General Description

The SNOW3G1 core implements SNOW 3G stream cipher in compliance with the ETSI SAGE specification version 1.1. It produces the keystream that consists of 32-bit blocks using 128-bit key and IV.

Basic SNOW3G1-8 core is very small (7,500 gates). The SNOW3G1-32 version is 4 times faster. Enhanced versions are available that support UEA2 and UIA2 confidentiality and integrity algorithms.

The design is fully synchronous and available in both source and netlist form. Test bench includes the ETSI/SAGE SNOW 3G test vectors.

SNOW3G1 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

Keystream generation using the SNOW 3G Algorithm

High throughput: up to 40 Gbps in 65 nm process, 10 Gbps in Altera Stratix III

Small size: from 7.5K ASIC gates, 1.1K LE in Altera Cyclone II, 1K ALUTs in Altera Stratix II

Satisfies ETSI SAGE SNOW 3G specification

Outputs keystream in 32-bit data blocks

Uses 128-bit key and IV

Completely self-contained: does not require external memory

Available as fully functional and synthesizable Verilog, or as a netlist for popular programmable devices and ASIC libraries

Deliverables include test benches

Symbol

Applications

- Secure mobile communications
- 3GPP Long Term Evolution (LTE) algorithms UEA2 and UIA2
- ISO standard IS 18033-4
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>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>START</td>
<td>Input</td>
<td>When goes HIGH, a cryptographic operation is started</td>
</tr>
<tr>
<td>READY</td>
<td>Output</td>
<td>Output data ready and valid</td>
</tr>
<tr>
<td>KEY[127:0]</td>
<td>Input</td>
<td>Encryption Key</td>
</tr>
<tr>
<td>IV[127:0]</td>
<td>Input</td>
<td>Input Plain or Cipher Text Data</td>
</tr>
<tr>
<td>Q[]</td>
<td>Output</td>
<td>Output Cipher or Plain Text Data (bit width depends on the configuration)</td>
</tr>
</tbody>
</table>

Function Description
Operation

A rising input on the START port triggers the beginning of a cryptographic operation, using the KEY and IV inputs to initialize the keystream. The core then starts to output the keystream per SNOW 3G algorithm.

When all the rounds are completed, the READY signal is raised and the next unit of keystream is available on the output Q.

The core continues to produce the keystream as long as START is kept high. To throttle the output, at any time the CEN input can be brought low to pause the core.

A cryptographic operation can be aborted at any time by lowering the START signal for at least one clock cycle.
Implementation Details

Representative synthesis results are shown below.

<table>
<thead>
<tr>
<th>Core</th>
<th>Technology</th>
<th>Max Frequency</th>
<th>Area</th>
<th>SNOW 3G Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNOW3G1-8</td>
<td>TSMC 65 nm G+</td>
<td>302 MHz</td>
<td>7,475 gates</td>
<td>2.4 Gbps</td>
</tr>
<tr>
<td>SNOW3G1-8</td>
<td>TSMC 65 nm G+</td>
<td>943 MHz</td>
<td>8,964 gates</td>
<td>7.5 Gbps</td>
</tr>
<tr>
<td>SNOW3G1-32</td>
<td>TSMC 65 nm G+</td>
<td>834 MHz</td>
<td>17,858 gates</td>
<td>26.7 Gbps</td>
</tr>
<tr>
<td>SNOW3G1-32</td>
<td>TSMC 65 nm G+</td>
<td>1.256 GHz</td>
<td>27,326 gates</td>
<td>40.2 Gbps</td>
</tr>
<tr>
<td>SNOW3G1-8</td>
<td>Altera Cyclone II</td>
<td>141 MHz</td>
<td>1,174 LE</td>
<td>1.1 Gbps</td>
</tr>
<tr>
<td>SNOW3G1-32</td>
<td>Altera Cyclone II</td>
<td>149 MHz</td>
<td>4,812 LE</td>
<td>4.77 Gbps</td>
</tr>
<tr>
<td>SNOW3G1-32</td>
<td>Altera Stratix II</td>
<td>256 MHz</td>
<td>1,125 ALUTs</td>
<td>8.2 Gbps</td>
</tr>
<tr>
<td>SNOW3G1-32</td>
<td>Altera Stratix III</td>
<td>321 MHz</td>
<td>1,121 ALUTs</td>
<td>10.3 Gbps</td>
</tr>
</tbody>
</table>

Export Permits

See the IP Cores, Inc. licensing basics page, [http://ipcores.com/export_licensing.htm](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) 815-7996
E-mail: info@ipcores.com
www.ipcores.com