A flexible and polynomial framework for integer arithmetic in CKKS

Lorenzo Rovida

Abstract: A new paradigm, called discrete-CKKS, proposes to restrict the plaintext space of the homomorphic encryption CKKS scheme from C to a discrete subset of it (e.g., 0, 1). While sacrificing approximate computations, this allows one to express an arithmetic similar to that available in exact schemes, but with significantly larger parallelism and flexibility due to SIMD computations and the underlying complex arithmetic, which remains available internally. A significant example is the recent work by Boneh and Kim [Crypto '25], where they present a method to operate on extremely large encrypted integers. In this work, we build a simple computational device that handles integers, decomposed as binary vectors, by evaluating standard mod 2 arithmetic operations using polynomials only. Since we do not resort to the modular reductions based on the functional bootstrapping proposed by Kim and Noh [CIC '25], this yields a more flexible parameterization, consistent with standard CKKS configurations, e.g., leveled supporting roughly 15 multiplicative levels before bootstrapping. This means that one can use CKKS in R and then switch to Z with the same set of parameters – we will refer to this as domain-switching. Experiments show that our solution has lower latency on all operations (i.e., additions, multiplications, comparisons and logical shifts) with respect to the current state of the art, although the throughput is smaller due to how data is represented.