General Description

The PRNG1 core implements a cryptographically secure pseudo-random number generator per NIST publication SP800-90.

Basic core is small (6,500 gates) and uses an external 256-bit entropy seed to generate 16 bytes (128 bits) of random data at a time (128 bits of security strength). Versions of the core are available supporting higher security strengths (192 and 256 bits), larger amounts of generated bits (up to $2^{15}$), and different internal datapath widths for size/performance tradeoff. The core includes the AES1 core.

The design is fully synchronous and available in both source and netlist form. Test bench uses vectors in plain text format.

PRNG1 core is supplied as portable Verilog (VHDL version available) thus allowing customers to carry out an internal code review to ensure its security.

Base Core Features

- Generates cryptographically secure pseudo-random numbers
- Uses the CTR_DRBG algorithm per NIST publication SP800-90
- Generates 128-bit data blocks with 8, 16, 32, 64 or 128-bit wide data interface
- Provides security strength of 128, 192 and 256 bits
- Self-contained; does not require external memory
- Available as fully functional and synthesizable Verilog or VHDL for Actel programmable devices
- Deliverables include Verilog test bench and test vectors

Applications

- Secure wireless communications, including 802.11i, 802.15.3, 802.15.4 (ZigBee), MBOA, 802.16e
- Electronic financial transactions
- Content protection, digital rights management (DRM), set-top boxes
- Secure RFID
- Secure Smart Cards
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>MODE</td>
<td>Input</td>
<td>When 0, the START going high will initiate a re-seed. When 1, the START will initiate a generate operation.</td>
</tr>
<tr>
<td>START</td>
<td>Input</td>
<td>Starts the core operation</td>
</tr>
<tr>
<td>RESET</td>
<td>Input</td>
<td>Asynchronous core reset</td>
</tr>
<tr>
<td>SRESET</td>
<td>Input</td>
<td>Synchronous core reset</td>
</tr>
<tr>
<td>READY</td>
<td>Output</td>
<td>Output data ready and valid</td>
</tr>
<tr>
<td>LOAD</td>
<td>Output</td>
<td>Input data request signal</td>
</tr>
<tr>
<td>DONE</td>
<td>Output</td>
<td>Indicates the completion of a re-seed or generate operation</td>
</tr>
<tr>
<td>SEED[]</td>
<td>Input</td>
<td>Input for seed data</td>
</tr>
<tr>
<td>Q[]</td>
<td>Output</td>
<td>Output of pseudorandom data</td>
</tr>
</tbody>
</table>

Function Description

A Re-seed operation transfers external random seed bits into the core. Some of the seed bits, at least the number equal to security strength, should represent entropy and come from a true random source. A Generate operation produces a predefined number of random bits (up to 2^{19}, depending on the configuration). The Generate can be invoked up to 2^{48} times after each re-seed. The core performs pseudorandom generation per CTR_DRBG algorithm as defined by NIST in SP800-90.

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>
</tr>
</thead>
<tbody>
<tr>
<td>Actel ProAsic-3</td>
<td>1,994 tiles</td>
<td>28 MHz</td>
</tr>
</tbody>
</table>

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
- Testbench (self-checking)
- Test vectors
- Expected results
- User Documentation

**Netlist Licenses**
- Post-synthesis EDIF
- Testbench (self-checking)
- Test vectors
- 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