

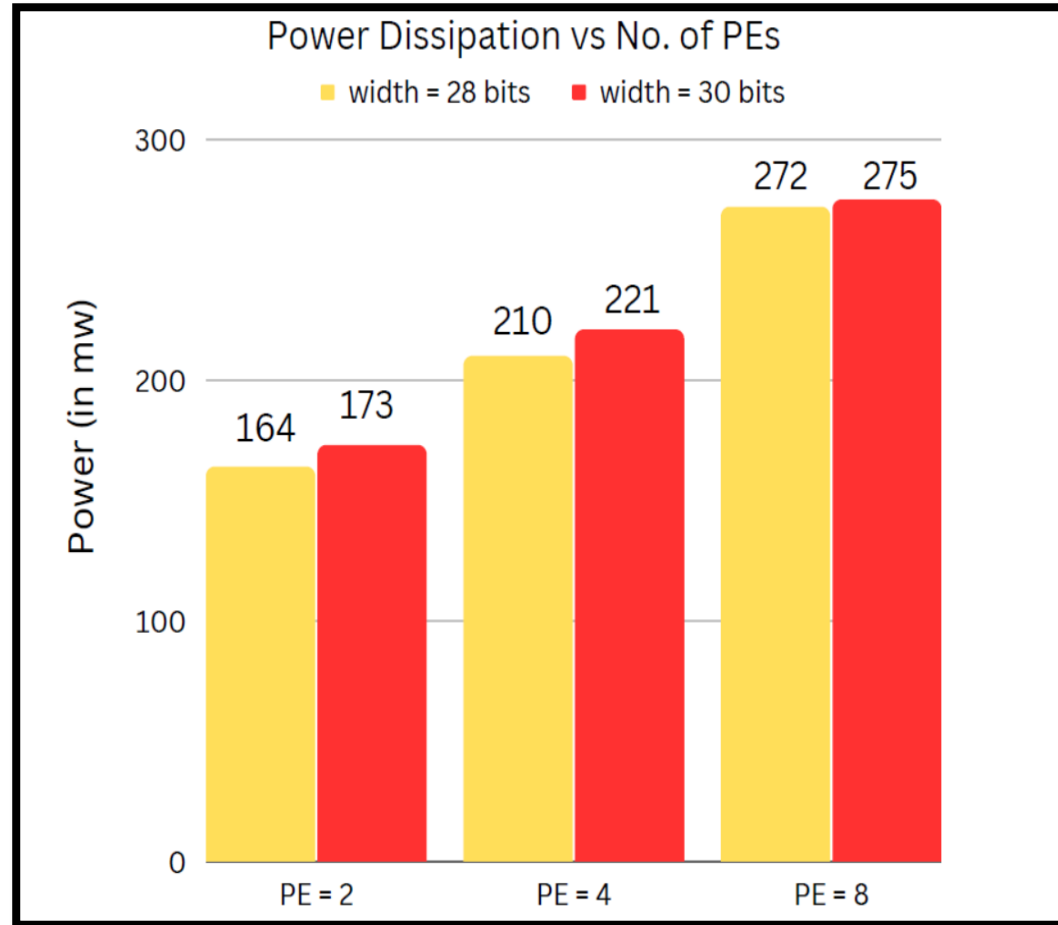
Optimization of Parametric NTT Hardware Accelerator

