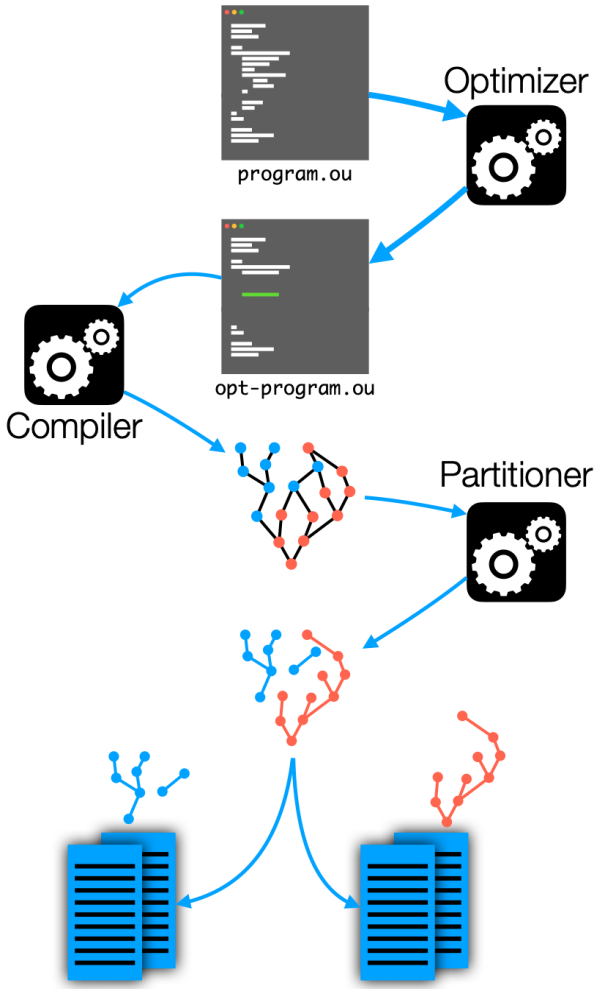
Automating and Synthesizing Parallel Zero-Knowledge Protocols

Challenge:

- Identifying the best distribution strategy for ZKP protocols
- Synthesizing ZK-specific optimizations leveraging prover-provided hints/witnesses and verifier-provided randomness



Solution:

- Maximize throughput by leveraging ZK-specific parallelism
- Automatically find optimizations harnessing extended witnesses

Scientific Impact:

- **Static and dynamic** analysis to **infer properties** towards ZK-specific optimizations.
- **Live variable analysis and simulations**, with prover witnesses and verifier-provided randomness, to find optimal circuit.
- Allowing for **knowledge-levels** and **atomic processing**.

Broader Impact and Broader Participation:

- Accelerating the deployment of Zero-Knowledge Proofs bringing auditability and transparency to legal, financial and healthcare systems
- Ning Luo, PhD student with PI Piskac and Postdoc with PI Wang, joined UIUC as a tenure-track assistant professor
- Open-source analysis tools, compilers and languages.

2318974, Yale University
2318975, Northwestern University
Ruzica Piskac (Yale), Xiao Wang (Northwestern), Timos Antonopoulos (Yale)