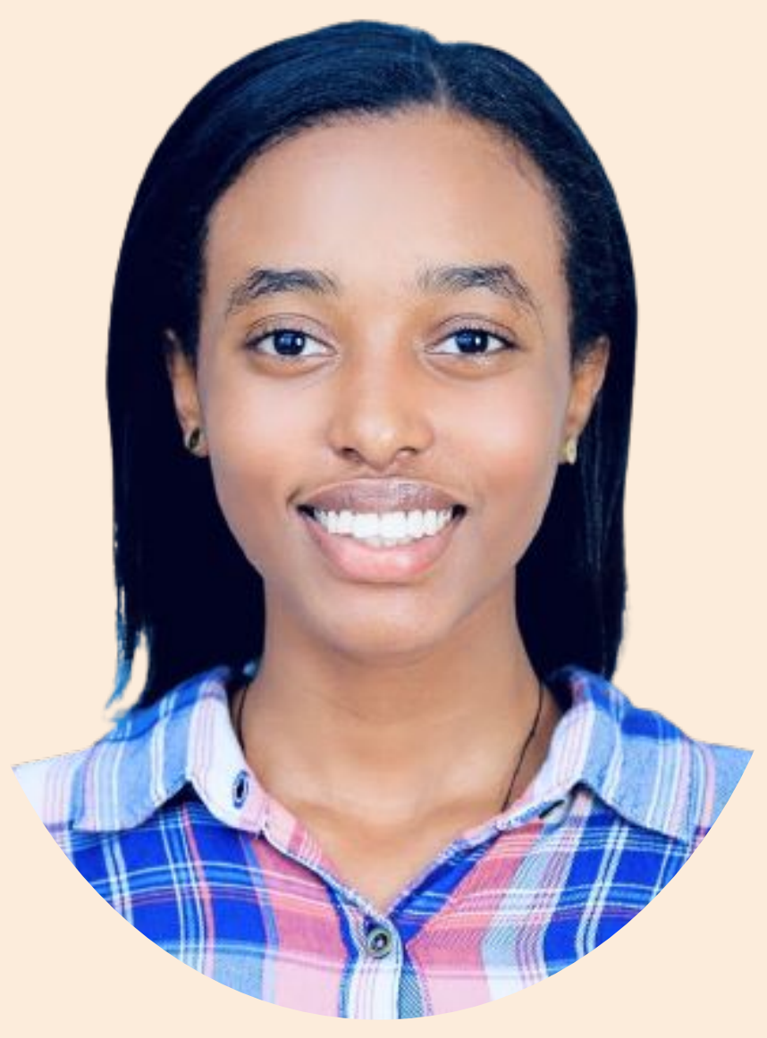


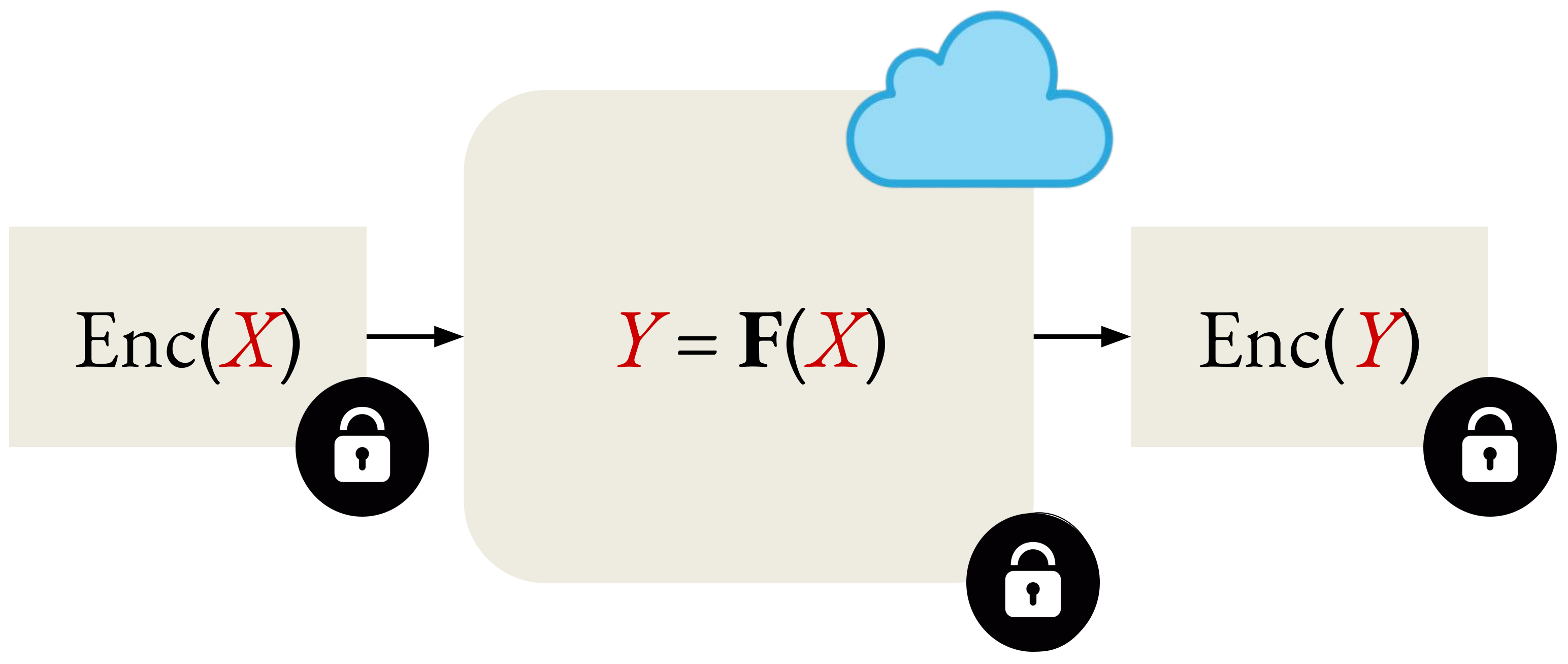
DAC Young Fellows

DESIGN AUTOMATION CONFERENCE
FROM CHIPS TO SYSTEMS — LEARN TODAY, CREATE TOMORROW

