SNOW3G1

Ultra-Compact Snow 3G Cipher Core

General Description

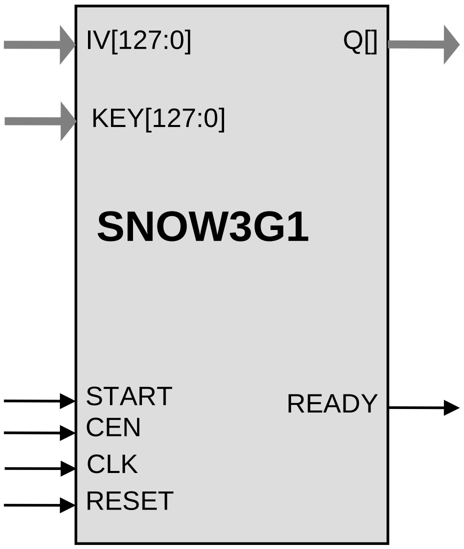
The SNOW3G1 core implements SNOW 3G stream cipher in compliance with the ETSI SAGE specification version 1.1. It produces the keystream that consists of 32-bit blocks using 128-bit key and IV.

Basic core is very small (7,500 gates). Enhanced versions are available that support UEA2 and UIA2 confidentiality an 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.

Symbol



Base Core Features

Keystream generation using the SNOW 3G Algorithm

High throughput: up to 7.5 Gbps in 65 nm process

Small size: from 7.5K ASIC gates

Satisfies ETSI SAGE SNOW 3G specification

Outputs keystream in 32-bit data blocks

Use 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

Applications

- Secure mobile communications
- 3GPP Long Term Evolution (LTE) algorithms UEA2 and UIA2
- ISO standard IS 18033-4

Pin Description

Name	Type	Description
CLK	Input	Core clock signal
RESET	Input	Core reset signal
CEN	Input	Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored.
START	Input	When goes HIGH, a cryptographic operation is started
READY	Output	Output data ready and valid
KEY[127:0]	Input	Encryption Key
IV[127:0]	Input	Input Plain or Cipher Text Data
Q[]	Output	Output Cipher or Plain Text Data (bit width depends on the configuration)

Function Description

A SNOW 3G operation produces a keystream in 32-bit data blocks as defined by ETSI/SAGE “Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 2: SNOW 3G Specification” Version: 1.1.

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.

Technology	Max Frequency	Area	SNOW 3G Throughput
TSMC 65 nm G+	302 MHz	7,475 gates	2.4 Gbps
TSMC 65 nm G+	943 MHz	8,964 gates	7.5 Gbps

Export Permits

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) 815-7996
E-mail: info@ipcores.com
www.ipcores.com