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

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

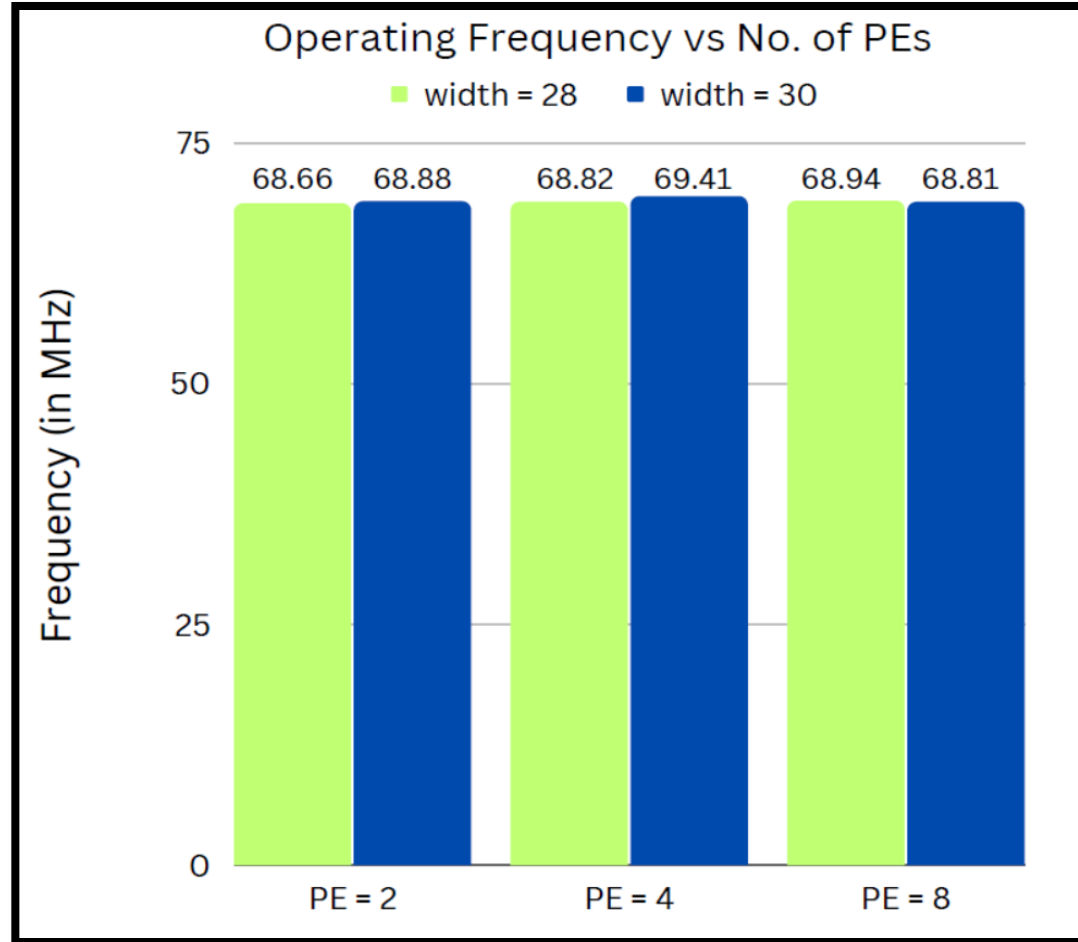
FPGA IMPLEMENTATION OF PARAMETRIC NTT HARDWARE ACCELERATOR

Conventional Algorithm



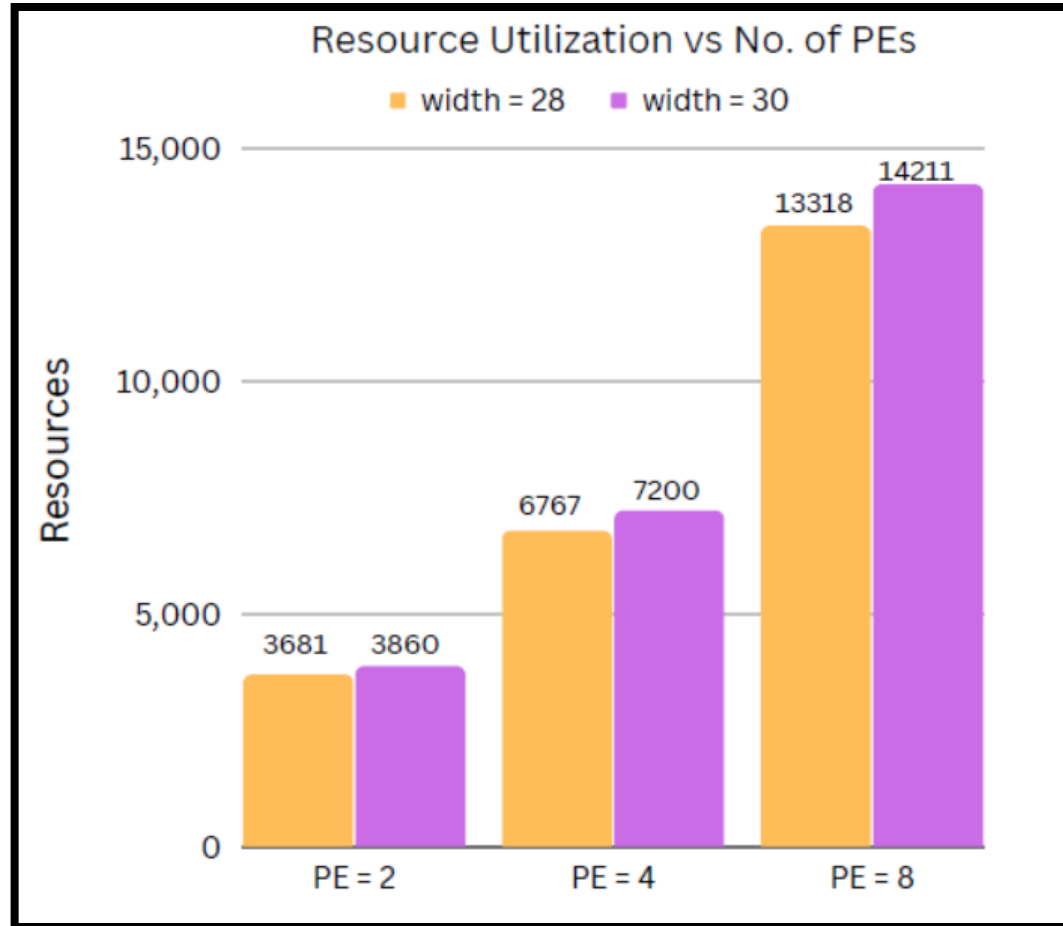
Power Analysis

