FLEXIBLE ARCHITECTURE AND INSTRUCTION FOR ADVANCED ENCRYPTION STANDARD (AES)

ABSTRACT

A flexible aes instruction set for a general purpose processor is provided. The instruction set includes instructions to perform a "one round" pass for aes encryption or decryption and also includes instructions to perform key generation. An immediate may be used to indicate round number and key size for key generation for 128/192/256 bit keys. The flexible aes instruction set enables full use of pipelining capabilities because it does not require tracking of implicit registers.

(Fig. 3)