KSM1

Ultra-Compact Kasumi Cipher Core

General Description

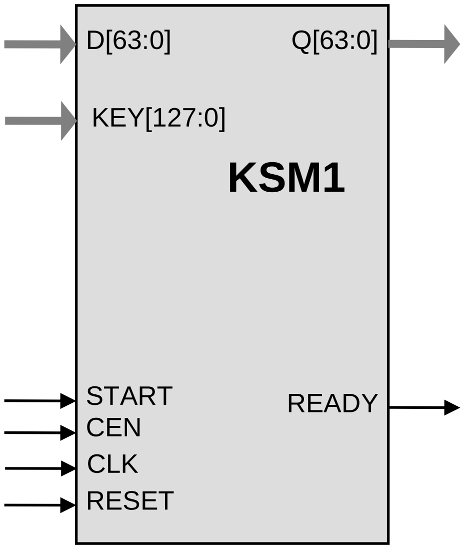
The KSM1 core implements Kasumi encryption in compliance with the ETSI SAGE specification. It processes 64-bit blocks using 128-bit key.

Basic core is very small (5,500 gates). Enhanced versions are available that support various cipher modes (ECB, CBC, OFB, CFB, CTR.

The design is fully synchronous and available in both source and netlist form. Test bench includes the Kasumi test vectors.

KSM1 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

Encryption using the Kasumi Block Cipher Algorithm

Since all practical uses of Kasumi utilize only the encryption operation, decryption is not part of the core

High throughput: up to 3 Gbps in 65 nm process

Small size: from 5.5K ASIC gates, 289 Xilinx slices, 617 Altera ALUTs

Satisfies ETSI SAGE Kasumi specification and 3GPP TS 35.202

Processes 64-bit data blocks

Use 128-bit key

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 phone communications
- 3GPP UMTS algorithms f8 and f9
- A5/3 implementation

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
D[63:0]	Input	Input Plain or Cipher Text Data
Q[63:0]	Output	Output Cipher or Plain Text Data

Function Description

A Kasumi encryption operation transforms a 64-bit data block into a block of the same size. The encryption key size is 128 bits. The block performs Kasumi encryption as defined by ETSI SAGE and 3GPP TS 35.202 version 7.

Operation

A rising input on the START port triggers the beginning of a cryptographic operation on the data D, using the KEY as key. The core then starts to process the state according to the Kasumi algorithm.

When all the rounds are completed, the READY signal is raised and the encrypted data is available on the output.

It is possible to start a new cryptographic operation as soon as the data from the previous one is output. A cryptographic operation can be aborted at any time by lowering the START signal for at least one clock cycle.

The core is fully pipelined. Loading of the new plain/cipher text data and key can be combined with outputting cipher/plain text data from the previous operation.

New key can be used for each cryptographic operation. The absence of gaps allows sustaining the throughput of 8 bits per clock.

Implementation Details

Representative synthesis results are shown below.

Technology	Max Frequency	Area	Kasumi Throughput
TSMC 65 nm G+	168 MHz	5,448 gates	1.3 Gbps
TSMC 65 nm G+	365 MHz	7,675 gates	2.9 Gbps
Xilinx Virtex 5	100 MHz	289 slices	800 Mbps
Altera Stratix 3	120 MHz	617 ALUT	960 Mbps

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) 814-0205
E-mail: info@ipcores.com
www.ipcores.com