www.ipcores.com

LRW3 Family of Cores

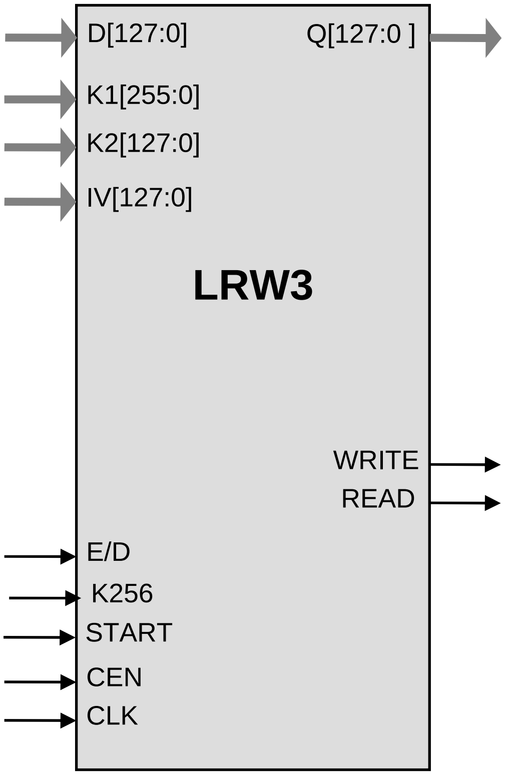
LRW-AES Cores

General Description

LRW3 implements the NIST standard AES cipher in the LRW mode for encryption and decryption. The LRW3 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. Each core contains the base AES core AES1 and is available for immediate licensing.

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

Symbol



Key Features

Small size: LRW3-18.2 starts at less than 50,000 ASIC gates at throughput of 18.2 bits per clock

Completely self-contained: does not require external memory

Supports both encryption and decryption

Includes key expansion

Support for Liskov-Rivest-Wagner encryption and decryption (LRW)

128+128 and 256+128 bit LRW keys supported.

Easily parallelizable for even higher data rates

Flow-through design

Test bench provided

Applications

- Hard drive encryption

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.
E/D	Input	When HIGH, core is encrypting, when LOW core is decrypting
K256	Input	When HIGH, core uses the 256-bit key
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[255:0]	Input	AES key
K2[127:0]	Input	Tweak key (K_2)
Q[127:0]	Output	Output plain or cipher text

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 LRW3 implementation fully supports the AES algorithm for 128+128 and 256+128 bit keys LRW mode.

The core is designed for flow-through operation, with 128-bit wide input and output interfaces. LRW3 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
LRW3-64	TSMC 0.09 µ LV	154,860 gates	215 MHz	13.7 Gbps
LRW3E-64 (encryption only)	TSMC 0.09 µ LV	125,002 gates	215 MHz	13.7 Gbps

Multiple LRW3 cores can be easily paralleled for throughputs of 100 Gbps and higher.

Export Permits

The core can be a subject of the US export control. It is the customer's responsibility to check with relevant authorities regarding the re-export of equipment containing the AES encryption technology. See the site of US Department of Commerce http://www.bxa.doc.gov/Encryption/ for details.

Deliverables

HDL Source Licenses

- Synthesizable Verilog RTL source code
- Testbench (self-checking)
- Vectors for testbenches
- Expected results
- User Documentation

Netlist Licenses

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