AES Encryption IP Cores Family

Compact, High-Throughput, Certified Hardware AES Encrypt/Decrypt Engines

CAST provides AES cores that perform encryption and decryption using the AES Rijndael Block Cipher Algorithm. They all satisfy the Federal Information Processing Standard (FIPS) Publication 197 or the Special Publication 800-38D and have been certified for compliance by the US National Institute of Standards and Technology (NIST). A variety of AES cores are available so you can choose the best combination of size, performance, and features for your particular application. The following table summarizes the family members and indicates their basic features.

AES IP Cores	**AES**[1] (-S or -F)	**AES-P** (-S or -F)	**AES-GCM** or **AES-CCM** (-S or -F)	**AES-GCM** (-X or -X2)	**AES-XTS** (-X or -X2)
Run time Programmable Encryption or Decryption operation	✓	✓	✓	✓	✓
Run-time Programmable Cipher-Key Length	✓	✓	✓	✓	✓
Run-time Programmable Block Cipher Mode	X	✓	X	X	X
ECB Mode	✓	✓	X	X	X
CBC Mode	✓	✓	X	X	X
CFB Mode	✓	✓	X	X	X
OFB Mode	✓	✓	X	X	X
CTR Mode	✓	✓	X	X	X
LRW Mode	✓	X	X	X	X
Key Expander	✓	✓	✓	✓	✓
Number of bits/cycle for128/192/256 key	2.91/2.46/2.13 or 11.64/9.85/8.53	2.91/2.46/2.13 or 11.64/9.85/8.53	2.91/2.46/2.13 or 11.64/9.85/8.53	128/na/128 or 256/na/256	128/na/128 or 256/na/256

✓= Included or user-configurable option ✓= On request X = Not supported

Notes:

1: only one encryption/decryption mode is supported by each release of the core