Accelerating Garbled Circuits for Arbitrary Privacy-Preserving Computation

Privacy and security have rapidly emerged as priorities in system design. One powerful solution for providing both is privacy-preserving computation, where functions are computed directly on encrypted data. Garbled circuits are a privacy-preserving technology that enable execution on encrypted data using Boolean logic. A key benefit of garbled circuits is that they support arbitrary functions, including conditionals. The main drawback is that they incur significant performance overheads compared to the plaintext alternative. We are proposing an accelerator and compiler to mitigate the performance overheads of garbled circuits, reducing the runtime and starting the key insights of the performance benefits. The result shows our accelerator provides an average speedup of 263× over software.

Presentation Video:
http://bit.ly/ADA-AS22-MoJ

Jianqiao Mo, Ph.D. student

Co-authors: Jayanth Gopinath
Affiliation(s): NYU
Faculty Advisor: Reagen
Research Interests: Privacy-preserving Computation Acceleration
Expected Graduation Date: 7/1/2025
Career Interest(s): Academia
Research Tasks: 2.7/2775.028 - Privacy-Enhanced Computation