

MISCELLANEOUS

Languages: Chinese (Native), English (Fluent, TOEFL 104)