AES1

## Ultra-Compact Advanced Encryption Standard Core

General Description

The AES core implements Rijndael encoding and decoding in compliance with the NIST Advanced Encryption Standard.

Basic core is very small (less than 3,000 gates). Enhanced versions are available that support encryption and decryption for various cipher modes (ECB, CBC, OFB, CFB, CTR), as well as different datapath widths for size/performance tradeoff. The core includes the key expansion logic.

The design is fully synchronous and available in both source and netlist form. Test bench includes vectors from FIPS-197 and the original Rijndael submission. AESAVS tests are also available.

AES Core is supplied as portable Verilog (VHDL version available) thus allowing customers to carry out an internal code review to ensure its security.

Symbol
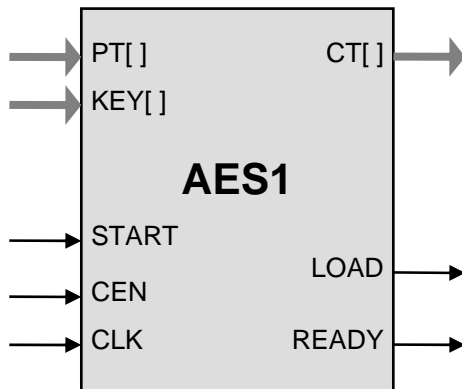
Base Core Features

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 blocks with 8, 16 or 32-bit data interface

Employs key size of 128,192 and 256 bit.

Includes the key expansion function

Supports simple modes of AES defined in SP800-38A: ECB, CBC, CFB, OFB and CTR

Completely self-contained: does not require external memory

Available as fully functional and synthesizable Verilog, or as a netlist for popular programmable devices and ASIC libraries

Deliverables include test benches

Applications

- Secure wireless communications, including 802.11i, 802.15.3, 802.15.4 (ZigBee), MBOA, 802.16e

- Electronic financial transactions

- Content protection, digital rights management (DRM), set-top boxes

- Secure video surveillance systems

- Encrypted data storage

- Secure RFID

- Secure Smart Cards

Pin Description

| Name	Type	Description
CLK	Input	Core clock signal
EN	Input	Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored.
START	Input	When goes HIGH, a cryptographic operation is started
LOAD	Output	Input data request signal
READY	Output	Output data ready and valid
8-bit Data Interface		
KEY[7:0]	Input	Encryption Key
PT[7:0]	Input	Input Plain Text Data
CT[7:0]	Output	Output Cipher Text Data
16-bit Data Interface		
KEY[15:0]	Input	Encryption Key
PT[15:0]	Input	Input Plain Text Data
CT[15:0]	Output	Output Cipher Text Data
32-bit Data Interface		
KEY[31:0]	Input	Encryption Key
PT[31:0]	Input	Input Plain Text Data
CT[31:0]	Output	Output Cipher Text Data

Function Description

An AES encryption operation transforms a 128-bit block into a block of the same size. The encryption key size is 128 bit. The key is expanded during cryptographic operations. The block performs AES encryption as defined by NIST in FIPS-197 and AESAVS validation suite.

Operation

A rising input on the START port triggers the beginning of a cryptographic operation on the data PT, using the KEY as key. The core then raises the LOAD signal requesting the data block. It then starts to process the state according to the AES algorithm.

The timing diagram below shows how the data is fed to the core at the start.

CLK

START

LOAD

KEY[7:0]   K0 K1 K2 ... ... K13 K14 K15

PT[7:0]   PT0 PT1 PT2 ... ... PT13 PT14 PT15
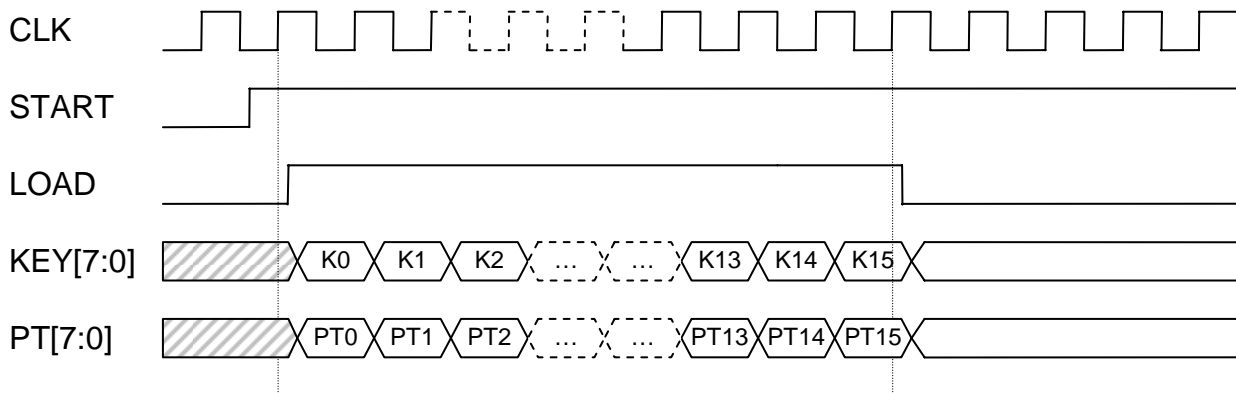
Key and data input at the start of encryption

Both the data and the key are input serially, 8, 16 or 32 bits at the time. The diagram above shows the case where the input data is 8 bit

When all the rounds are completed, the READY signal is raised and the encrypted data starts to flow out. This is shown in the timing diagram below.

