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.

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

Applications

- IEEE P1619 hard drive encryption

Symbol

![Diagram of LRW1 Core](image)
## Pin Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLK</td>
<td>Input</td>
<td>Core clock signal</td>
</tr>
<tr>
<td>CEN</td>
<td>Input</td>
<td>Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored.</td>
</tr>
<tr>
<td>E/D</td>
<td>Input</td>
<td>When HIGH, core is encrypting, when LOW core is decrypting</td>
</tr>
<tr>
<td>START</td>
<td>Input</td>
<td>HIGH level starts the input data processing</td>
</tr>
<tr>
<td>READ</td>
<td>Output</td>
<td>Read request for the input data byte</td>
</tr>
<tr>
<td>WRITE</td>
<td>Output</td>
<td>Write signal for the output interface</td>
</tr>
<tr>
<td>D[127:0]</td>
<td>Input</td>
<td>Input Data (other data bus widths are also available)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• plain or cipher text</td>
</tr>
<tr>
<td>IV[127:0]</td>
<td>Input</td>
<td>IV (logical position)</td>
</tr>
<tr>
<td>K1[127:0]</td>
<td>Input</td>
<td>AES key (256-bit key option is also available)</td>
</tr>
<tr>
<td>K2[127:0]</td>
<td>Input</td>
<td>Tweak key (K₂)</td>
</tr>
<tr>
<td>Q[127:0]</td>
<td>Output</td>
<td>Output plain or cipher text</td>
</tr>
</tbody>
</table>

## Function Description


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.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Area / Resources</th>
<th>Max Frequency</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSMC 0.13 µ LV</td>
<td>30,000 gates</td>
<td>250 MHz</td>
<td>3.2 Gbps</td>
</tr>
<tr>
<td>TSMC 0.09 µ LV</td>
<td>60,000 gates</td>
<td>600 MHz</td>
<td>7.68 Gbps</td>
</tr>
</tbody>
</table>

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/](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](http://www.ipcores.com)