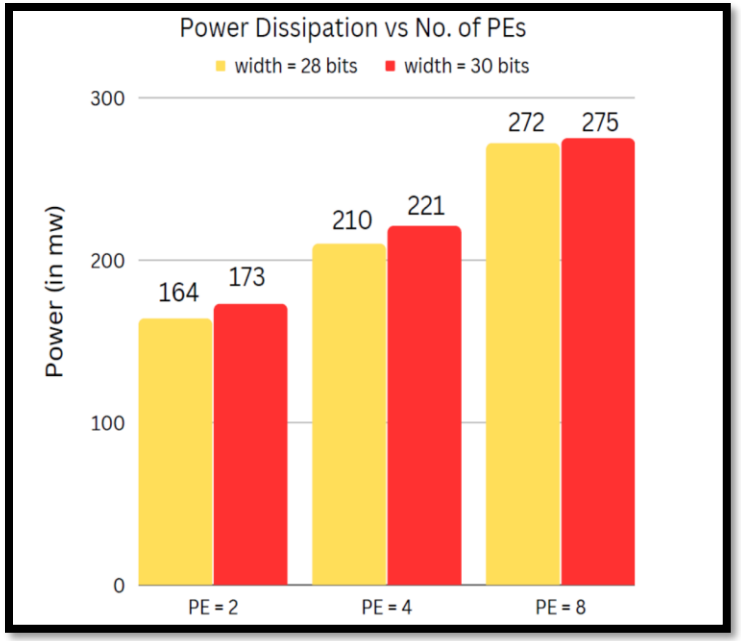
Optimization of Parametric NTT Hardware Accelerator

Aman Prajapati [MT2022501] [Aman.Prajapati@iiitb.ac.in]

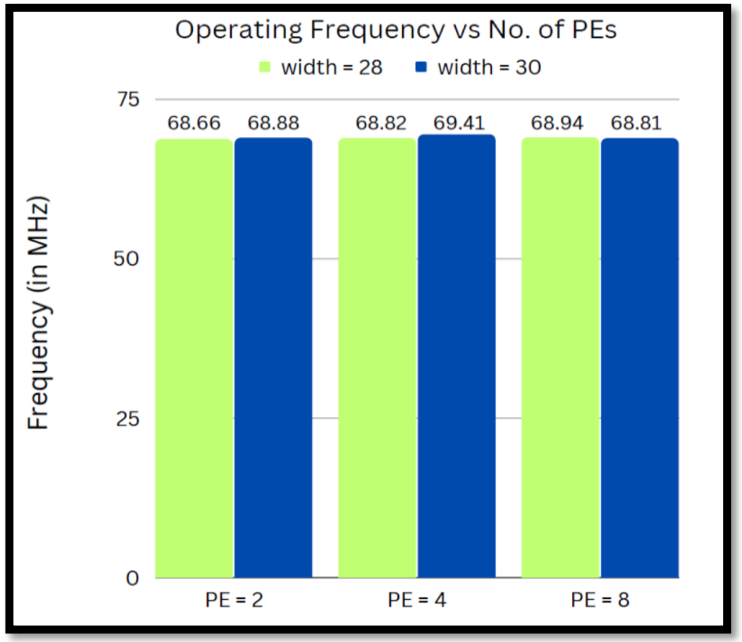
Lokesh Maji [MT2022509] [Lokesh.Maji@iiitb.ac.in]