Conventional Algorithm



Performance Analysis

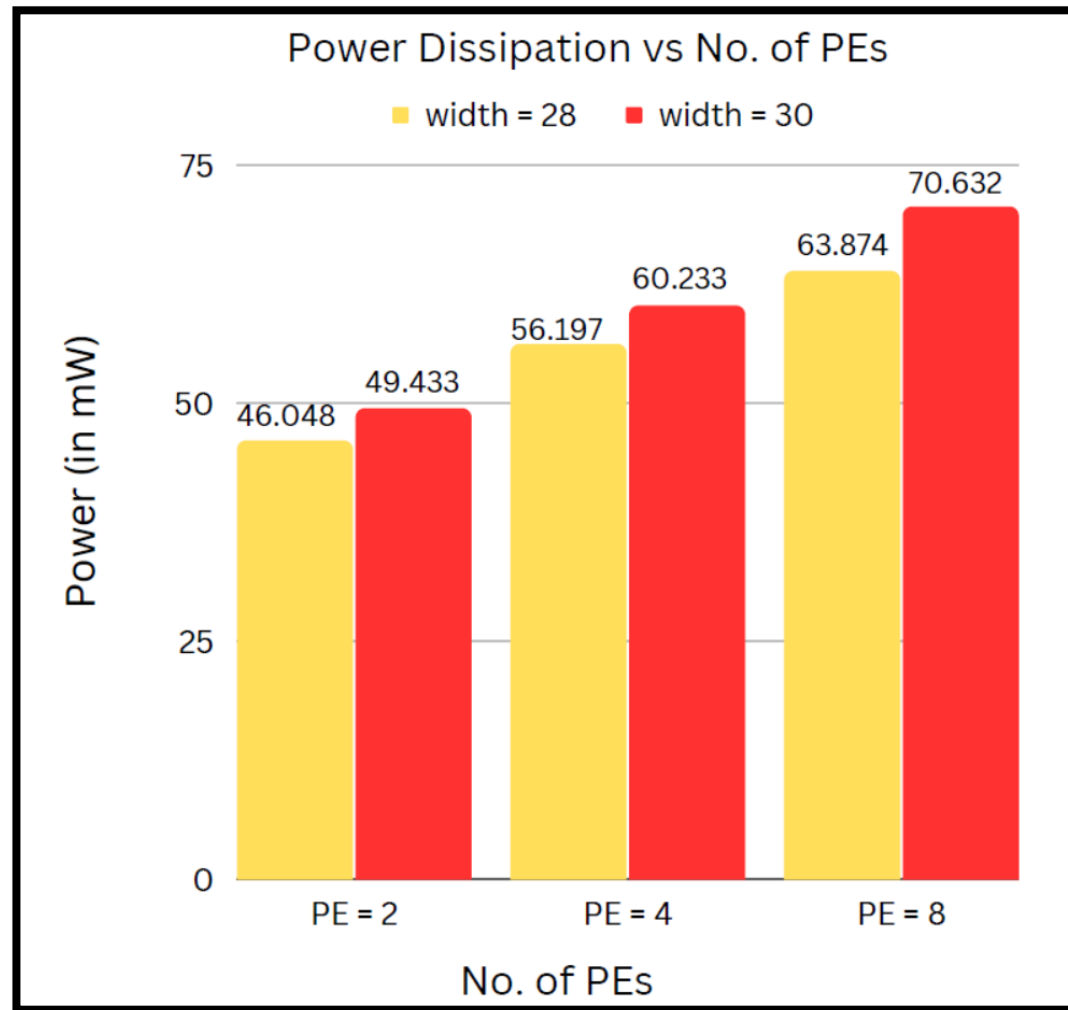
Conventional Algorithm



Area Analysis

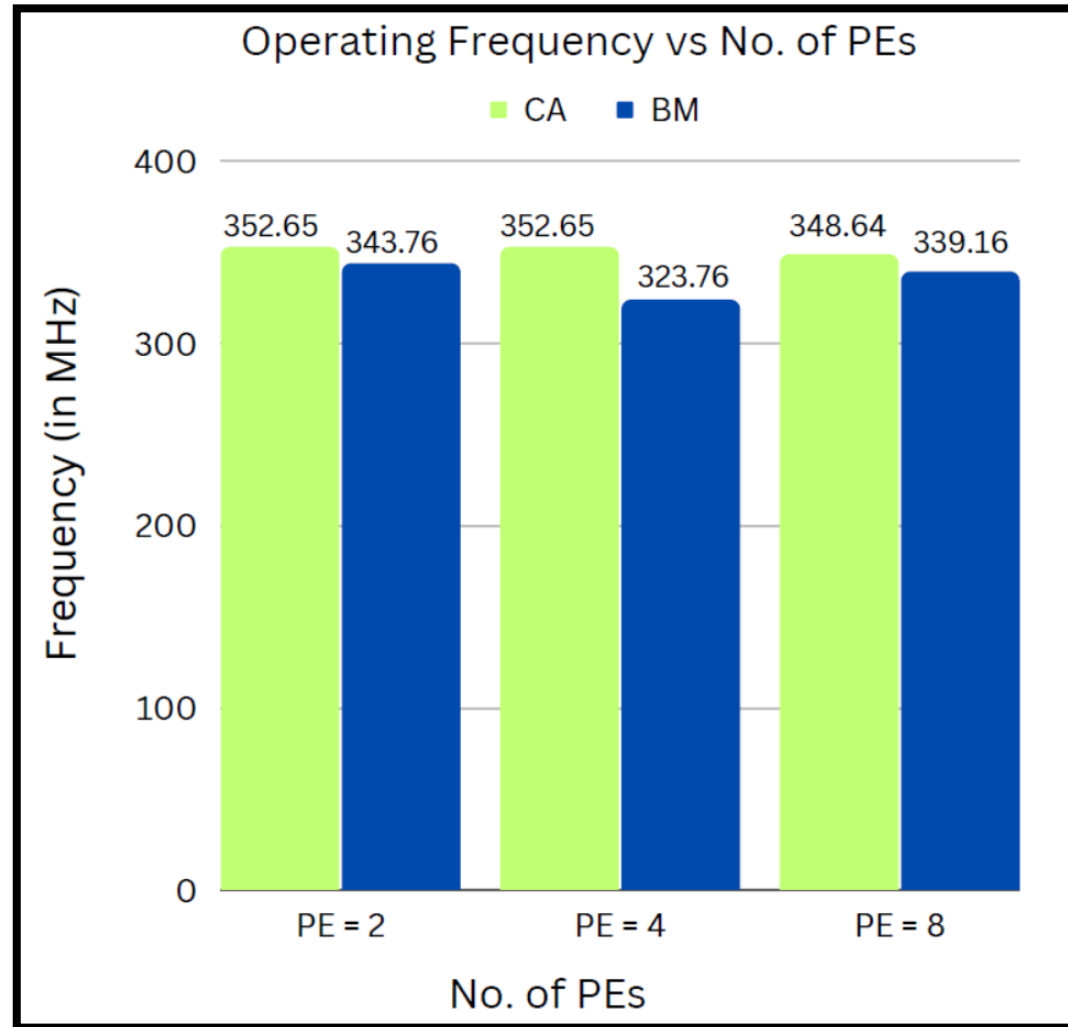
ASIC SYNTHESIS OF PARAMETRIC NTT HARDWARE ACCELERATOR

Conventional Algorithm



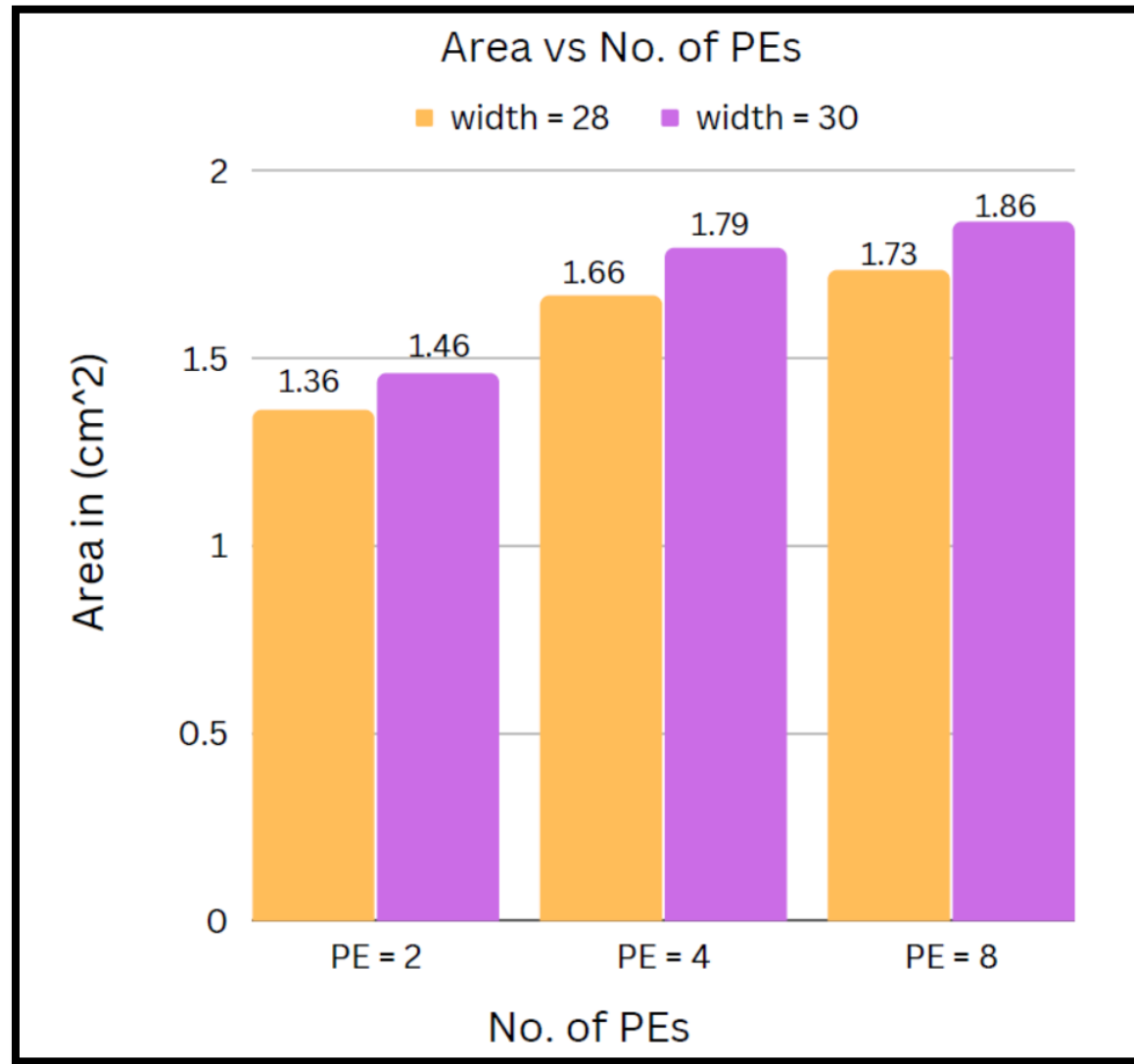
Power Analysis

