Kunming Jiang

Gates & Hillman Centers, Office 5103
4902 Forbes Ave, Pittsburgh, PA 15213
E: kunmingj@andrew.cmu.edu P: 646-220-7606

EDUCATION

Carnegie Mellon University   **Pittsburgh, PA**
Ph.D. candidate in Computer Science   since September 2022
Advisors: Riad Wahby and Fraser Brown

New York University   **New York, NY**
Bachelor of Art, *Summa Cum Laude*   May 2022
Major in Mathematics and Computer Science, Minor in German

RESEARCH PROJECTS

CoBBl, *with Riad Wahby and Fraser Brown*   September 2022 — Present
- Explored verifiable computation through the lens of program basic blocks.
- Compiler-proof system co-design that minimizes proving time of SNARK systems.
- Implemented in *Rust* an end-to-end system ranging from high-level programs down to low-level polynomial evaluation.
- Paper under review in IEEE S&P 2025.

Ceno Recursive Verifier, *with Scroll Team*   June 2024 — Present
- Explored the viability of CoBBl as a recursive verifier to Scroll's newest zkVM system.
- Developed CoBBl to match industry-level performance as well as co-designed and implemented a batched version of the WHIR polynomial commitment scheme.

DictOSON, *with Garret Swart and Oracle Team*   June 2023 — August 2023
- Drafted and implemented a new JSON encoding format that reduces storage space by up to 50% while maintaining the same data retrieval speed.
- Collaborated with designers of previous JSON encodings to evaluate the performance of the new format across real-life use cases.
- Project currently under patent review.

Distiller, *with Michael Walfish and Thomas Wies*   May 2020 — May 2023
- Formulated a standardized technique to prove the correlation between a C program and its high-level specification. Enabled more concise SNARK proofs without losing any correctness guarantees.
- Constructed in *C* an end-to-end automated system that verifies the correctness of selected benchmarks and records the improvement.
- Paper accepted to IEEE S&P 2023. See citation underline below.

PUBLICATIONS

K. Jiang, D. Chait-Roth, Z. DeStefano, M. Walfish and T. Wies, "Less is more: refinement proofs for probabilistic proofs," *2023 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2023, pp. 1112-1129, doi: 10.1109/SP46215.2023.10179393