Evaluation of SEAL functions on Linux:

Parameters:

* poly\_modulus: 1x4096 + 1
* coeff\_modulus size: 109 bits
* plain\_modulus: 786433
* noise standard deviation: 3.19

|  |  |
| --- | --- |
| Key generation | 6872 microseconds |
| Encryption | 7516 microseconds |
| Decryption | 1926 microseconds |
| Addition (plain+cipher) | 140 microseconds |
| Addition (cipher+cipher) | 29 microseconds |
| Multiplication (plain+cipher) | 2291 microseconds |
| Multiplication (cipher+cipher) | 13150 microseconds |
| Secret key size | 120 |
| Public key size | 96 |
| Plain-text size | 56 |
| Ciphertext size | 96 |

Parameters:

* poly\_modulus: 1x8192 + 1
* coeff\_modulus size: 218 bits
* plain\_modulus: 786433
* noise standard deviation: 3.19

|  |  |
| --- | --- |
| Key generation | 37827 microseconds |
| Encryption | 14863 microseconds |
| Decryption | 3599 microseconds |
| Addition (plain+cipher) | 398 microseconds |
| Addition (cipher+cipher) | 96 microseconds |
| Multiplication (plain+cipher) | 8675 microseconds |
| Multiplication (cipher+cipher) | 60759 microseconds |
| Secret key size | 120 |
| Public key size | 96 |
| Plain-text size | 56 |
| Ciphertext size | 96 |