Conventional Algorithm



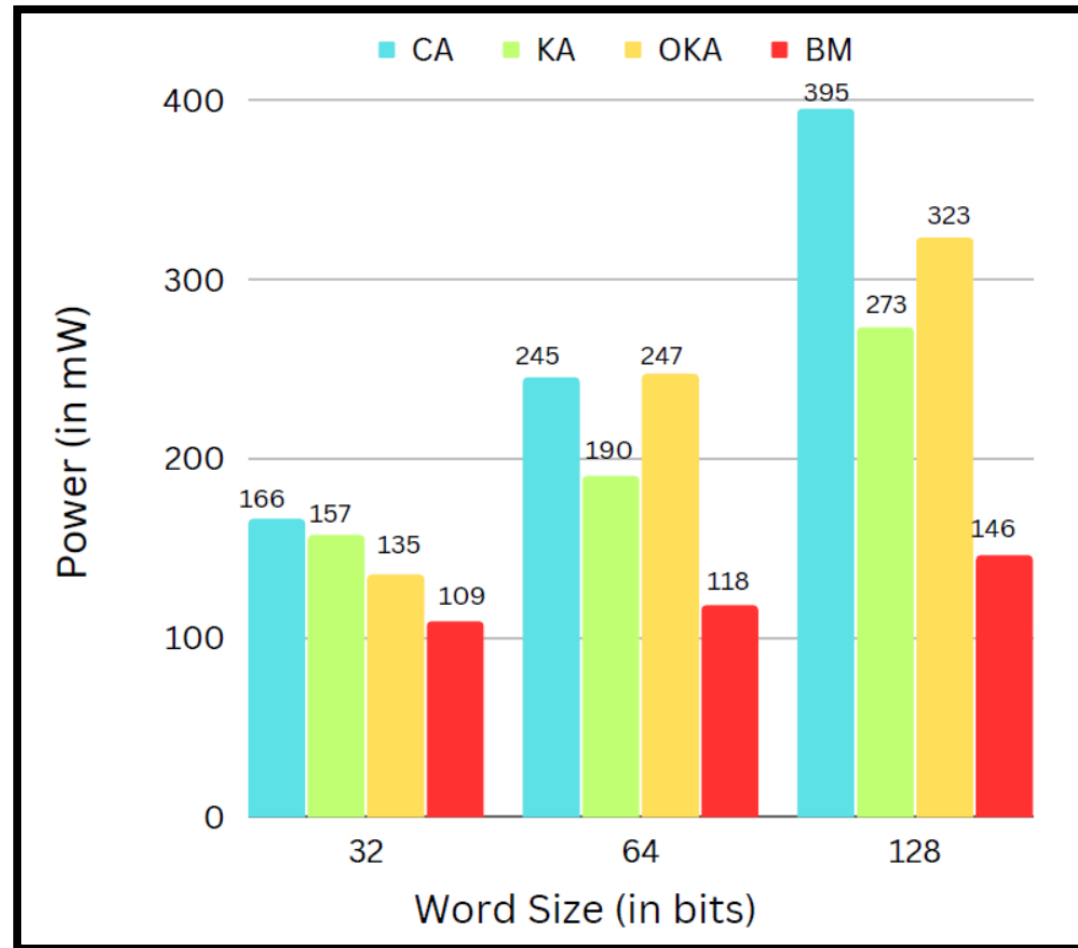
Performance Analysis

Conventional Algorithm

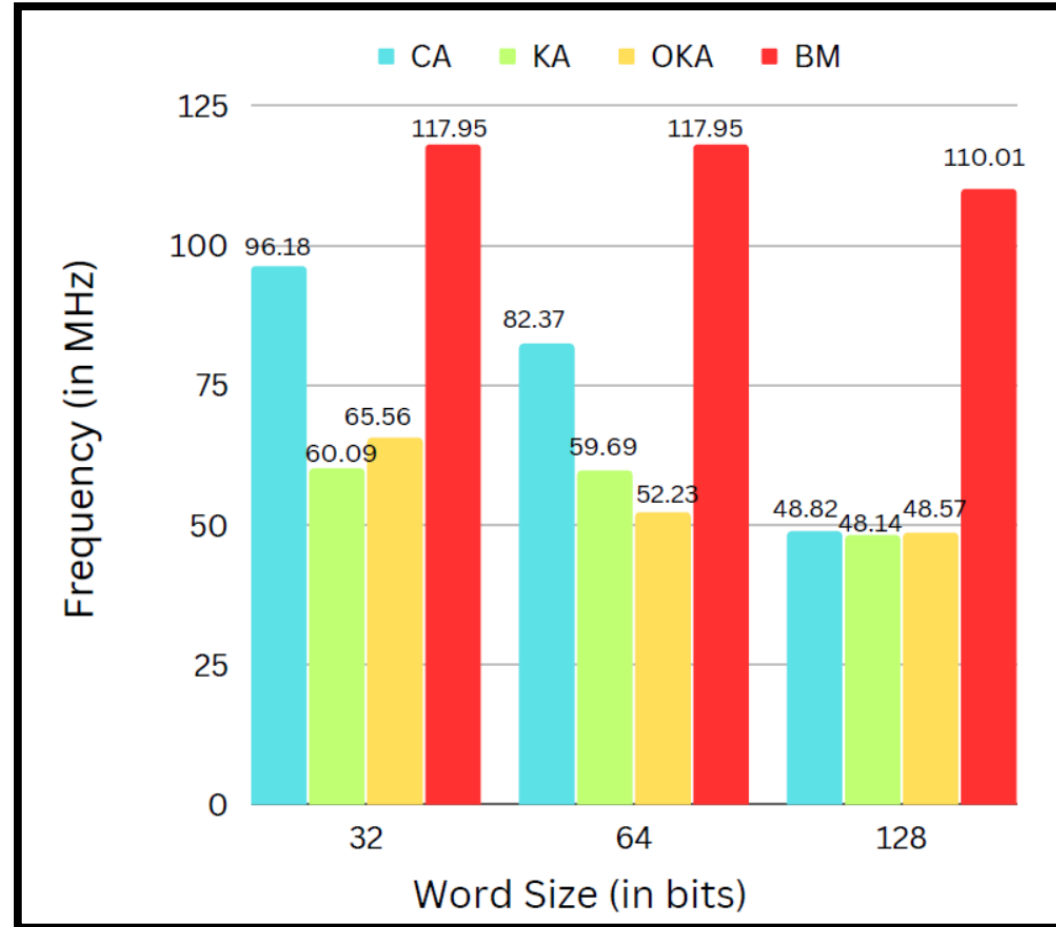


Area Analysis

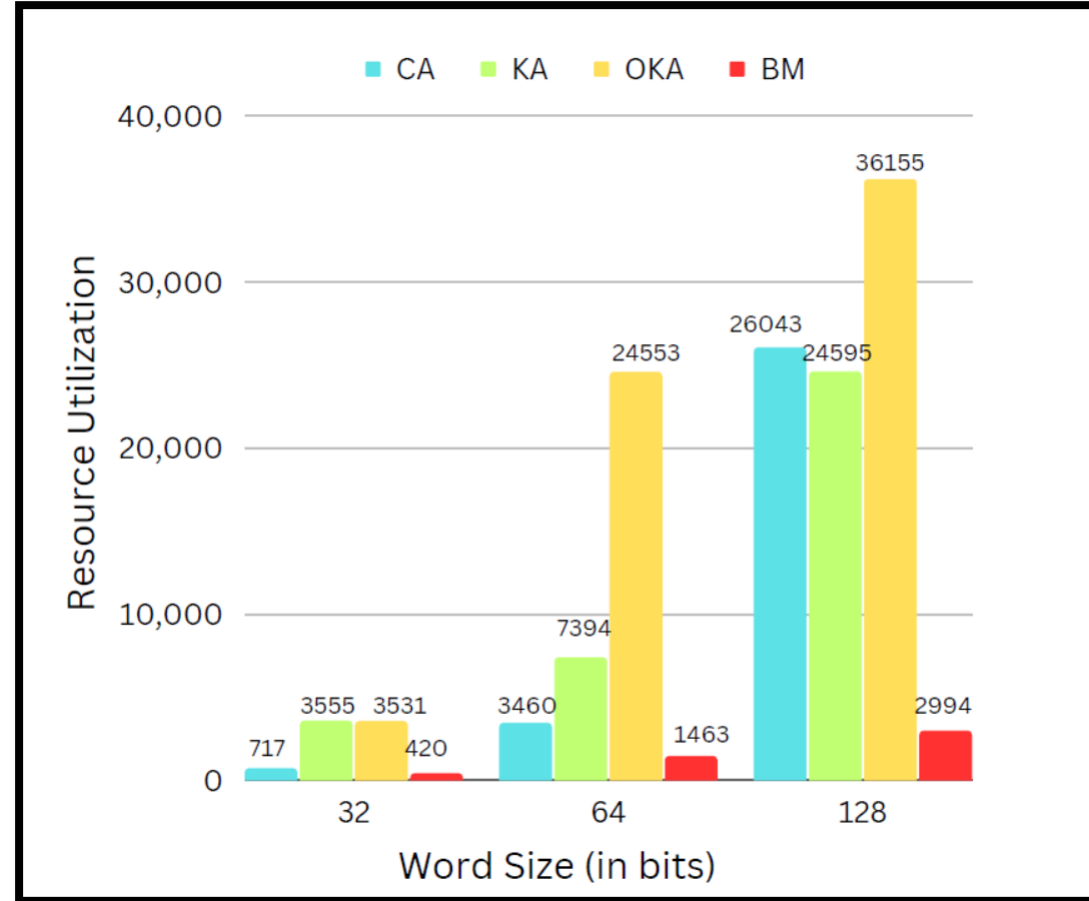
FPGA SYNTHESIS OF MODULUS REDUCTION BLOCK OF PARAMETRIC NTT HARDWARE ACCELERATOR



