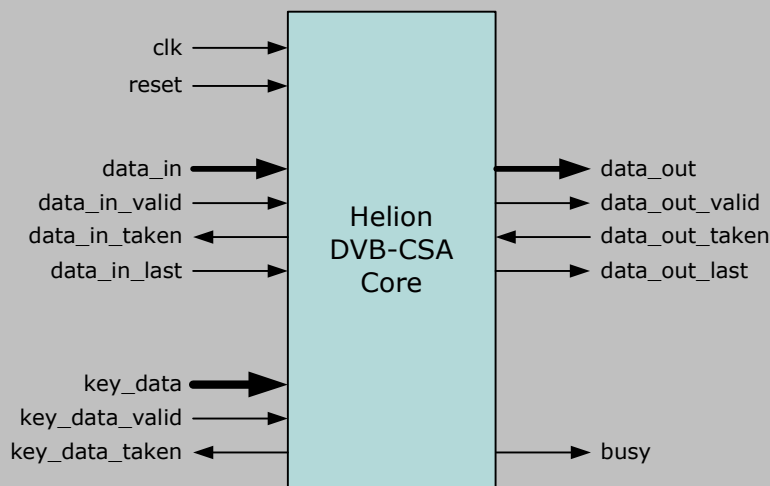# Helion Technology

FULL DATASHEET – Common Scrambling Algorithm Cores for Altera FPGA

Features

- Implements ETSI specified DVB Common Scrambling Algorithm
- Ideal for use in BISS-E and BISS Mode-1 Digital Satellite News Gathering applications
- Available as separate Scrambler and Descrambler cores for optimum system efficiency
- Internal 3-stage pipeline for optimum Scrambler data throughput
- Capable of Scrambler/Descrambler data throughputs of 400 Mbps
- Simple interfacing to user logic with separate key and data ports
- Highly optimised for use in Altera FPGA technology

Deliverables

- Target specific netlist or fully synthesisable RTL VHDL/Verilog
- VHDL/Verilog simulation model and testbench with ETSI test vectors
- Comprehensive user documentation

Overview

The Helion DVB-CSA cores implement the ETSI specified Common Scrambling Algorithm (CSA) which is used to provide the conditional access mechanism for MPEG-2 video streams for use in Pay-TV systems adopted by Digital Video Broadcasting (DVB) consortium. It has also been specified by the European Broadcasting Union (EBU) for use within Digital Satellite News Gathering (DSNG) applications, where it provides data security within the Basic Interoperable Scrambling System (BISS) Mode 1 and Mode E specifications.

Both cores have been designed especially for use in Altera FPGA technology to provide high performance combined with low logic resource utilisation. They can support DVB scrambling and descrambling applications capable of data throughputs in excess of 200 Mbps using low cost Cyclone devices.

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

Functional Description

The Helion DVB-CSA Scrambler core encrypts transport stream payloads using a two-stage process. Due to the nature of the scrambling algorithm, each complete payload must be transferred into the core by the user application before encryption can begin. As a first stage the CSA encrypts the payload using a block cipher starting at the end of the payload and working towards the start of the payload. The second stage applies a stream cipher to the output from the block cipher, which is used to further encrypt the data in the forwards direction i.e. beginning at the front and working towards the end of the partially encrypted payload.

The Helion DVB-CSA Descrambler core decrypts scrambled transport stream payloads using the reverse two-stage process to the Scrambler core. First it initialises the stream cipher and decrypts the data beginning at the start of the payload. It then applies the block cipher to the output of the stream cipher in the forward direction i.e. working from the front towards the end of the payload. This completes the descrambling process to recover the original unencrypted transport stream payload.

Both cores use a simple synchronous handshaking protocol to transfer data between the core and the user logic. A separate 64-bit key interface is used to load the CSA common key into the cores.

Logic Utilisation and Performance

Helion has a long history in high-end FPGA design, and we therefore take our FPGA implementations very seriously indeed. Our cores have been designed from the ground up to be highly optimal in Altera FPGA technology - they are not simply based on a synthesised generic ASIC design.

Both the Helion DVB-CSA Scrambler and Descrambler cores have been specifically designed to be highly optimal in Altera designs to yield high functionality for the logic resources used. Both cores are available for all current Altera FPGA technologies although they can also be provided for older technologies where addition of CSA to legacy designs is required. Please contact Helion for more details.

	——————Scrambler——————			——————Descrambler——————		
technology	Cyclone III C6	Cyclone IV C6	Stratix IV C2	Cyclone III C6	Cyclone IV C6	Stratix IV C2
logic resource	865 LEs 3 M9K	863 LEs 3 M9K	446 ALMs 3 M9K	780 LEs 1 M9K	784 LEs 1 M9K	367 ALMs 1 M9K
max clock	207 MHz	201 MHz	391 MHz	211 MHz	221 MHz	403 MHz
max throughput	223 Mbps	216 Mbps	421 Mbps	226 Mbps	236 Mbps	431 Mbps

NOTE: We are only able to license these cores to customers that have signed the ETSI Non-Disclosure Agreement and are in possession of a valid license to use the Common Scrambling Algorithm.

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