Going Beyond Hacking with Encrypted and Tamper-proof Computation

**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**.

**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.

**Future Work**

- **Encrypted Data in SE**
  - Sensitive Value
  - Salt
- **Sensitive Value**
- **Salt**
- **Metadata**

**RESULT**

Did the server run the program using my inputs?