XTS2 Family of Cores

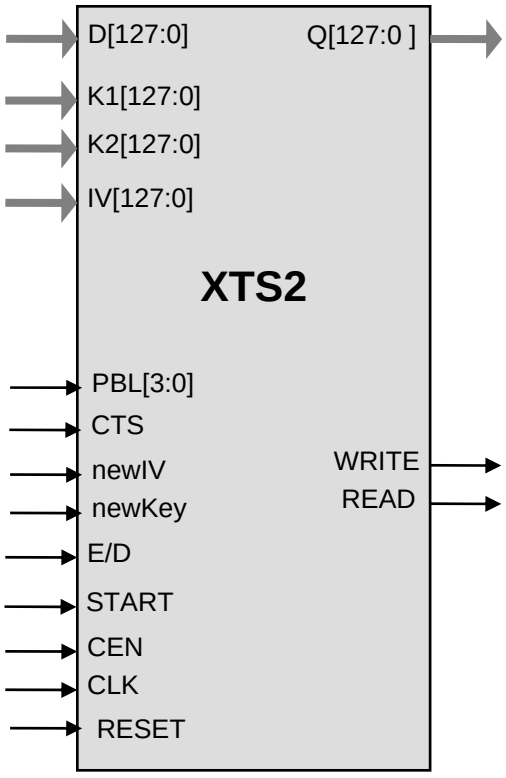
IEEE P1619 XTS-AES Cores

General Description

XTS2 implements the NIST standard AES cipher in the XTS mode for encryption and decryption with ciphertext stealing (CTS). The XTS2 family of cores covers a wide range of area / throughput combinations, allowing the designer to choose the smallest core that satisfies the desired clock/throughput requirements. Cores contain the base AES core AES1 and are available for immediate licensing.

The design is fully synchronous and available in both source and netlist form.

Symbol



Key Features

Small size: XTS2-25.6 starts at less than 30,000 ASIC gates and throughput of 25.6 bits per clock

Completely self-contained: does not require external memory

Support for XTS mode encryption and decryption. Encryption-only and decryption-only versions are available.

Includes key expansion and CTS support

128+128 AES keys supported.

Easily parallelizable for even higher data rates

Flow-through design

Test bench provided

Applications

- Hard drive encryption compliant with the IEEE P1619

Pin Description

Name	Type	Description
CLK	Input	Core clock signal
CEN	Input	Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored.
RESET	Input	HIGH level asynchronously resets the core
E/D	Input	When HIGH, core is encrypting, when LOW core is decrypting. This pin is not present on encryption only or decryption only versions of the core
START	Input	HIGH level starts the input data processing
READ	Output	Read request for the input data byte
WRITE	Output	Write signal for the output interface
D[127:0]	Input	Input Data (other data bus widths are also available) • plain or cipher text
IV[127:0]	Input	IV (logical position)
K1[127:0]	Input	AES key
K2[127:0]	Input	Tweak key (K_2)
Q[127:0]	Output	Output plain or cipher text
newKey	Input	New AES Key available on K1 input
newIV	Input	New Tweak Key available on K2 input, and new IV available on IV input
cts	Input	Marks the last full 128-bit block of the data unit in case that the next block of this data unit is less than 128 bit (CTS mode)
PBL[3:0]	Input	Partial Block length (in bytes)

Function Description

The Advanced Encryption Standard (AES) algorithm is a new NIST data encryption standard as defined in the http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

The XTS2 implementation fully supports the AES algorithm for 128+128 bit keys XTS mode as defined by the P1619 draft standard.

The core is designed for flow-through operation, with 128-bit wide input and output interfaces. XTS2 supports both encryption and decryption modes.

Implementation Results

Area Utilization and Performance

Representative area/resources figures are shown below.

Core Type	Technology	Area / Resources	Max Frequency	Throughput
XTS2-64	TSMC 0.09 µ LV	110,000 gates	215 MHz	13.7 Gbps

Multiple XTS2 cores can be easily paralleled for throughputs of 100 Gbps and higher.

Export Permits

US Bureau of Industry and Security has assigned the export control classification number 5E002 to the AES1 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
- Verilog testbench (self-checking)
- Vectors for testbench
- Expected results
- User Documentation

Netlist Licenses

- Post-synthesis EDIF
- Testbench (self-checking)
- Vectors for testbench
- 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