

LAC Performance on Intel64 AVX2

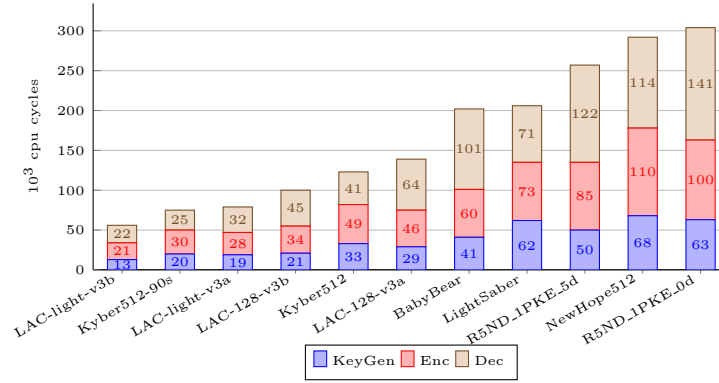


Fig. 1. Performance of 128-bits security level (AVX2 version)

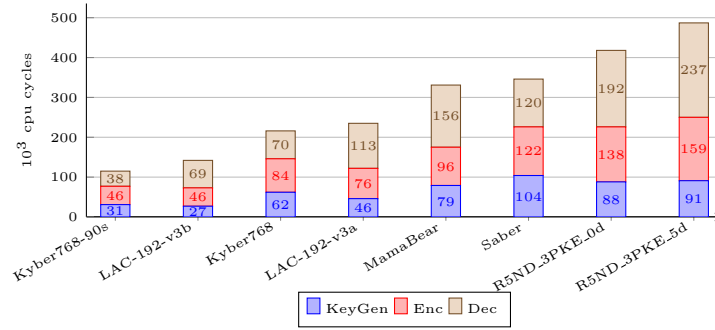


Fig. 2. Performance of 192-bits security level (AVX2 version)

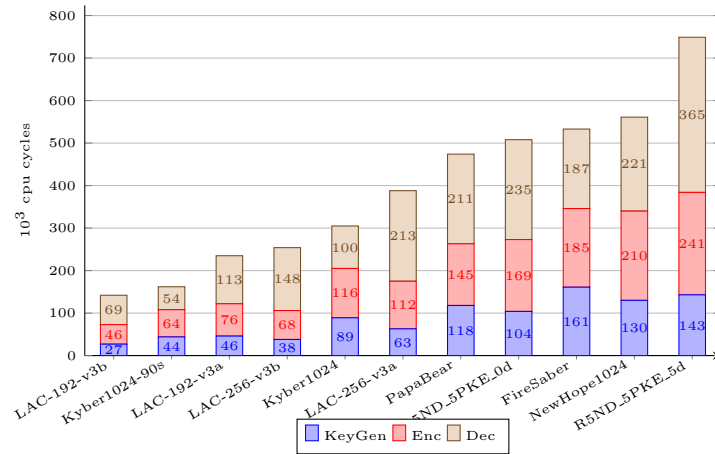


Fig. 3. Performance of 256-bits security level (AVX2 version)