General Description

Implementation of the new WLAN security standard (802.16e) requires the NIST standard AES cipher in CTR and CBC modes (a.k.a. CCM) for encryption and message authentication. The CCM6 AES core is tuned for 802.16e applications. 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: From 8,900 ASIC gates at 802.16 data speeds
- Completely self-contained: does not require external memory
- Supports encryption and decryption,
- Includes key expansion (scheduling)
- Support for Counter Mode Encryption (CTR) operation and CCM extensions (Counter Mode with CBC MAC)
- Support for CMAC and MBS-CTR
- Flow-through design
- Test bench provided

Applications

- IEEE 802.16e
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>RESET</td>
<td>Input</td>
<td>Core reset signal</td>
</tr>
<tr>
<td>MODE</td>
<td>Input</td>
<td>Operation mode of the core</td>
</tr>
<tr>
<td>START</td>
<td>Input</td>
<td>HIGH starting input data processing</td>
</tr>
<tr>
<td>READ</td>
<td>Output</td>
<td>Read request for the input data byte</td>
</tr>
<tr>
<td>DATA_VALID</td>
<td>Input</td>
<td>HIGH when valid data byte present on the input</td>
</tr>
<tr>
<td>WRITE</td>
<td>Output</td>
<td>Write to the output interface</td>
</tr>
<tr>
<td>OUT_READY</td>
<td>Input</td>
<td>HIGH when output interface is ready to accept data byte</td>
</tr>
<tr>
<td>D[7:0]</td>
<td>Input</td>
<td>Input Data</td>
</tr>
<tr>
<td>Q[7:0]</td>
<td>Output</td>
<td>Output Data</td>
</tr>
<tr>
<td>DONE</td>
<td>Output</td>
<td>Data processing completed</td>
</tr>
</tbody>
</table>

Function Description


The CCM6 implementation fully supports the AES algorithm for 128 bit keys in Counter Mode (CTR) method of encryption with CBC message integrity check as required by the CCM protocol of the 802.16e standard, as well as MBS-CTR and CMAC modes as required by the WiMAX standard.

The core is designed for flow-through operation, with byte-wide input and output interfaces. CCM key precedes the frame in the flow of data. CCM6 supports encrypt/decrypt modes and include on-the-fly key expansion (scheduling).
Implementation Results

Area Utilization and Performance
Representative area/resources figures are shown below.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Area / Resources</th>
<th>Frequency</th>
<th>Max Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSMC 0.13 µ</td>
<td>11,861 gates</td>
<td>250 MHz</td>
<td>800 Mbps</td>
</tr>
<tr>
<td>TSMC 0.13 µ</td>
<td>24,763 gates</td>
<td>150 MHz</td>
<td>960 Mbps</td>
</tr>
</tbody>
</table>

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 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