

enc/dec				
RLWE CPAKEM				
sample			polynomial arithmetics	
zero center	hwt	discrete Gaussian	poly-mpi & poly-rns	
random number generator (rng)			ntt	
			Montgomery	Barrett
			thread	