Power Analysis

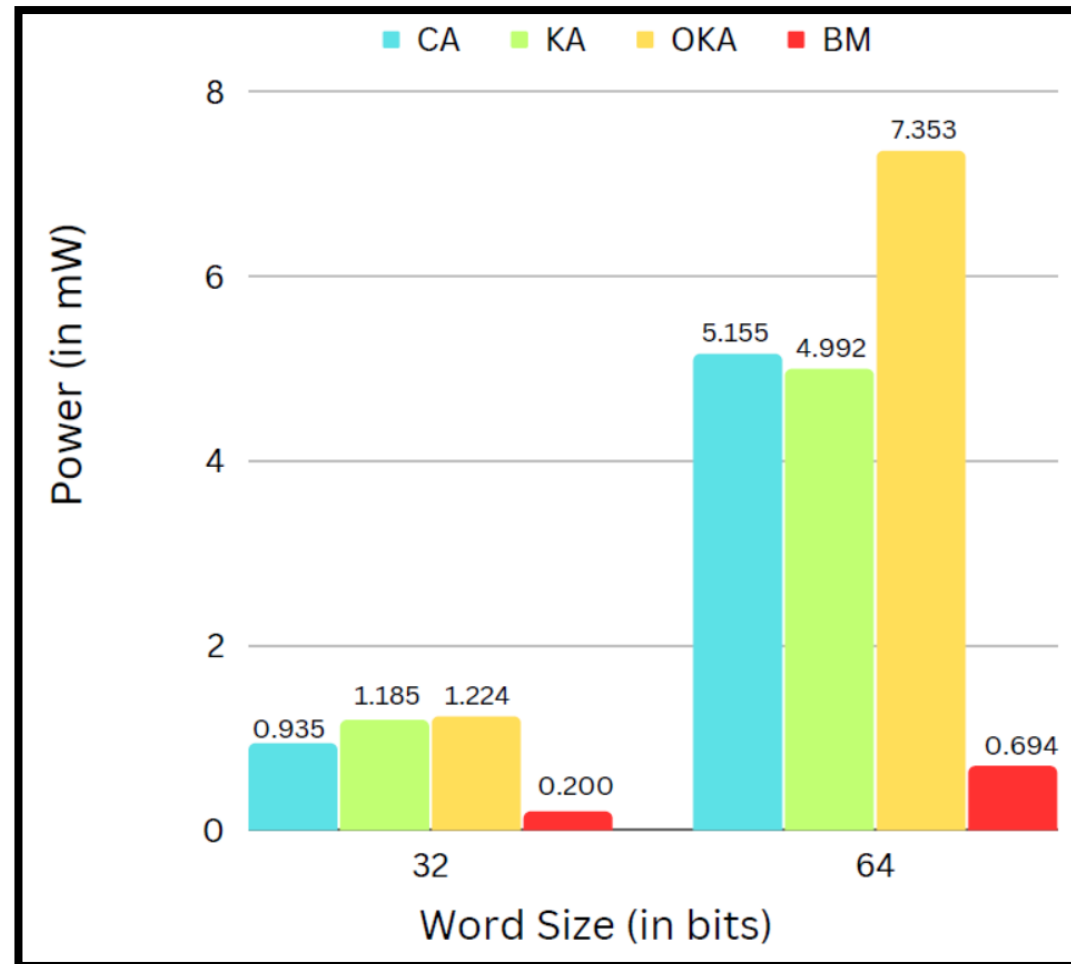


Performance Analysis

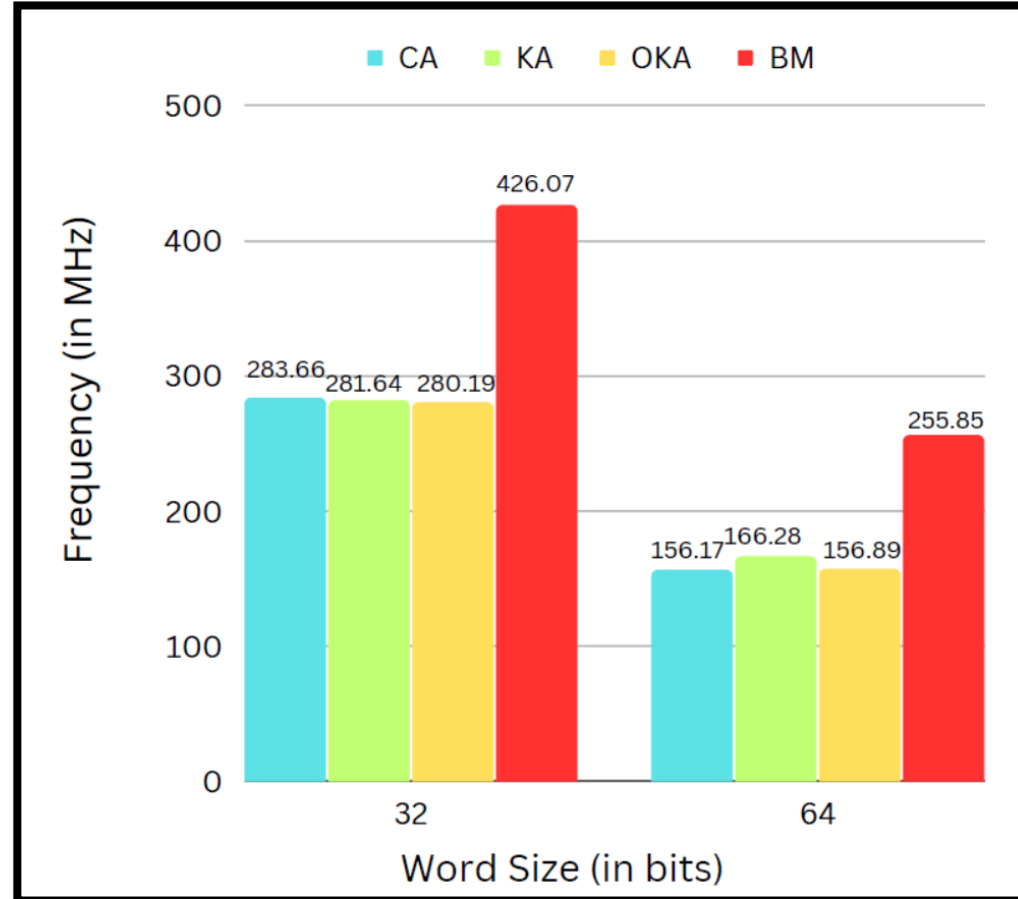


Area Analysis

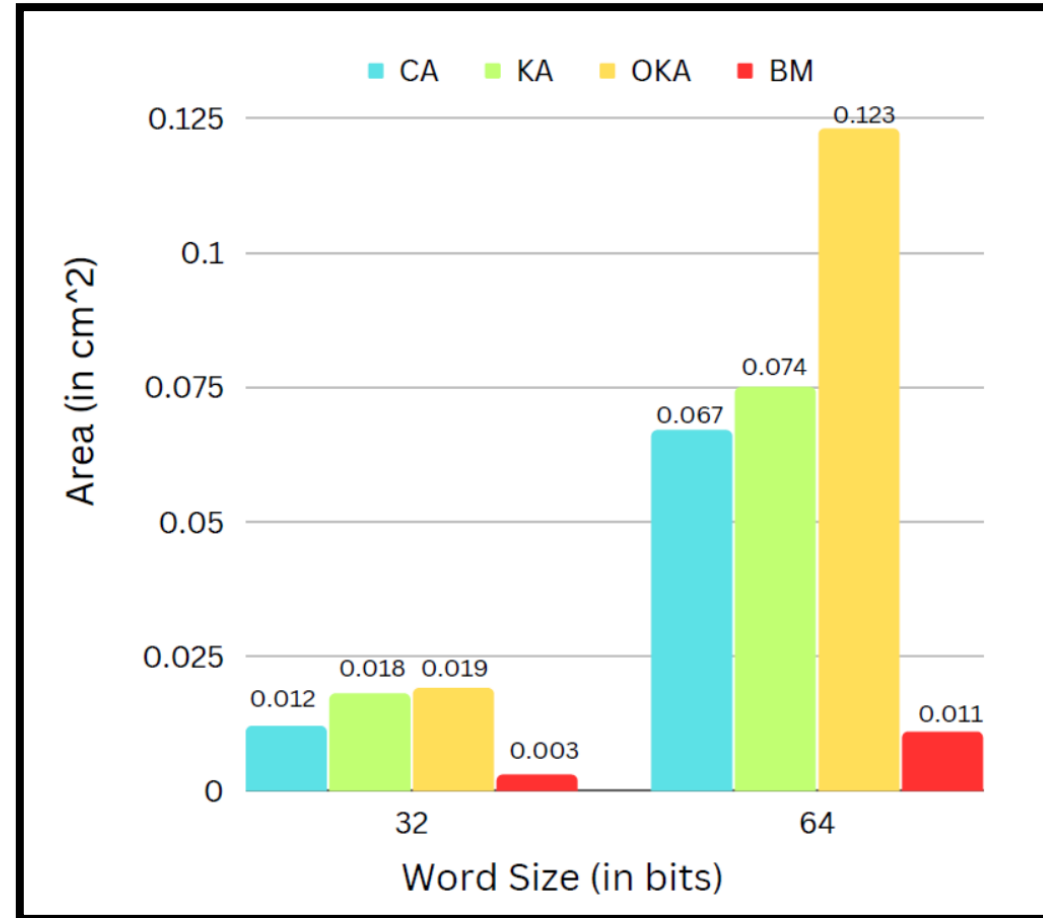
ASIC SYNTHESIS OF MODULUS REDUCTION BLOCK OF PARAMETRIC NTT HARDWARE ACCELERATOR



