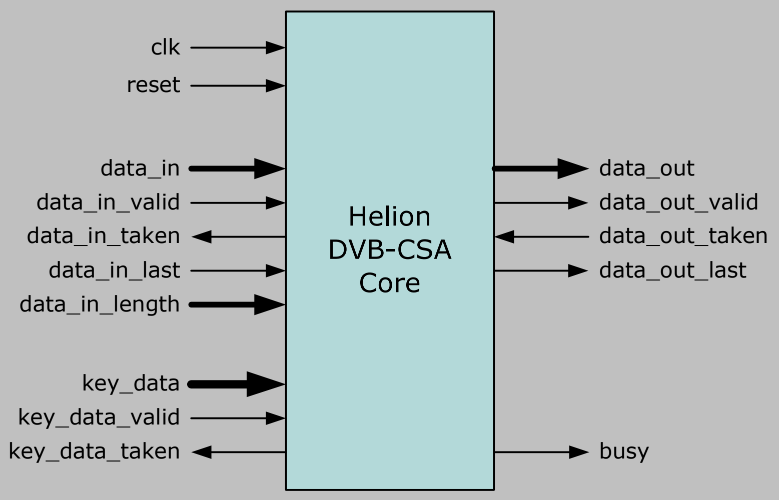
Helion Technology

FULL DATASHEET – Common Scrambling Algorithm Cores for 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 up to 400 Mbps
- Simple interfacing to user logic with separate key and data ports
- Highly optimised for use in each individual 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 each supported 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 100 Mbps using the lowest cost FPGA devices.

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

Copyright © 2007-2009 Helion Technology Limited. Revision 1.0 (22/01/2009)

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. NOTE: Helion 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.

Logic Utilisation and Performance

Helion has a long history in high-end FPGA design, and we therefore take great care when implementing our IP cores. As a result they have been designed from the ground up to be highly optimal for each individual FPGA technology - they are not simply based on a synthesised generic RTL ASIC design. The Helion DVB-CSA cores make use of the architectural features available in each FPGA technology to achieve the highest performance combined with the most efficient logic resource utilisation.

The latest logic area, performance figures, and datasheets for the Helion DVB-CSA cores in a range of different technologies are available at http://www.heliontech.com/dvb_csa.htm. Please feel free to contact us should you require further details.

About Helion

Helion is a long established British company based in Cambridge, England, offering a range of product-proven Data Security silicon IP cores backed up by our highly experienced and professional design service capabilities. Although we specialise in providing the highest performance data encryption and authentication IP, our interest does not stop there. Unlike broadline IP vendors who try to supply a very diverse range of solutions, being specialists we can offer much more than just the IP core itself.

For instance, we are pleased to be able to supply up-front expert advice on any security applications which might take advantage of our technology. Many of our customers are adding data security into their existing systems for the first time, and are looking for a little assistance with how best to achieve this. We are pleased to help with suitable advice and support where necessary, and pride ourselves in our highly personal approach.

The quality of our IP is however the main reason our customers keep coming back for more. We passionately believe that if you are buying IP, it should have been designed with the ultimate in care, crafted to achieve the ultimate performance in each target technology, and thoroughly tested to ensure compliance with any associated standards. All this comes as standard with IP from Helion.

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

Copyright © 2007-2009 Helion Technology Ltd; All rights reserved. This document contains Proprietary Trade Secrets of Helion Technology Limited; its receipt or possession does not convey any right to reproduce, disclose its contents, or to use its contents to manufacture, use, or sell anything that it may describe without the written authorisation of Helion Technology Limited. The products described in this document are subject to continuous development and all information is supplied strictly "as is" with no warranties implied or expressed and Helion Technology Limited shall not be liable for any loss or damage arising from the use of any information contained in this document.