AES-256 E Advanced Encryption Standard Encoding Core

The AES_E core implements Rijndael encoding 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), 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 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 (OFB) and Counter (CTR)
- Works with a pre-expended key or can integrate the optional key expansion function
- Simple, fully synchronous, reusable design
- Available as fully functional and synthesizable VHDL or Verilog, or as a netlist for popular programmable devices
- Complete deliverables include test benches

Applications:

Protected Network
Electronic financial transactions
Secured Wireless Communication
Secured Video surveillance
Encrypted Data Storage

- Works with a pre-expended key or can integrate the optional key expansion function
- Simple, fully synchronous, reusable design
- Available as fully functional and synthesizable VHDL or Verilog, or as a netlist for popular programmable devices

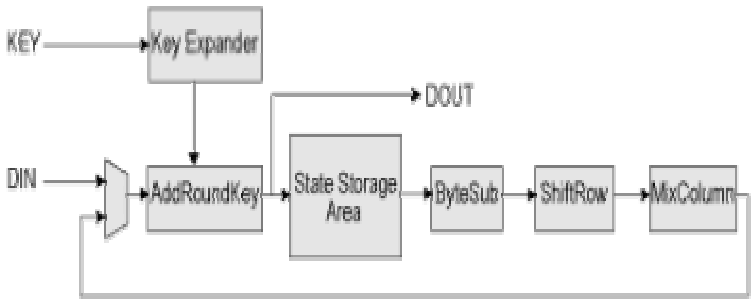
Implementation Results

Device Utilization and Performance

Typical performance figures for 32-bit data-path ECB mode with optimization for speed are shown in Table

Core	Technology	Area	Speed	Throughput with 128-bit key
AES_E	0.18 u	4.9 Kgates	384 MHz	~1.11 Gbit/s
AES_E	0.25 u	6.0 Kgates	294 MHz	~855 Mbit/s
KEXP_E	0.18 u	5.9 Kgates	400 MHz	~1.16 Gbit/s
KEXP_E	0.25 u	5.7 Kgates	315 MHz	~913 Mbit/s

Block Diagram



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