Meron Zerihun Demissie, Todd Austin, University of Michigan

Introduction

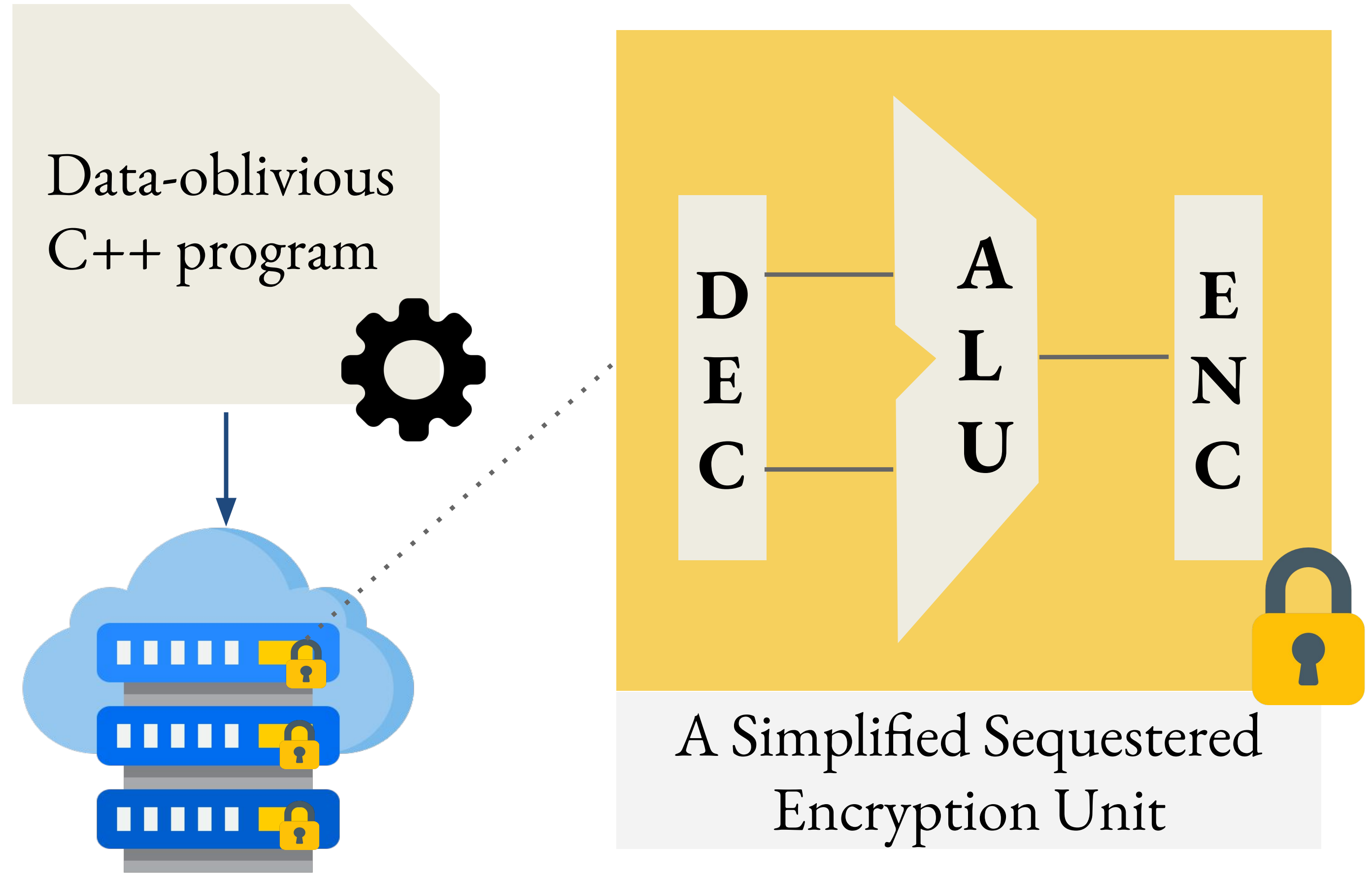
Privacy-enhanced computation frameworks enable software to **operate on private data** *without* exposing their data values.



