Fast Assembler Implementations of the AES

CPU	*Mode*	*API*	*Table sizes*	*Cycles/Block*	*Best previous*
Pentium III	CBC	n-block	4k + 4k	224	226 (Lipmaa)
Pentium IV	CBC	n-block	4k + 4k	260	260 (Lipmaa)
Athlon	ECB	1-block	8k + 8k	225	319 (Lipmaa, C)

Dag Arne Osvik
University of Bergen
osvik@ii.uib.no
http://www.ii.uib.no/~osvik