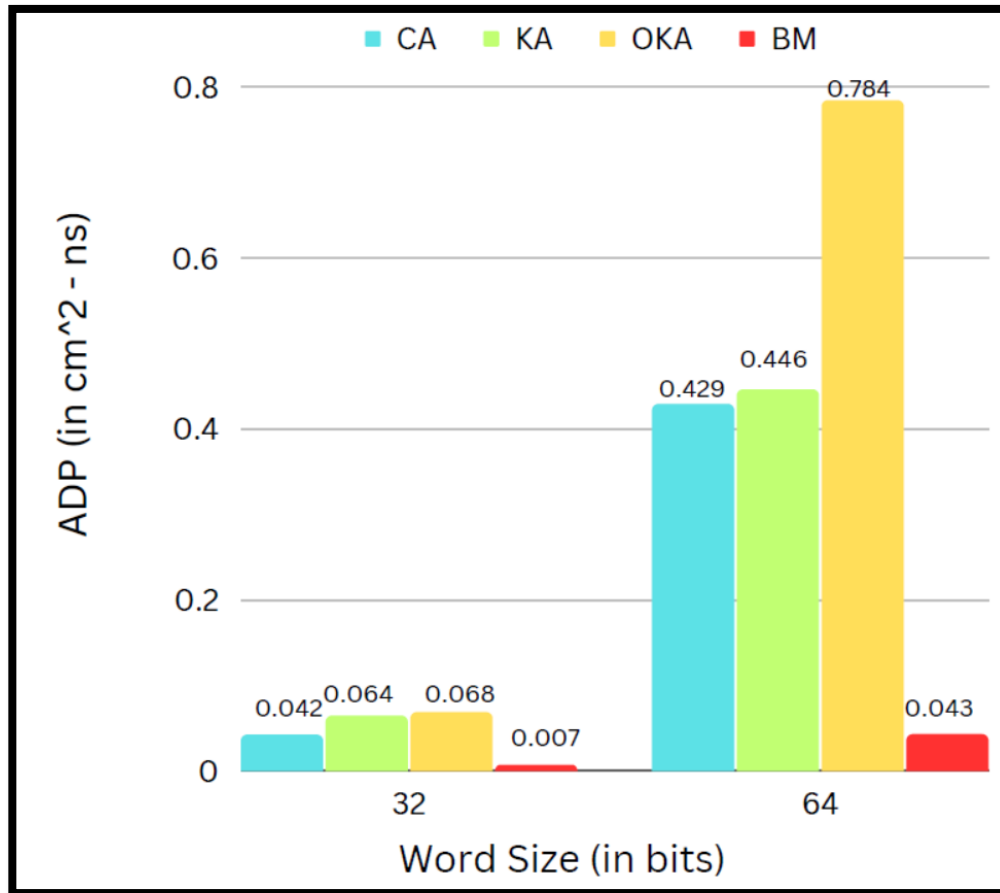
Power Analysis



Performance Analysis



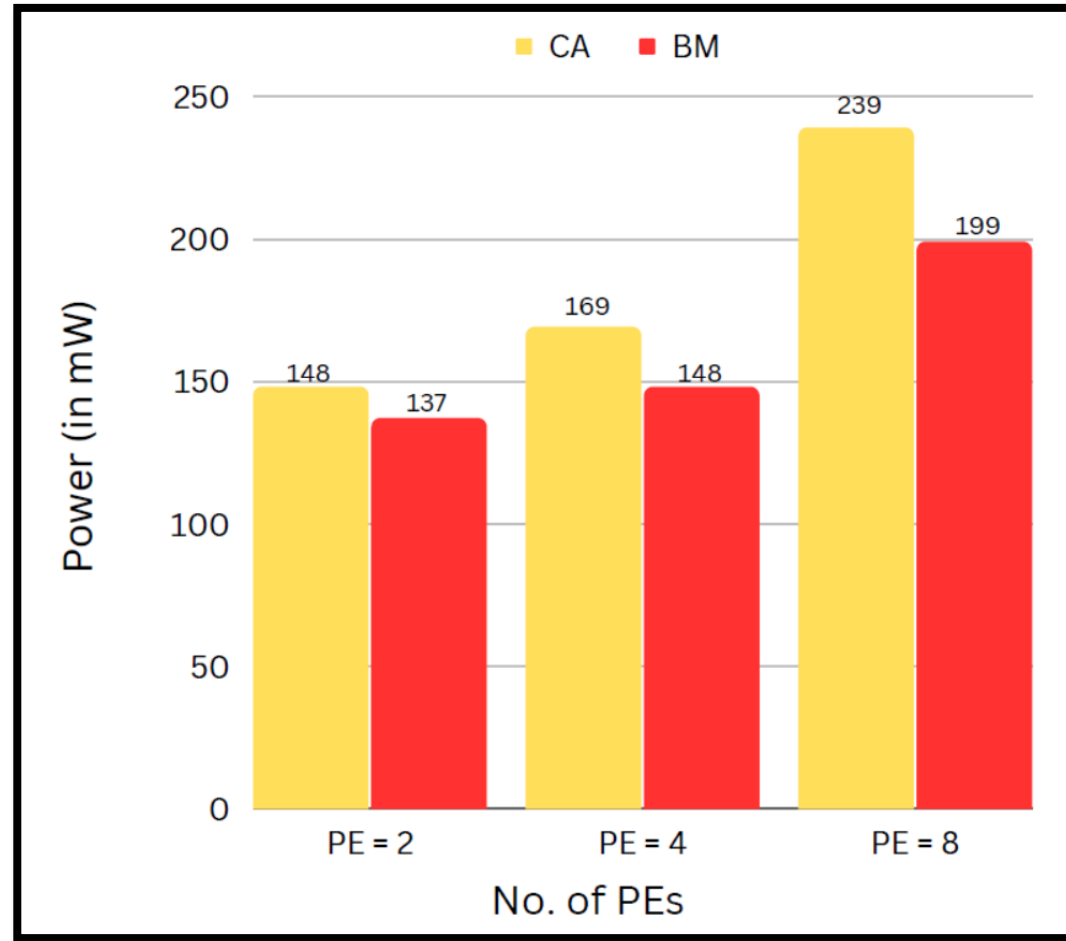
Area Analysis



