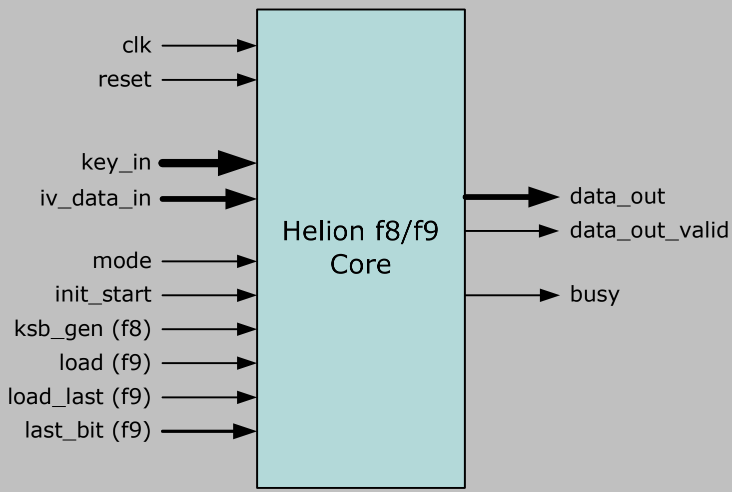
Helion Technology

DATASHEET – 3GPP KASUMI f8 and f9 Cores for Xilinx FPGA



Features

- Implement 3GPP f8 confidentiality and f9 integrity to 3GPP TS 35.201
- Both cores support KASUMI ECB mode encryption to 3GPP TS 35.202
- f8 core generates 64-bit wide keystream output data
- f9 core performs bit padding of last block and outputs 32-bit MAC-I
- Both cores support throughputs up to 800 Mbps in Virtex-6
- Ideal for use in Xilinx FPGA based GSM/EDGE and UMTS applications
- f8 core fully supports GSM A5/3 and GPRS GEA3 encryption algorithms
- Highly optimised for use in Xilinx FPGA technology

Deliverables

- Target specific netlist or fully synthesisable Verilog RTL code
- Simulation model and HDL testbench with 3GPP TS 35.204 test vectors
- Comprehensive user documentation

Overview

The Helion 3GPP f8 and f9 cores perform the confidentiality and integrity algorithms required to provide data security within the GSM/EDGE and UMTS mobile communication standards. Both algorithms are based on the KASUMI 64-bit block cipher which uses a 128-bit key. The KASUMI algorithm was designed by the Security Algorithms Group of Experts (SAGE) within ETSI, and is an optimised version of the MISTY1 block cipher originally developed by Mitsubishi Electric Corporation of Japan. Within ETSI, the f8 and f9 algorithms are now known as UEA1 and UIA1 respectively.

The cores are ideally suited to accelerating the f8 and f9 algorithms within Xilinx FPGA based GERAN and UTRAN implementations, where one or more instantiations of the cores can be used to provide 3GPP confidentiality and integrity at very high data throughputs. The f8 confidentiality core can also be used to perform the A5/3 encryption algorithm used for GSM and the GEA3 encryption algorithm used in GPRS.

Helion Technology Limited
Ash House, Breckenwood Road,
Fulbourn, Cambridge CB21 5DQ, England

Functional Description

The Helion 3GPP f8 core performs the stream cipher that generates the keystream required to implement the f8 (UEA1) confidentiality algorithm. The core must firstly be initialised by the user readying the 64-bit initial value (Count, Bearer and Direction) on the *iv_data_in* input, and the 128-bit key on the *key_in* input, before asserting the *init_start* input. Once initialisation is complete (as indicated by the *busy* output) the core may be used to generate successive keystream blocks by asserting the *ksb_gen* input. The availability of a valid keystream block on *data_out* is indicated by the assertion of *data_out_valid*.

The Helion 3GPP f9 core performs the Message Authentication Code (MAC) calculation required to implement the f9 (UIA1) integrity algorithm. When the 128-bit key input is valid, the core may be started by asserting the *init_start* input. The user application then inputs consecutive message data blocks for authentication using the *load* and *iv_data_in* inputs. At the end of the message data, coincident with the final *load*, the user indicates the presence of the last message block by asserting the *load_last* input and indicating the position of the last message bit on the *last_bit* input. The core then applies padding to the last block and completes computation of the final 32-bit MAC value. The MAC value is available on *data_out* when *data_out_valid* is asserted by the core.

Alternatively, using the *mode* input, both cores also support KASUMI ECB mode encryption.

Logic Utilisation and Performance

Unlike most FPGA core vendors, Helion is both a certified Xilinx AllianceCORE IP provider and Xilinx Alliance Program consultancy. We therefore take great care when implementing our Xilinx IP, and as a result our cores have been designed from the bottom up to be highly optimal in Xilinx FPGA technology - they are not simply based on a synthesised generic ASIC design.

Both the Helion f8 confidentiality core and f9 integrity core have been specifically designed to be highly optimal in Xilinx FPGA designs to yield a high level of functionality and performance for the logic resources used. Both cores are available in all current Xilinx FPGA technologies, please contact Helion for further details of support for device families not shown in the table below.

	f8 confidentiality			**f9 integrity**		
technology	Virtex5 -3	Spartan6 -2	Virtex6 -3	Virtex5 -3	Spartan6 -2	Virtex6 -3
logic resource	263 slices	274 slices	275 slices	285 slices	289 slices	289 slices
max clock	186 MHz	80 MHz	215 MHz	186 MHz	80 MHz	221 MHz
max throughput	700 Mbps	300 Mbps	808 Mbps	700 Mbps	300 Mbps	830 Mbps

More Information

For more detailed information on this or any of our other products and services, please contact Helion and we will be pleased to discuss how we can assist with your individual requirements.

Helion Technology Limited
Ash House, Breckenwood Road,
Fulbourn, Cambridge CB21 5DQ, England

tel: +44 (0)1223 500 924   email: info@heliontech.com
fax: +44 (0)1223 500 923   web: www.heliontech.com