FPGA IMPLEMENTATION OF PARAMETRIC NTT HARDWARE ACCELERATOR

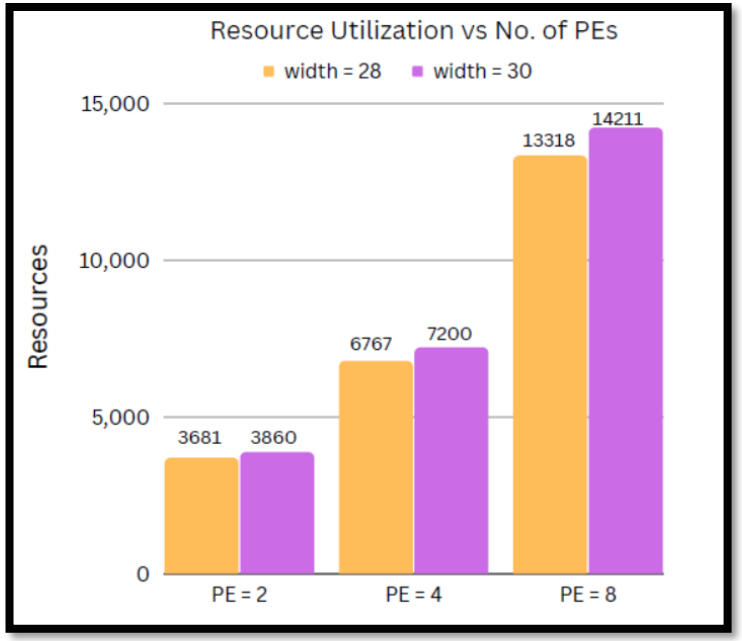
Conventional Algorithm



Power Analysis



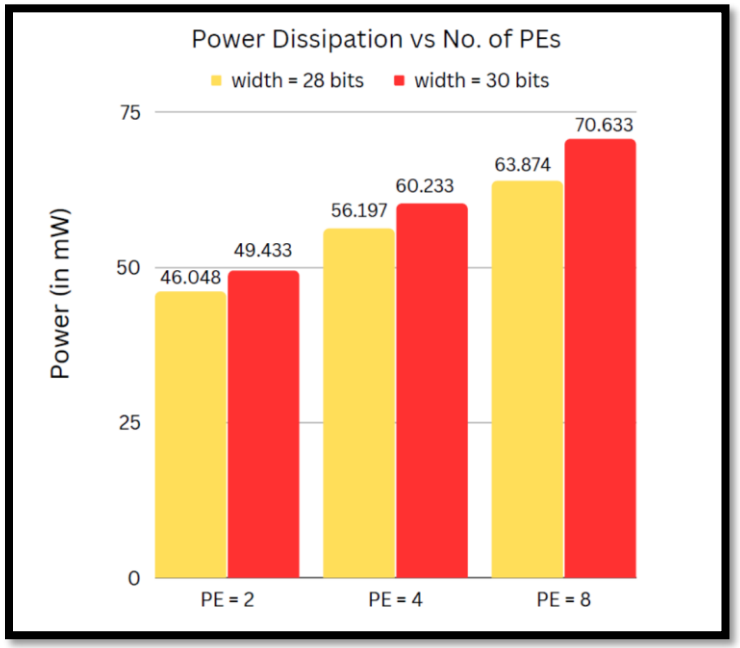
Performance Analysis



