

running time of  $2 \times 10^6$  searches on  $n$  128-bit values

