The secure multiparty computation problem

- In the secure multiparty computation (MPC) problem, a group of parties seeks to compute a joint function over their private inputs, without revealing more than the final result.
- The MPC problem is general and can model a broad range of applications from privacy-preserving statistics to secure federated learning.
- There exists several cryptographic protocols realizing MPC under a variety of models. But they often come with high performance costs.

Homomorphic encryption

- Homomorphic Encryption (HE) enables computation to be performed on encrypted data, without requiring decryption. This enables private-data processing by untrusted entities and has important applications for outsourced architectures.
- In the last decade, the overhead of HE (w.r.t. plaintext computation) has been reduced from six down to three orders of magnitude. In coming hardware accelerators are expected to further close this gap in the next few years.
- HE provides a direct solution to the MPC problem for two parties.

The Lattigo library

✓ 100% written in Go, as fast as C++
✓ Cross-platform (Linux, Darwin, Windows, WASM, ...)
✓ Easy builds and dependency management
✓ Standalone optimized ring arithmetic layer
✓ Generic RLWE layer
✓ Complete HE scheme layer
✓ Encrypted integer-arithmetic (BGV [3])
✓ Encrypted scale-invariant integer-arithmetic (BFV [4])
✓ Encrypted complex/real arithmetic (CKKS [5,6])
✓ Parameterizable CKKS bootstrapping [7,8]
✓ Homomorphic evaluation of lookup tables
✓ Multiparty extensions layer
✓ Multiparty BFV, BGV and CKKS
✓ N-out-of-N-threshold [1]