Advanced Encryption Standard

SILVACO

70136

DESCRIPTION

The Advanced Encryption Standard (AES) IP Core is a complete hardware implementation encryption/decryption algorithm described in the U.S. Government Federal Information Processing Standards Publication 197 (FIPS 197). The AES IP Core implements the Rijndael algorithm which is a symmetric block cipher that can process 128 bit data blocks using 128, 192, or 256 bit cipher keys.

The United States Government designed the Advanced Encryption Standard (AES) in 2000 to replace the older Data Encryption Standard (DES). AES is a symmetric block cipher which means that the same key is used for both encryption and decryption of the data block.

For further information, refer to: Federal Information Processing Standards Publication 197, November 26, 2001, Announcing the ADVANCED ENCRYPTION STANDARD (AES).

The AES IP Core operates as the FIPS 197 standard specifies. This is the most basic Electronic Codebook (ECB) mode. Other modes such as Cipher Block Chaining (CBC) and Cipher Feedback (CFB) modes can be added external to the AES IP Core and controlled by a set of additional registers.

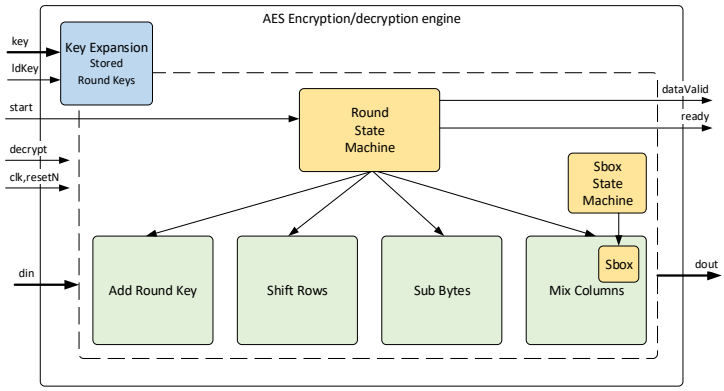
See AHB AES Encryption/Decryption w/ AHB DMA (product number 70122) for how the AES IP Core is used in ECB, CBC, and CFB modes.

AES IP CORE FEATURES

- Advanced Encryption Standard FIPS 197 compliant
- Implements Rijndael algorithm
- Efficient “Tower Field” SBox implementation
- Encrypts / Decrypts 128 bit data blocks
- Supports key lengths of 128, 192, and 256 bits
- Low gate count or higher performance pipelined options
- Verilog IP Core

AES IP CORE DELIVERABLES

- Verilog Source
- Complete Test Environment



SILVACO

Headquarters
2811 Mission College Boulevard, 6th floor
Santa Clara, Ca 95054 USA
Phone: 408-567-1000
Fax: 408-496-6080

California	sales@silvaco.com
	408-567-1000
Massachusetts	masales@silvaco.com
	978-323-7901
Texas	txsales@silvaco.com
	512-418-2929
Japan	jpsales@silvaco.com
Europe	eusales@silvaco.com
France	eusales@silvaco.com
Korea	krsales@silvaco.com
Taiwan	twsales@silvaco.com
Singapore	sgsales@silvaco.com
China	cnsales@silvaco.com

WWW.SILVACO.COM

Rev 111516_01