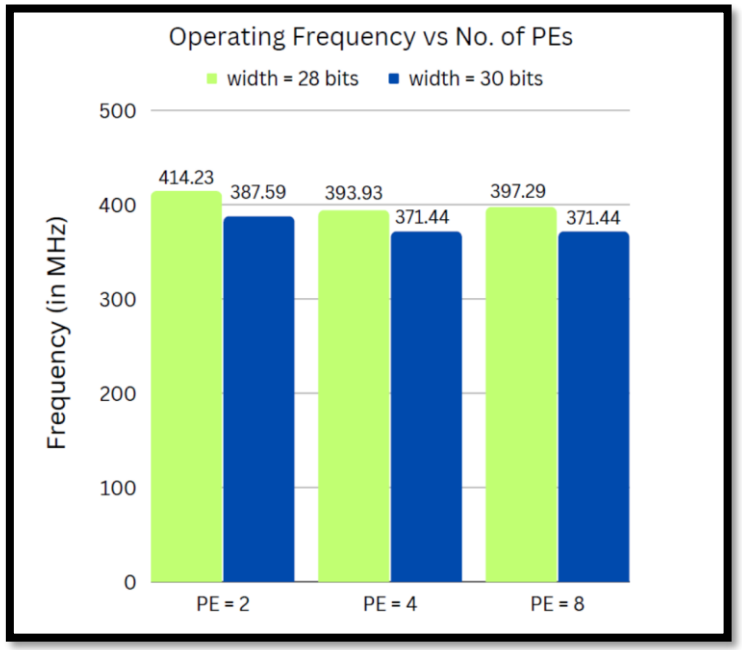
Area Analysis

ASIC IMPLEMENTATION OF PARAMETRIC NTT HARDWARE ACCELERATOR

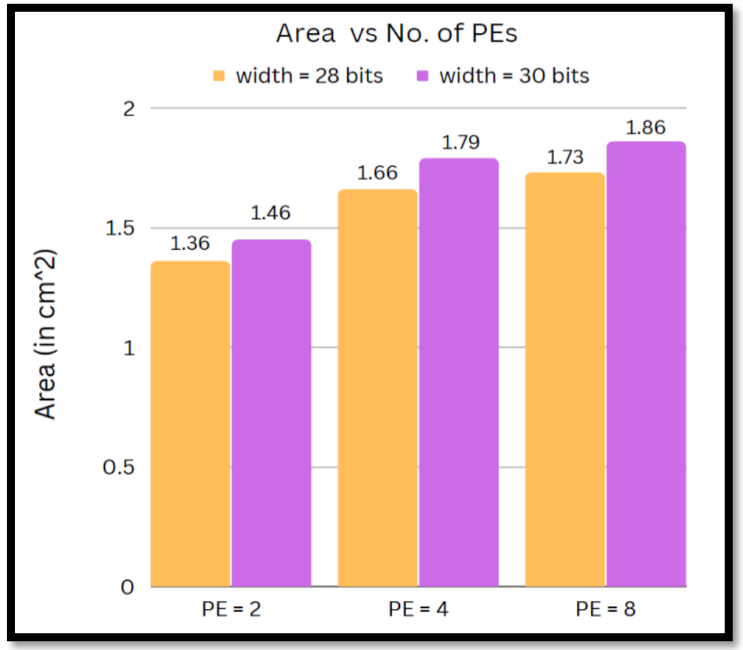
Conventional Algorithm



Power Analysis

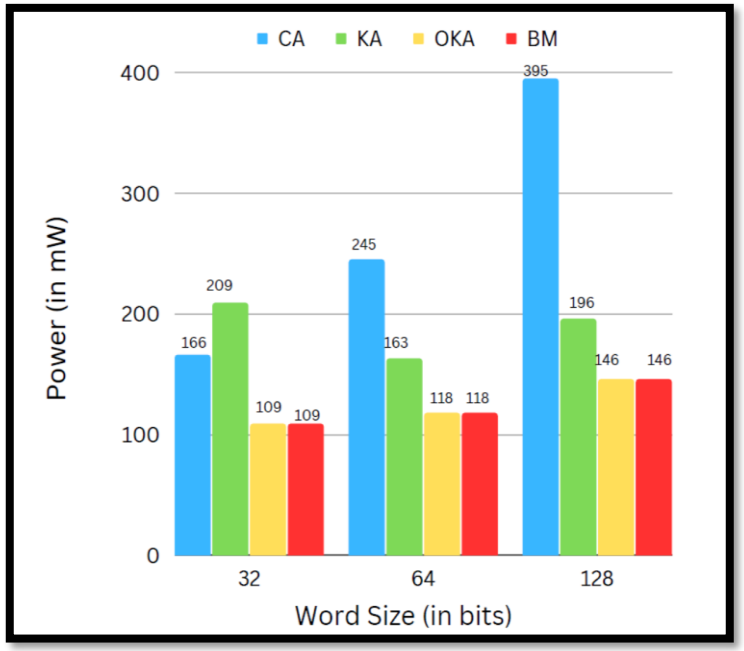


