LRW1 Core

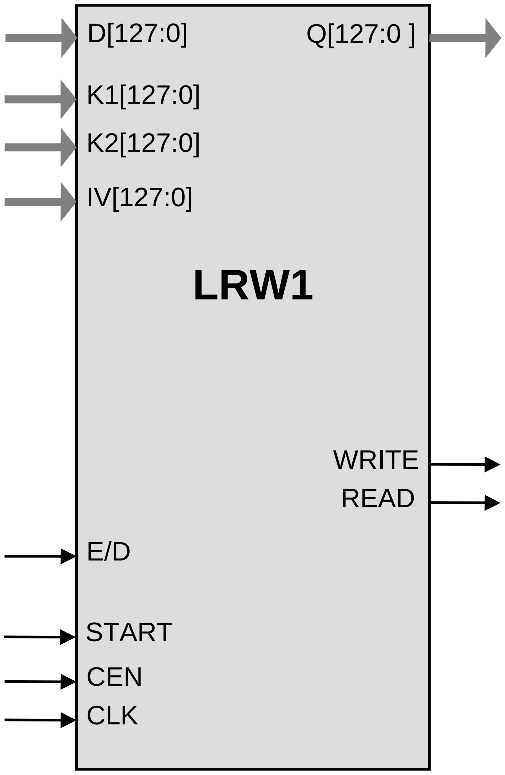
P1619 (Storage Security) LRW-AES Core

General Description

Implementation of the new encrypted shared storage media draft standard P1619 requires the NIST standard AES cipher in the LRW mode for encryption. The LRW1 AES core is tuned for P1619 applications at the data rates of 3 Gbps and higher. The 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: 30,000 ASIC gates at throughput of 12.8 bits per clock

Synthesized for 600+ MHz clock speeds (7.68 Gbps throughput)

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 higher data rates

Flow-through design

Test bench provided

Applications

- IEEE P1619 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
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 (256-bit key option is also available)
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 LRW1 implementation fully supports the AES algorithm for 128+128 and 256+128 bit keys LRW mode as required by the P1619 IEEE draft standard.

The core is designed for flow-through operation, with selectable width of input and output interfaces. LRW1 supports both encryption and decryption modes.

Implementation Results

Device Utilization and Performance

Representative area/resources figures are shown below.

Technology	Area / Resources	Max Frequency	Throughput
TSMC 0.13 µ LV	30,000 gates	250 MHz	3.2 Gbps
TSMC 0.09 µ LV	60,000 gates	600 MHz	7.68 Gbps

Multiple LRW1 cores can be easily paralleled for throughputs of 10 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