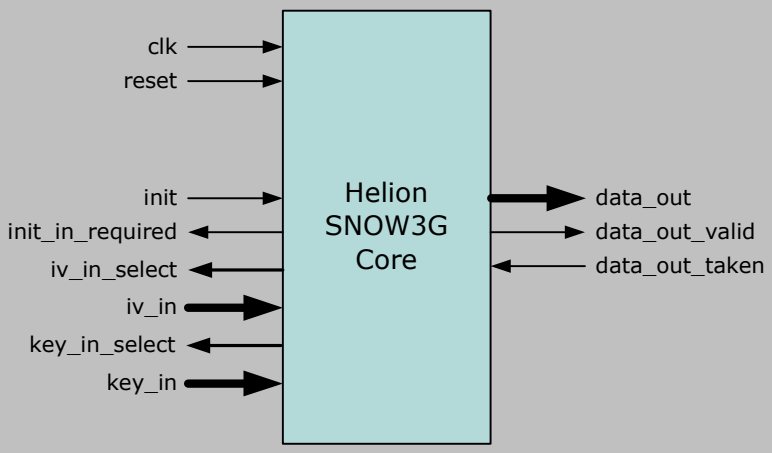
Helion Technology

DATASHEET – SNOW3G Stream Cipher Core for Xilinx FPGA



Features

- Implements SNOW3G stream cipher algorithm to 3GPP TS 35.216
- Supports UEA2 confidentiality algorithm to 3GPP TS 35.215
- Optional wrapper available to perform UIA2 integrity algorithm to 3GPP TS 35.215
- Capable of data throughputs in excess of 10 Gbps in Virtex5/6
- Ideal for use in Xilinx FPGA based UMTS and LTE applications
- Simple external interface
- 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 35.217 test vectors
- Comprehensive user documentation

Overview

The Helion SNOW3G core efficiently implements the stream cipher used as the basis for the UEA2 confidentiality algorithm and UIA2 integrity algorithm which provide data security within the 3GPP UMTS and LTE mobile communication standards. The core also fully supports the 128-EEA1 confidentiality and 128-EIA1 integrity algorithms which were introduced in 3GPP Specification Release 8, and which are identical to UEA2 and UIA2 respectively.

The core reads in the 128-bit IV and 128-bit Key and generates the Keystream words required to implement the UEA2 (or 128-EEA1) confidentiality algorithm, using only an external XOR gate. Support for the UIA2 (or 128-EIA1) integrity algorithm is also available as an option. The core is ideally suited for use in Xilinx FPGA based UTRAN and E-UTRAN implementations where it can support data throughputs up to 12 Gbps in Xilinx Virtex6 technology whilst using minimal logic resources and power.

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

Functional Description

The Helion SNOW3G core performs the stream cipher that generates the keystream words required to implement the UEA2/128-EEA1 confidentiality and UIA2/128-EIA1 integrity algorithms.

The core must firstly be initialised by the user readying the 128-bit IV (Count, Bearer and Direction) at the *iv_in* input, and the 128-bit key at the *key_in* input, before asserting the *init* input. The core then reads in the key and IV using a combination of the *init_in_required, iv_in_select* and *key_in_select* inputs.

Once SNOW3G initialisation is complete, *data_out_valid* is asserted, and the core is then capable of generating a new keystream output word on *data_out,* on every subsequent clock cycle until the core is re-initialised with new Key and IV values. The actual rate at which keystream words are generated may be regulated by the user application control of the *data_out_taken* input if required. For maximum throughput this may simply be tied high.

UEA2/128-EEA1 confidentiality may be very simply implemented using an external XOR gate to combine the keystream output from the core with the incoming plaintext or ciphertext to perform encryption or decryption.

UIA2/128-EIA1 integrity requires a Galois Hash (GHASH) function to be used in conjunction with the SNOW3G core. Helion can optionally provide a wrapper incorporating SNOW3G and GHASH which performs UIA2/128-EIA1 integrity.

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.

The Helion SNOW3G core has been specifically designed to be highly optimal in Xilinx FPGA designs to give a high level of performance whilst using the absolute minimum logic resources to minimise power. 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.

	SNOW3G		
technology	Virtex5 -3	Spartan6 -2	Virtex6 -3
logic resource	164 slices	159 slices	163 slices
max clock	366 MHz	161 MHz	415 MHz
max throughput	11712 Mbps	5152 Mbps	13280 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