Performance Analysis

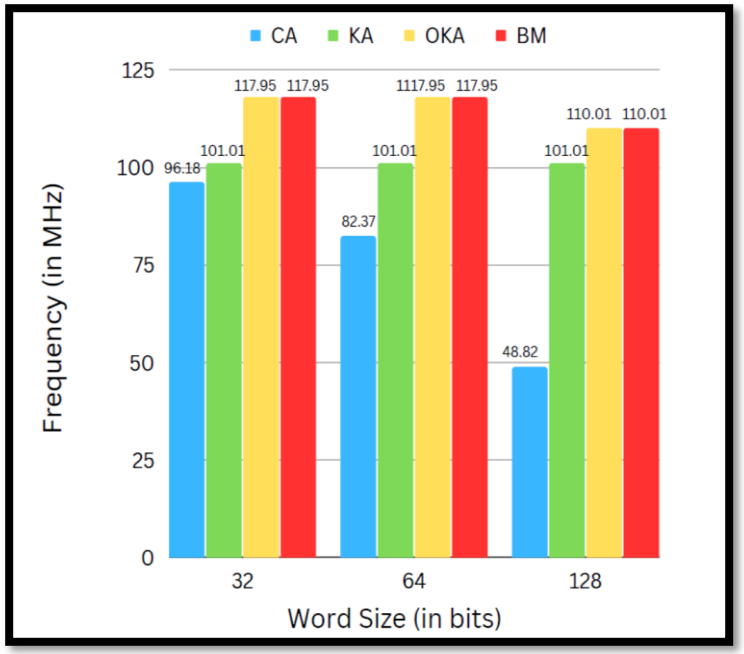


Area Analysis

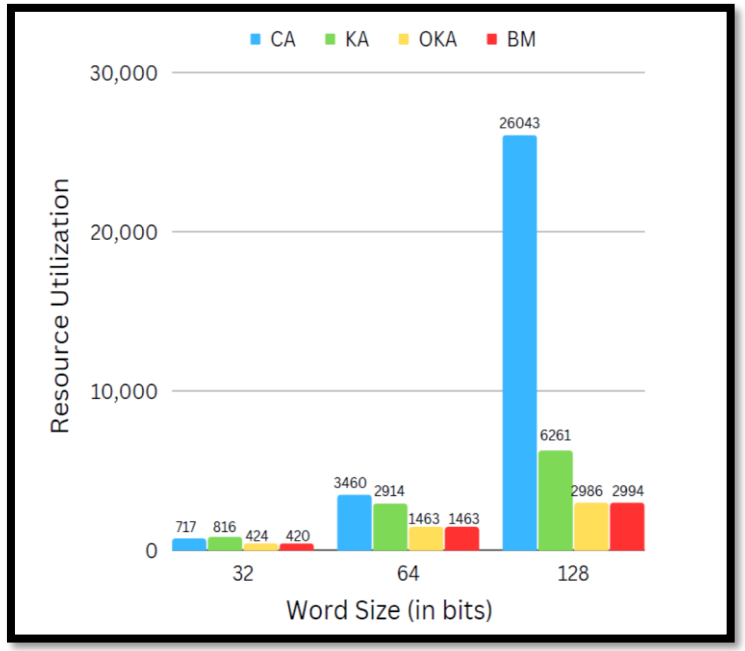
FPGA SYNTHESIS OF MODULUS MULTIPLICATION BLOCK OF PARAMETRIC NTT HARDWARE ACCELERATOR



