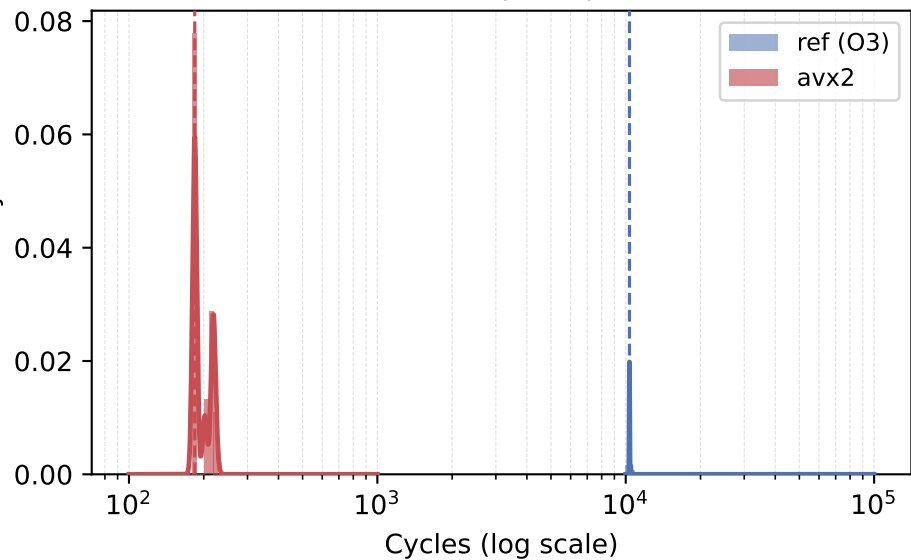
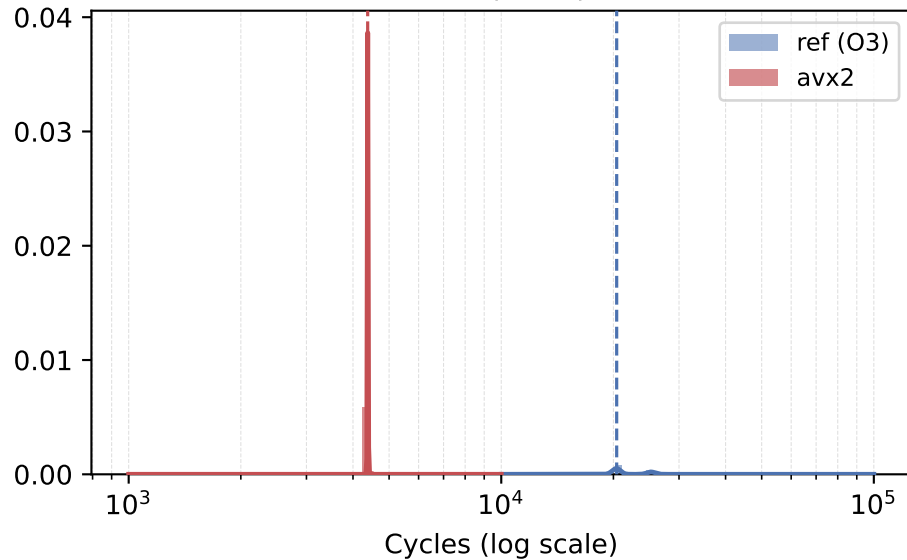


Cycle Count Distributions — ref vs. avx2 (ML-KEM-512)  
Dashed lines show medians. Distributions are right-skewed  $\rightarrow$  nonparametric statistics.

INVNTT  
( $\sim 55\times$  speedup)



gen\_a  
( $\sim 4\times$  speedup)



noise  $\eta_1$   
( $\sim 1.3\times$  speedup)