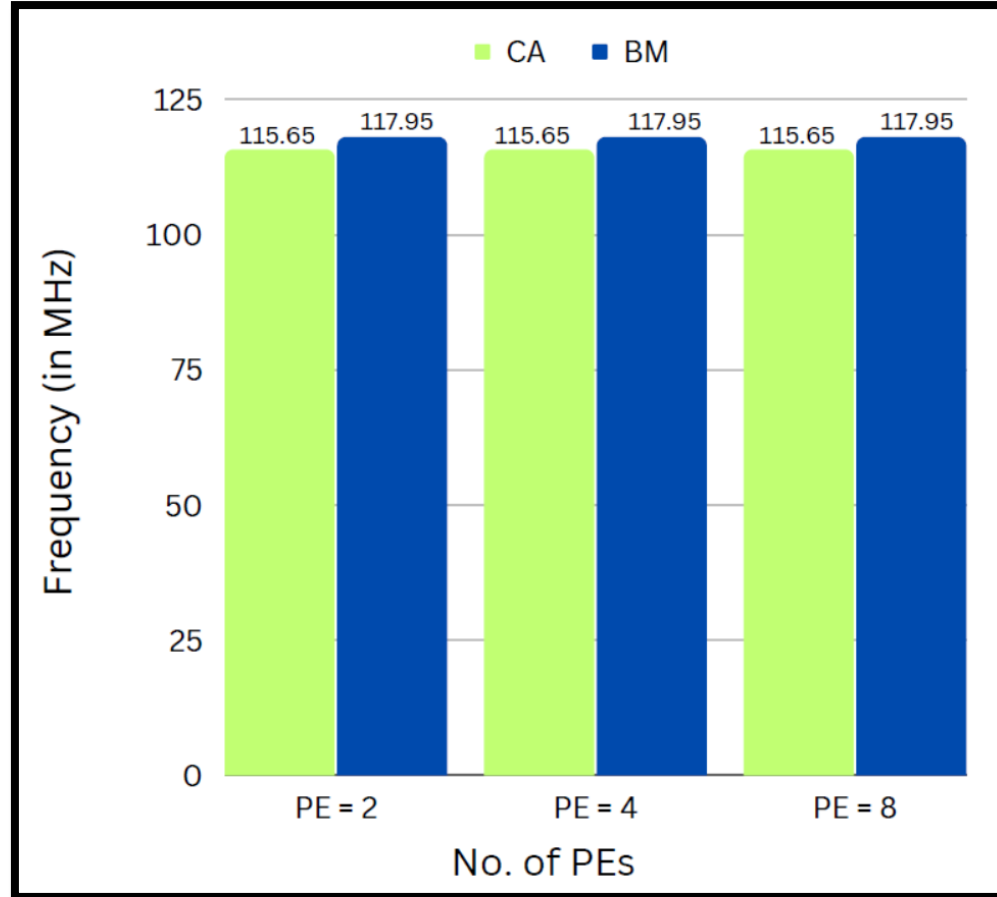
ADP Analysis

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

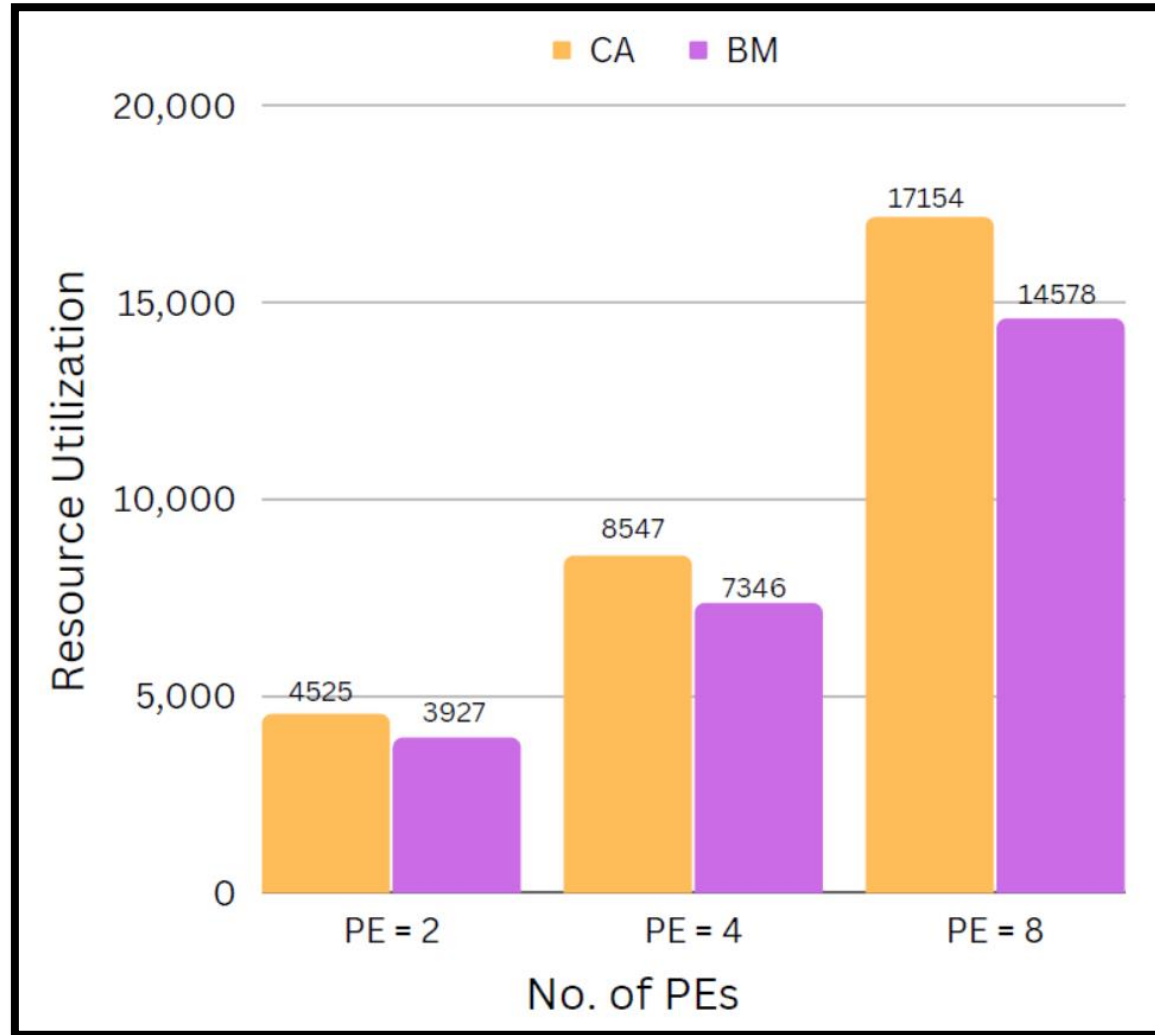
[word size = 32 bits]