Power Analysis

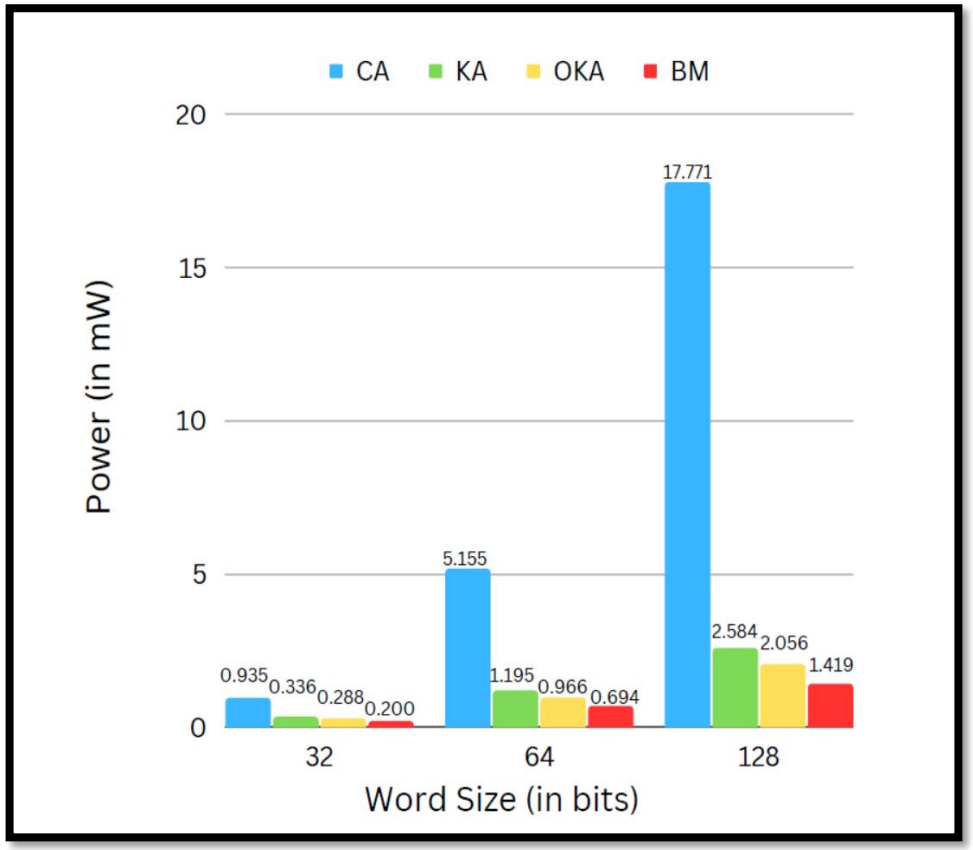


Performance Analysis

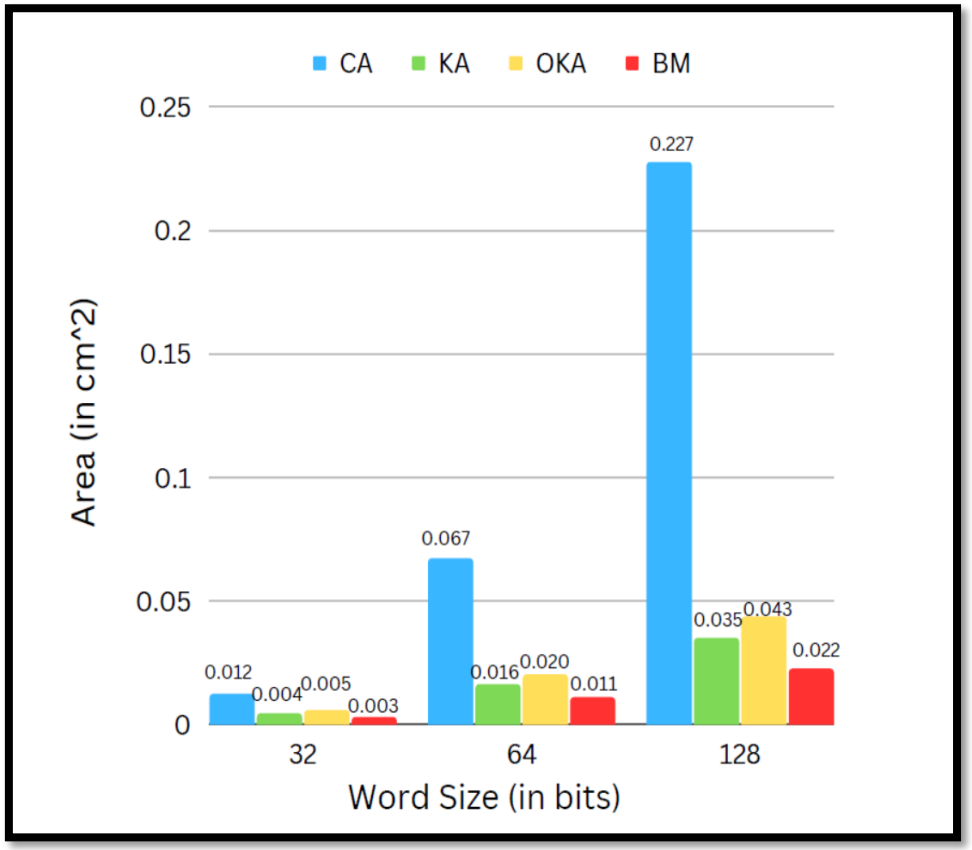


Area Analysis