CLK

START

READY

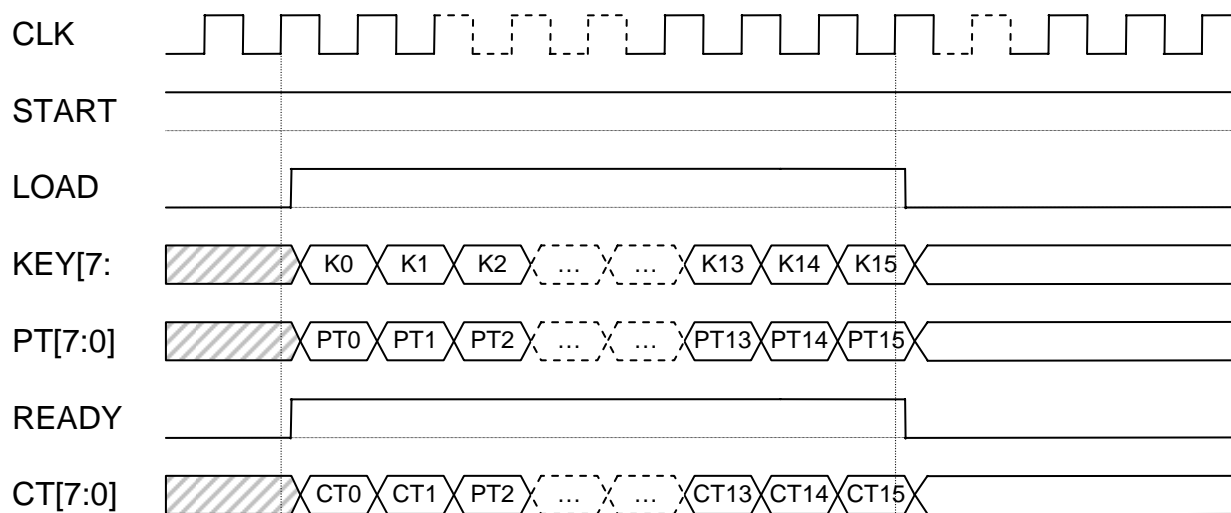CT[7:0]   CT0 CT1 CT2 ... ... CT13 CT14 CT15
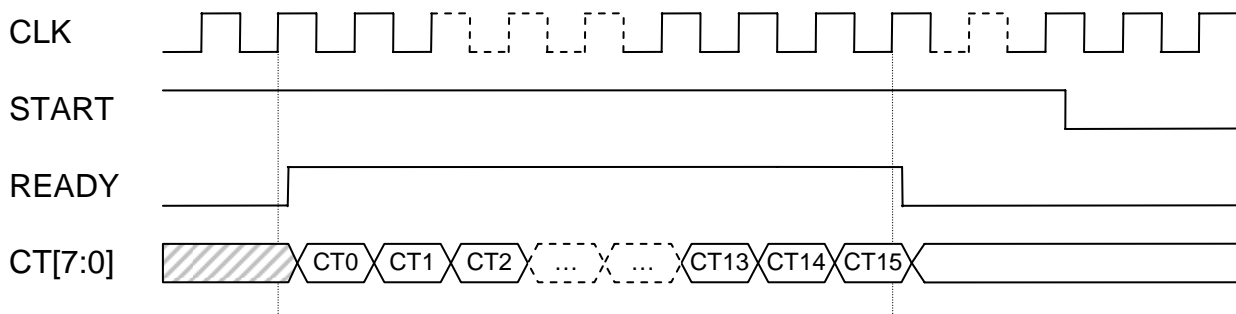
Cipher text output

It is possible to start a new cryptographic operation as soon as the data from the previous one is output. A cryptographic operation can be aborted at any time by lowering the START signal for at least one clock cycle.

The core is fully pipelined. Keeping the START signal HIGH causes the new cryptographic operation to start simultaneously with ending of previous one; in this case LOAD and READY signals are generated by the core simultaneously. Loading of the new plain text data and key is combined with outputting cipher text data from

the previous operation. This is shown in the timing diagram below.

CLK	
START	
LOAD	
KEY[7:	▨ K0 K1 K2 ... ... K13 K14 K15
PT[7:0]	▨ PT0 PT1 PT2 ... ... PT13 PT14 PT15
READY	
CT[7:0]	▨ CT0 CT1 PT2 ... ... CT13 CT14 CT15

Cipher text from a previous operation is being output while new plaintext is input

New key can be used for each cryptographic operation. The absence of gaps allows sustaining the throughput listed in the table below.

Datapath Width, bit	8	16	32	64
Cycles	160	80	40	20
Bit per clock cycle	0.8	1.6	3.2	6.4

Throughput as a function of datapath width for 128-bit key

Implementation Details

Representative area/resources figures for 8-bit datapath ECB mode are shown below.

Technology	Area / Resources
TSMC 0.18 **u**	2948 gates
Altera FPGA	639 LUT
Xilinx FPGA	236 SLICEs

Available Versions

The AES core is available in ECB, CFB, CBC, OFB and CTR modes, and for different datapath widths. Decryption option is also available.

Export Permits

US Bureau of Industry and Security has assigned the export control classification number 5E002 to the core. The core is eligible for the license exception ENC under section 740.17(A) and (B)(1) of the export administration regulations. See the IP Cores, Inc. licensing basics page, http://ipcores.com/export_licensing.htm, for links to US government sites and more details.

Deliverables

HDL Source Licenses

- Synthesizable Verilog RTL source code

- Testbench (self-checking)

- Test vectors

- Expected results

- User Documentation

Netlist Licenses

- Post-synthesis EDIF

- Testbench (self-checking)

- Test vectors

- Expected results

Contact Information

IP Cores, Inc.
3731 Middlefield Rd.
Palo Alto, CA 94303, USA
Phone: +1 (650) 814-0205
E-mail: info@ipcores.com
www.ipcores.com