Int-11600

AES Advanced Encryption/Decryption Standard Core

The AES core implements Rijndael encoding and decoding in compliance with the NIST Advanced Encryption Standard. It processes 128-bit blocks, and is programmable for128-, 192-, and 256-bit key lengths.

Different versions provide the best speed/area results for specific applications. Various cipher modes can be supported (ECB, CBC, OFB, CFB, CTR, CCM), different datapath widths are possible, and smaller or faster architectures are available. The core works with a pre-expanded key, or with optional key expansion logic.

The fully synchronous design is available in source or netlist forms.

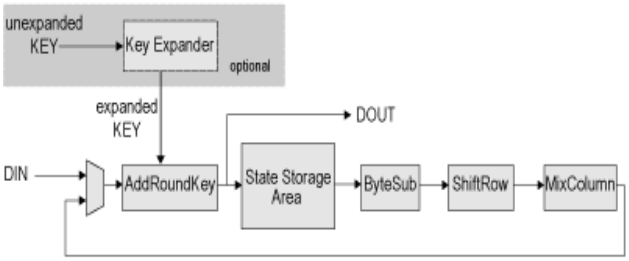
Features

- Encrypts and decrypts using the AES Rijndael Block Cipher Algorithm
- Satisfies Federal Information Processing Standard (FIPS) Publication 197 from the US National Institute of Standards and Technology (NIST)
- Processes 128-bit data in 32-bit blocks
- Employs user-programmable key size of 128, 192 or 256 bits
- Smallest version supports a single block cipher mode, Electronic Codebook (ECB); these modes can be added as needed: Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback

Applications

- Protected network routers
- Electronic financial transactions
- Secure wireless communications
- Secure video surveillance systems
- Encrypted data storage

Block Diagram



I I Implementation Results:

Device Utilization and Performance. Typical

Representative performance figures are shown here.

Core	Technology	Area	Speed	Throughput	Optimized for:
AES 32-bit	TSMC 0.13 u	5 Kgates	152 MHz	~440 Mbit/s	area
AES 32-bit	UMC 0.18 u	5 Kgates	142 MHz	~411 Mbit/s	area
AES 32-bit	TSMC 0.13 u	8.4 Kgates	400 MHz	~1.16 Gbit/s	speed
AES 32-bit	UMC 0.18 u	9.3 Kgates	344 MHz	~997 Mbit/s	speed
AES 128-bit	TSMC 0.13 u	17.5 Kgates	151 MHz	~1.75 Gbit/s	area
AES 128-bit	UMC 0.18 u	16 Kgates	144 MHz	~1.67 Gbit/s	area
AES 128-bit	TSMC 0.13 u	36.8 Kgates	400 MHz	~4.64 Gbit/s	speed
AES 128-bit	UMC 0.18 u	34.6 Kgates	344 MHz	~3.99 Gbit/s	speed
KEXP 32-bit	TSMC 0.13 u	6 Kgates	196 MHz	~568 Mbit/s	area
KEXP 32-bit	UMC 0.18 u	5.6 Kgates	226 MHz	~800 Mbit/s	area
KEXP 32-bit	TSMC 0.13 u	7.3 Kgates	500 MHz	~1.45 Gbit/s	speed
KEXP 32-bit	UMC 0.18 u	5.8 Kgates	400 MHz	~1.16 Gbit/s	speed
KEXP 128-bit	TSMC 0.13 u	8.7 Kgates	196 MHz	~2.27 Gbit/s	area
KEXP 128-bit	UMC 0.18 u	8.1 Kgates	150 MHz	~1.74 Gbit/s	area
KEXP 128-bit	TSMC 0.13 u	19.4 Kgates	400 MHz	~4.64 Gbit/s	speed
KEXP 128-bit	UMC 0.18 u	11.6 Kgates	226 MHz	~3.20 Gbit/s	speed

intelop

Intelop Corporation 4800 Great America Pkwy. Ste-201 Santa Clara CA. 95054. www.intelop.com
Ph: 408-496-0333. Fax: 408-496-0444 Email: sales@intelop.com