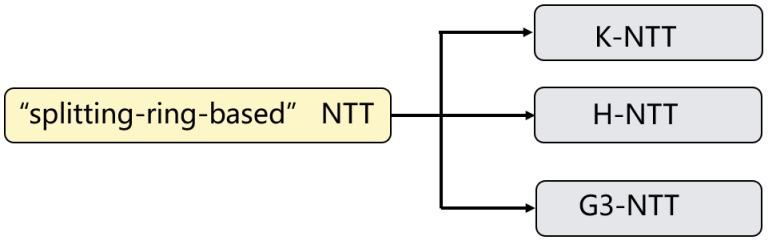
Generalized Splitting-Ring Number Theoretic Transform

Zhichuang LIANG, Yunlei ZHAO, Zhenfeng ZHANG

Frontiers of Computer Science, DOI: 10.1007/s11704-024-3288-9

Problems & Ideas

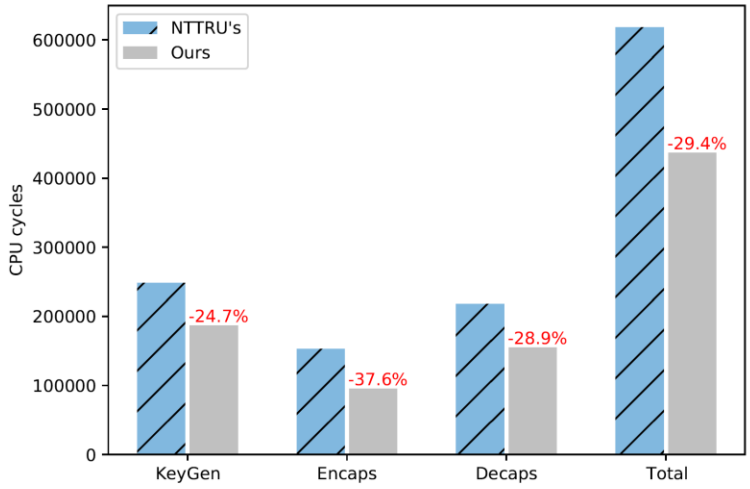
- Problems:
  - What is the relationship between the NTT variants that are constructed by splitting the original polynomials into groups of lower-degree sub-polynomials, such as K-NTT, H-NTT, and G3-NTT? Can they be seen as special cases of a certain algorithm under different parameterizations?
- Ideas: This raises the question of whether K-NTT, H-NTT, and G3-NTT can be considered as special cases of a more general algorithm that encompasses all such “splitting-ring-based” NTT algorithms. We propose the first Generalized Splitting-Ring Number Theoretic Transform.



Relationship between K-NTT, H-NTT, and G3-NTT.

Main Contributions

- Contributions:
  - We propose the first Generalized Splitting-Ring Number Theoretic Transform, referred to as GSR-NTT. We demonstrate that K-NTT, H-NTT, and G3-NTT can be regarded as special cases of GSR-NTT under different parameterizations;
  - We introduce a succinct methodology for complexity analysis;
  - We apply our GSR-NTT to accelerate polynomial multiplication in the lattice-based scheme and single polynomial multiplication.



Comparison between original NTT algorithm of NTTRU and our GSR-NTT for KEM schemes. Our 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%.