Present-day privacy-enhanced computation frameworks like **homomorphic encryption** suffer from **prohibitive overheads** (>10,000x).

Sequestered Encryption

Sequestered Encryption (SE) is a hardware technique that enables privacy-enhanced computation by **encrypting data** throughout the pipeline and enforcing **data-oblivious programming**.

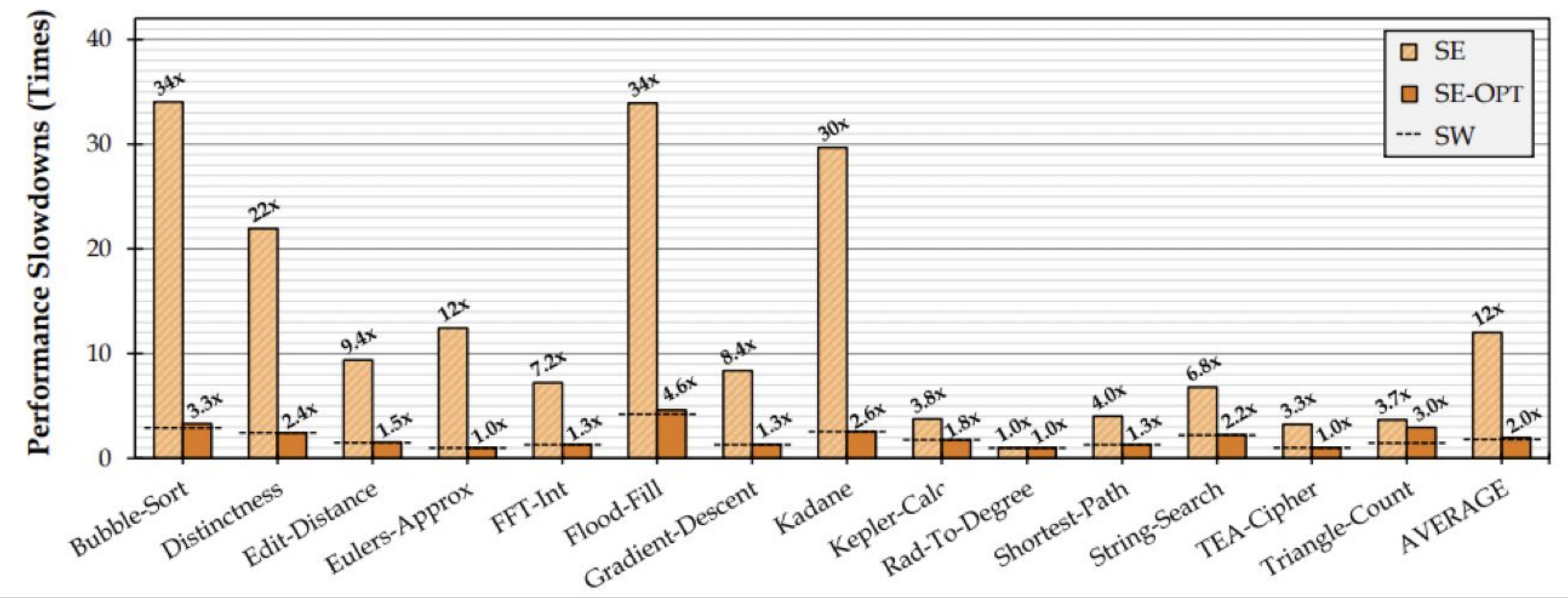


A Simplified Sequestered Encryption Unit