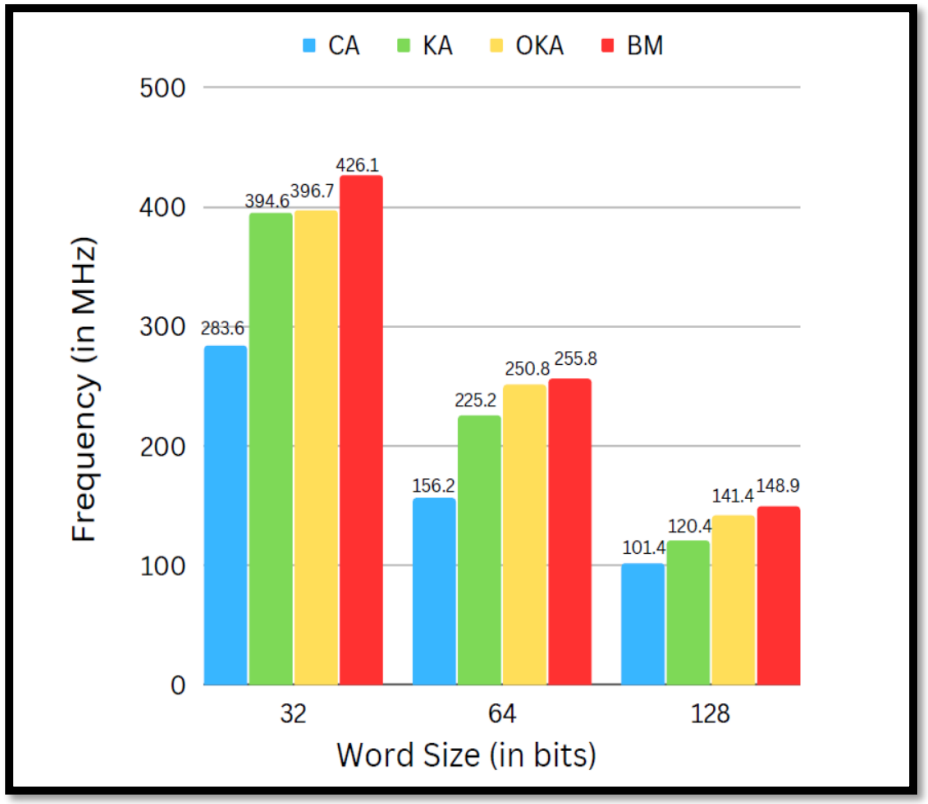
ASIC SYNTHESIS OF MODULUS MULTIPLICATION BLOCK OF PARAMETRIC NTT HARDWARE ACCELERATOR



