General Description

The RC4 core implements the RC4 stream cipher in compliance with the ARC4 specification. It produces the keystream that consists of 8-bit words using a key with the length up to 256 bits.

The design is fully synchronous and available in both source and netlist form.

RC4 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 RC4 algorithm
- Small size: from 20K ASIC gates
- Satisfies the ARC4 specification
- Capability to save and restore internal state using a data bus with parameterized width.
- Outputs keystream in 8-bit data words
- Uses a key of up to 256 bits
- 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

Applications

- SSL/TLS accelerators
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>QVALID</td>
<td>Output</td>
<td>If HIGH, output data ready and valid on the Q bus</td>
</tr>
<tr>
<td>QREADY</td>
<td>Input</td>
<td>If HIGH, the external circuitry is ready to accept data from the Q bus</td>
</tr>
<tr>
<td>KEY[255:0]</td>
<td>Input</td>
<td>Encryption key (in the MSB)</td>
</tr>
<tr>
<td>KLEN[4:0]</td>
<td>Input</td>
<td>Encryption key length in bytes</td>
</tr>
<tr>
<td>MODE</td>
<td>Input</td>
<td>If LOW, START initiates key expansion and keystream generation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If HIGH, START continues the keystream using the state read from the Sin pins</td>
</tr>
<tr>
<td>Q[7:0]</td>
<td>Output</td>
<td>Output keystream data (other bit widths available)</td>
</tr>
<tr>
<td>Sin[ ]</td>
<td>Input</td>
<td>Saved state input (configurable width)</td>
</tr>
<tr>
<td>Sout[ ]</td>
<td>Output</td>
<td>State output (configurable width)</td>
</tr>
<tr>
<td>Sactive</td>
<td>Output</td>
<td>If HIGH, Sout outputs valid state data. If HIGH and MODE is also HIGH, Sin shall have valid state</td>
</tr>
</tbody>
</table>

Function Description

An RC4 keystream generator produces a keystream in 8-bit increments per ARC4 (ARCFOUR) specification.

Operation

A rising input on the START port triggers the beginning of a cryptographic operation, using the either the KEY or Sin inputs to initialize the keystream. In any case the old state is evacuated via the Sout pins. The core then starts to output the keystream per RC4 algorithm.

External circuitry can also pause the core by deasserting the QREADY pin, and has to read the keystream value off the Q output if QVALID is asserted.

The core continues to produce the keystream as long as START is kept high. To throttle the output, also 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.
Export Permits

See the IP Cores, Inc. licensing basics page, http://ipcores.com/exportinformation.htm, for links to US government sites and more details. An RC4-NLR version restricted to 56 bits of the key is available without any license requirements.

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