Going Beyond Hacking with Encrypted and Tamper-proof Computation

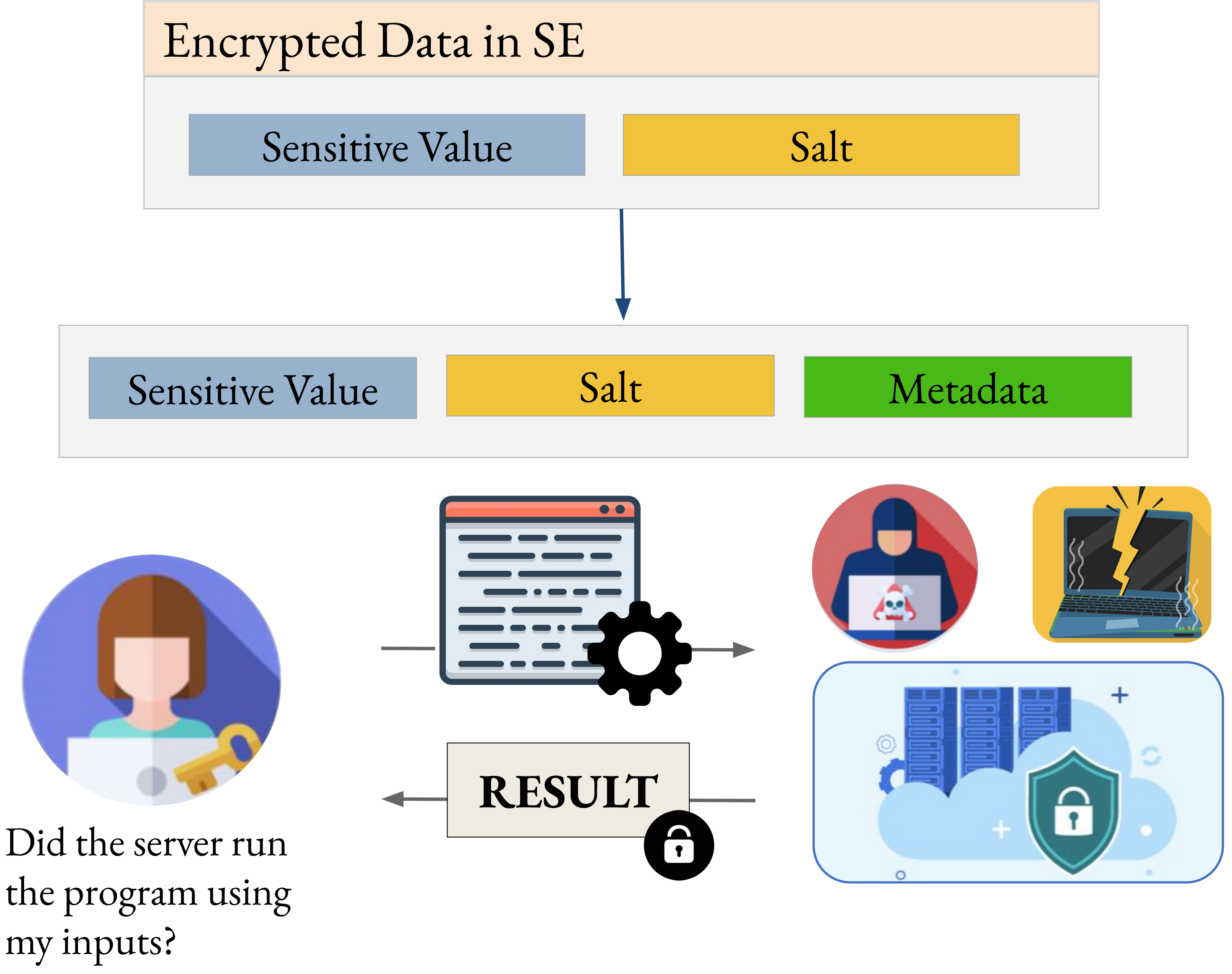
Performance Evaluation

We prototyped Sequestered Encryption in gem5 and evaluated it on VIP-Bench. With the help of micro-architectural optimizations, the overheads incurred using QARMA lowered to **2x** geomean.



Performance Overheads of SE using QARMA

Future Work



UNIVERSITY OF MICHIGAN