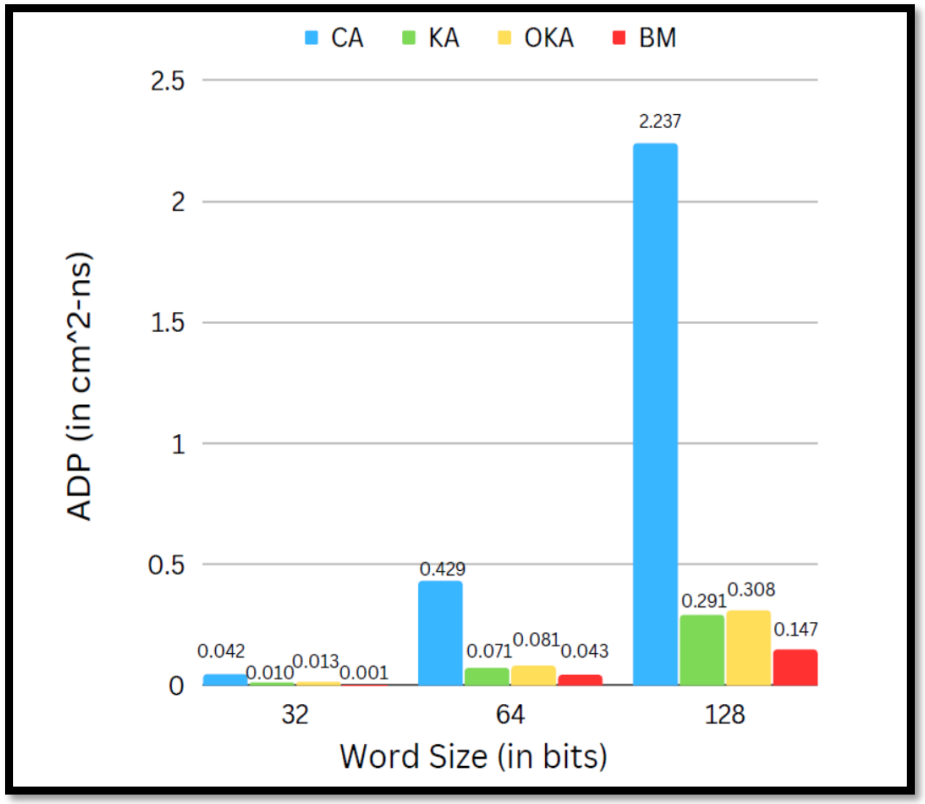
Power Analysis



Area Analysis

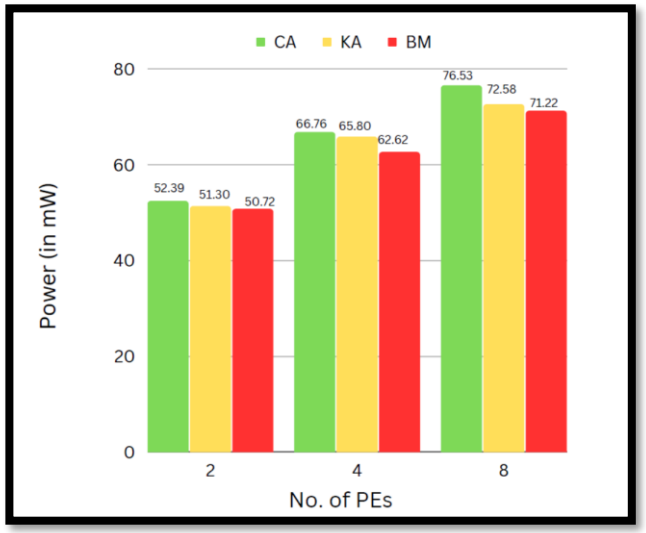


Performance Analysis

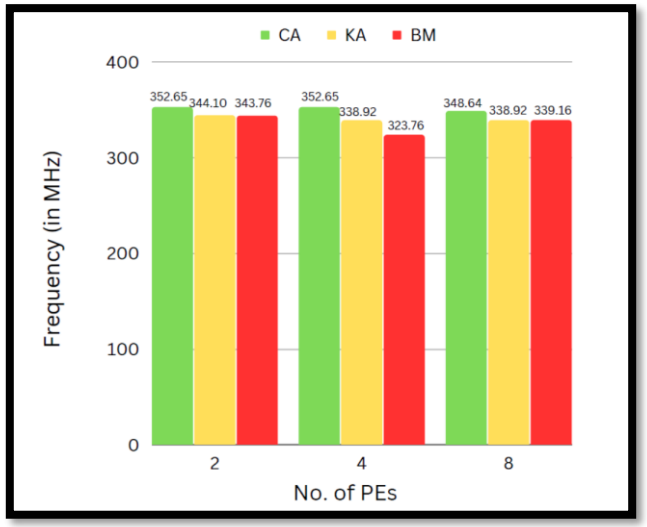


ADP Analysis

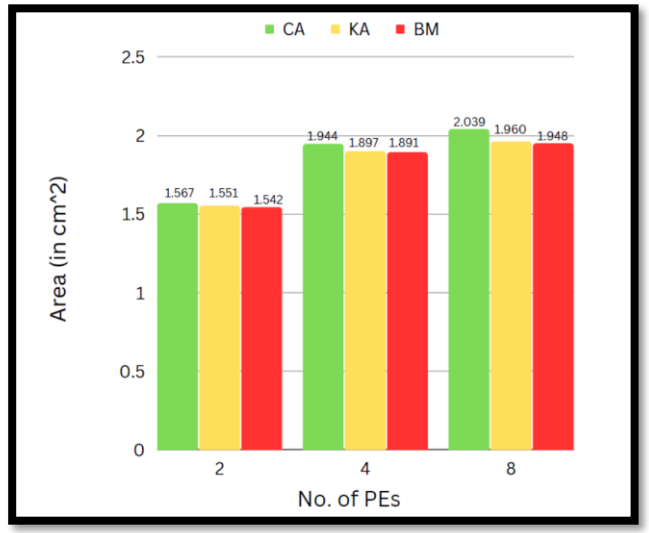
ASIC SYNTHESIS OF PARAMETRIC NTT HARDWARE ACCELERATOR USING CONVENTIONAL ALGORITHM, KARATSUBA ALGORITHM AND BOOTH MULTIPLIER RADIX-4 ALGORITHM



Power Analysis



Performance Analysis



Area Analysis