Power Analysis



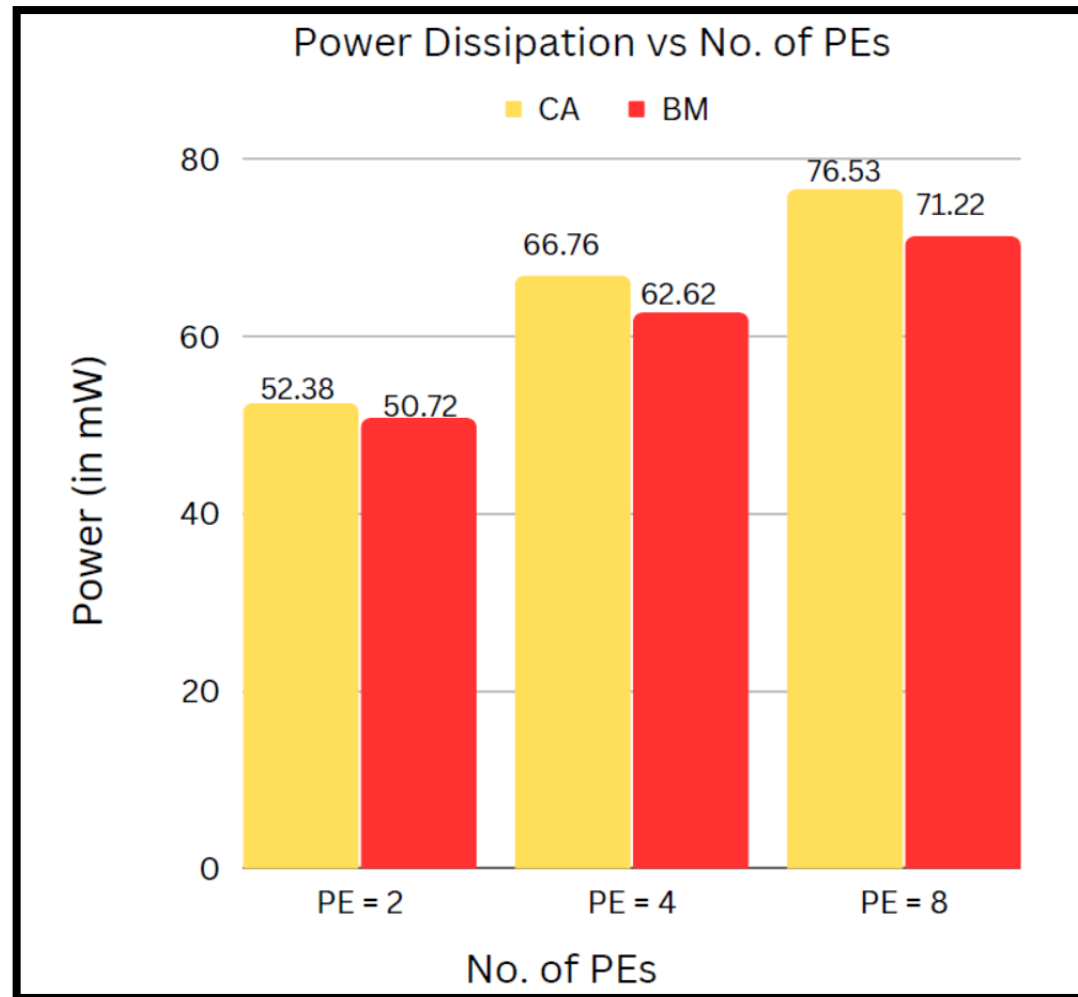
Performance Analysis



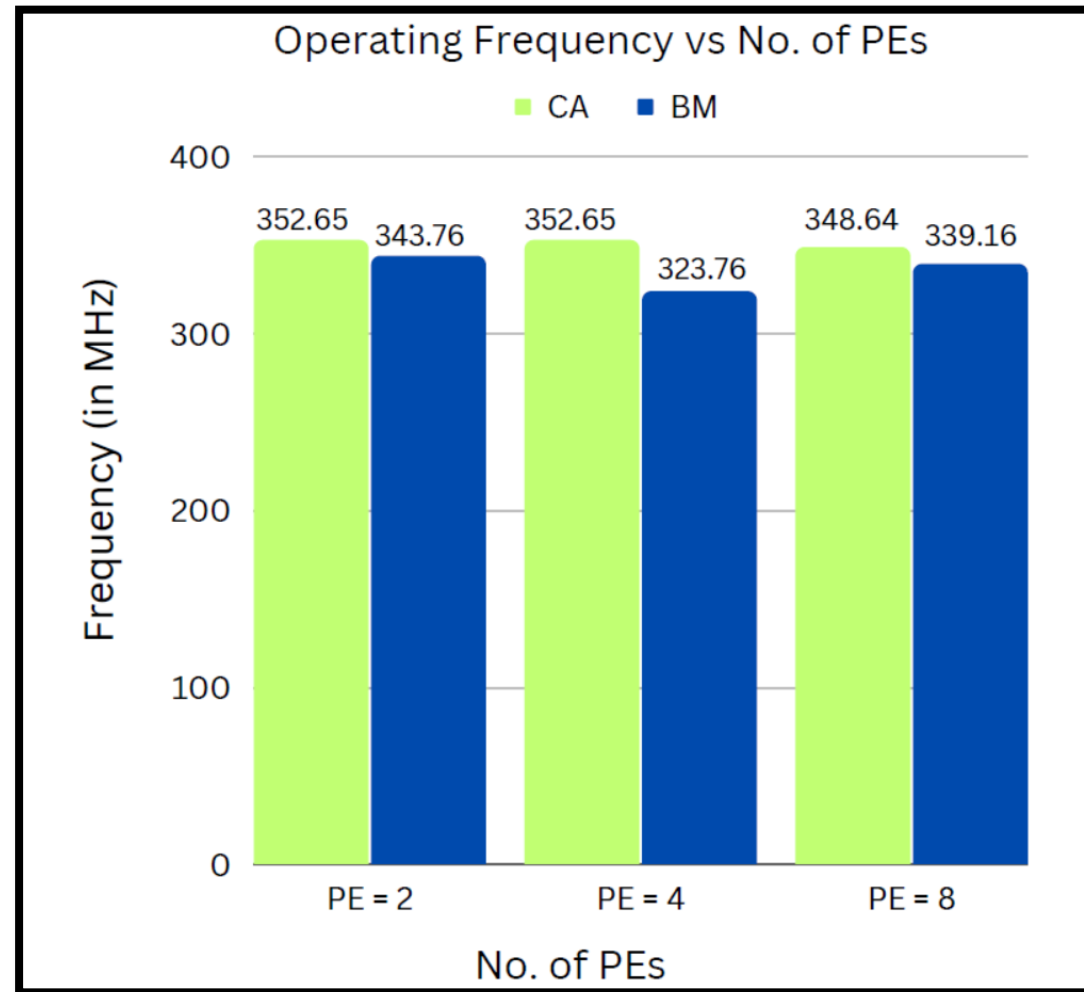
Area Analysis

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

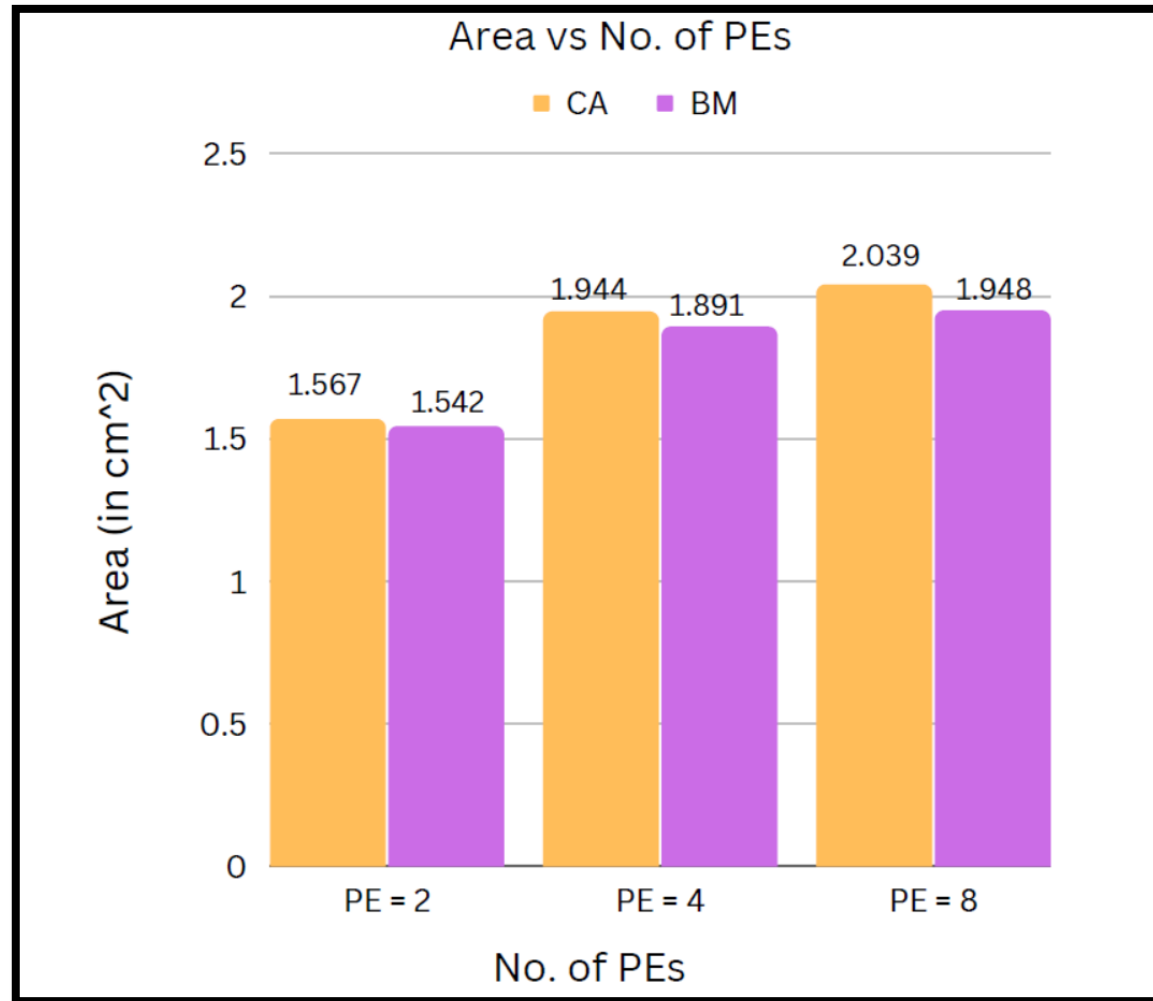
[word size = 32 bits]



Power Analysis



Performance Analysis



Area Analysis