CS576: Project Summary

Atharva Ranade

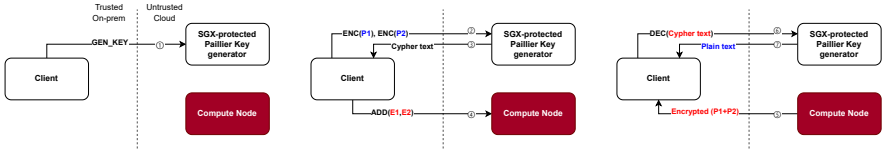
This project uses the opensgx emulator to demonstrate how an SGX enclave can be used as a "key factory" for FHE / PHE schemes.

1 Design and Implementation

SGX provides a restrictive programming environment. I choose Paillier cryptosystem, a simple PHE scheme that can be implemented without using any libraries.

The project has 3 components:

- SGX-server: A server that runs inside an SGX enclave with capability to generate keys, encrypt and decrypt data.
- non-SGX-server (normal server): A server that runs computations on the encrypted text.
- Client: A simple client that outsources the computation to the trusted sgx-server and the un-trusted non-sgx-server.



As shown in the figure, the non-SGX-server never sees the plain text.

2 Limitations

As I am using 64 bit integers, the primes that can be used are of limited size. For now, I have hard coded primes to be 13 and 17. These primes ensure that no step in the algorithm leads to an overflow.

Sometimes, the emulator crashes without any error message / debug information. If this happens, reboot the VM.

3 Changes from the proposal

Instead of using CKKS (via seal library), I implemented Paillier cryptosystem.