Generalized splitting-ring number theoretic transform

August 28 2024

Credit: AI-generated image

Number theoretic transform (NTT) is widely recognized as the most efficient method for computing polynomial multiplication with high dimension and integral coefficients, due to its quasilinear complexity.

What is the relationship between the NTT variants that are constructed

by splitting the original polynomials into groups of lower-degree sub-polynomials, such as K-NTT, H-NTT, and G3-NTT? Can they be seen as special cases of a certain algorithm under different parameterizations?

To solve the problems, a research team led by Yunlei Zhao published new research on 15 August 2024 in *Frontiers of Computer Science*.

The team proposed the first Generalized Splitting-Ring Number Theoretic Transform, referred to as GSR-NTT. Then, they investigated the relationship between K-NTT, H-NTT, and G3-NTT.

In the research, they investigate generalized splitting-ring polynomial multiplication based on the monic incremental polynomial variety, and they propose the first Generalized Splitting-Ring Number Theoretic Transform, referred to as GSR-NTT. They demonstrate that K-NTT, H-NTT, and G3-NTT can be regarded as special cases of GSR-NTT under different parameterizations.

They introduce a succinct methodology for complexity analysis, based on which GSR-NTT can derive its optimal parameter settings. They provide GSR-NTT other instantiations based on cyclic convolution-based polynomials and power-of-three cyclotomic polynomials.

They apply GSR-NTT to accelerate polynomial multiplication in the lattice-based scheme named NTTRU and single polynomial multiplication over power-of-three cyclotomic polynomial rings. The experimental results show that, for NTTRU, GSR-NTT achieves speed-ups of 24.7%, 37.6%, and 28.9% for the key generation, encapsulation, and decapsulation algorithms, respectively, leading to a total speed-up of 29.4%.

Future work can focus on implementing GSR-NTT on more platforms.

More information: Zhichuang Liang et al, Generalized splitting-ring number theoretic transform, *Frontiers of Computer Science* (2024). DOI: 10.1007/s11704-024-3288-9

Provided by Frontiers Journals