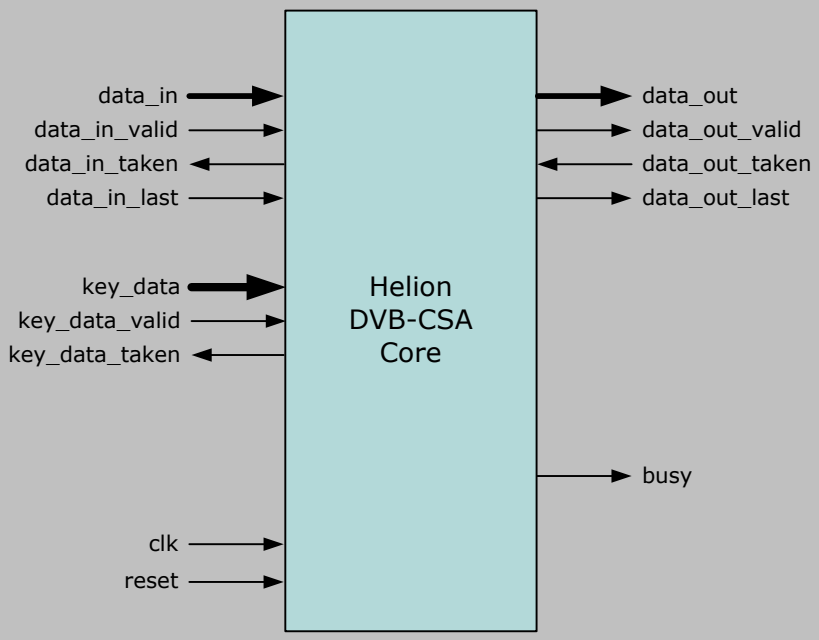
Helion Technology

PRODUCT BRIEF | **Common Scrambling Algorithm IP 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 best system efficiency
- Internal 3-stage pipeline for optimum Scrambler data throughput
- Capable of Scrambler/Descrambler data throughputs in excess of 500 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 source code
- VHDL/Verilog simulation model and testbench
- 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 the Scrambling and Descrambling cores have been carefully designed for optimal use in FPGA technology, and offer high throughput rates combined with low logic resource utilisation. They can support DVB scrambling and descrambling applications at data throughputs in excess of 200Mbps even in the lowest cost FPGA devices, and at rates over 500Mbps in the higher performance FPGA families – all whilst using only modest logic resources.

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

Functional Description

Background
The Common Scrambling Algorithm (CSA) is an ETSI specified algorithm used for providing MPEG-2 transport stream data security within Digital Video Broadcasting (DVB) applications. It uses a combination of a block cipher and a stream cipher to provide encryption and decryption whilst maintaining the size of plaintext and ciphertext; i.e. encrypted and unencrypted payloads are the same length, which is an important property in this application.

Helion split the Scrambling and Descrambling functions into separate cores, since in most applications these processes will be carried out at different places in the system – typically at each end of a unidirectional link of some kind. Thus appropriate cores can be deployed where required in the system, using the minimum of hardware resources.

How does CSA Scrambling work?
Due to the nature of the scrambling algorithm, the Helion DVB-CSA Scrambler core encrypts transport stream payloads using a two-stage process. 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 then 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 two pass nature of the algorithm clearly has an impact on the latency of encryption, but all the necessary processing is taken care of internally by the core, without any requirements on the user.

What about Descrambling?
The Helion DVB-CSA Descrambler core decrypts scrambled transport stream payloads using the reverse of the two-stage process described for 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 will recover the original unencrypted transport stream payload. Note that the latency of decryption is always much lower than that of encryption, due to the reversed order of processing through the data payload.

How do the Data and Key interfaces work?
Both cores use a simple synchronous handshaking protocol to transfer data between the core and the user logic. The data interfaces are byte-wide for simple compatibility with most existing applications. A separate 64-bit key interface is used to load the CSA common key into the cores, this width matching the size of key used.

Optional Transport Stream packet wrappers

Helion can optionally provide wrappers which instantiate the DVB-CSA cores plus a technology specific FIFO to implement MPEG Transport Stream Scrambler and Descrambler functions. Both wrappers have simple data interfaces that accept and decode 188-byte TS packets at the input, and output the resulting scrambled or descrambled 188-byte TS packets. Using these wrappers makes deployment of the CSA cores even easier and quicker for most applications.

What do they decode?
These MPEG TS wrappers use the Scrambling Control (TSC) bits within the packet header to determine whether the packet payload requires scrambling/descrambling or not, and if so, whether the odd or even key input should be used. The wrapper also examines the Transport Error flag (TEF) and Adaptation Field and Payload present bits within the header to determine what action to take.

Scrambler wrapper functionality
In the scrambler wrapper, the TSC bits determine whether encryption is applied, and if so, whether the odd or even key is used. However encryption is only applied when payload is indicated as being present, otherwise the data is passed unchanged, regardless of the state of the TSC bits. Note that the user must set the TSC bits as required on the incoming TS packet, to enable the required behaviour of the scrambler.

Descrambler wrapper functionality
In the descrambler wrapper, if a demodulator transport error is indicated, or the packet does not contain a payload, no further processing of the packet takes place, and it is passed directly to the output unchanged, irrespective of the settings of the TSC bits. If a payload is present, the TSC bits determine whether decryption is applied, and if so, whether the odd or even key is used. If descrambling occurs, the TSC bits will be reset by the wrapper to indicate that the TS packet is no longer scrambled.

Core Choice

As described above, this is extremely simple - the only core choice to be made is whether scrambling or descrambling functions are required.

Core Throughput

The tables below show the minimum number of cycles of latency and the maximum data throughput as a function of core clock frequency for the DVB-CSA cores, separately covering scrambling and descrambling operation.

version	**CSA Scrambling**	**CSA Descrambling**
TS packet length (for figures below)	184-bytes	184-bytes
min data latency	1538 clock cycles	57 clock cycles
max data throughput (Mbps per MHz)	1.08	1.06

For any specific application, a core version should be chosen that will achieve the required throughput, with an appropriate and achievable core clock frequency

Logic Utilisation and Performance

Helion cores are fully characterised in all supported FPGA types (please see overleaf for supported FPGA technologies), with specific results available for each device type and speed grade. This yields a huge amount of data, so we don't include it in this Product Brief. Please contact Helion with your vendor requirements, and we will be delighted to send the appropriate information.

For general guidance however, the typical maximum achievable clock rates in the latest fast FPGA silicon might be between ~400MHz and ~500MHz in a mid speed grade part, whilst in lower cost FPGA devices these rates may be closer to ~200MHz. These figures can be used as a starting point to determine which version of the core could be suitable for your requirements. A selection of the most popular combinations are also shown on our DVB-CSA core web pages, at http://www.heliontech.com/dvb_csa.htm.

Looking for Higher Rates?

The CSA algorithm does have certain inherent limitations in terms of the throughput it can support, due to the nature of the internal processing it requires. This makes increasing performance difficult. Hence when a single core is not sufficient, the only way forwards is to use multiple cores in parallel. The data being packetised does make this feasible.

Alternatively, if you have flexibility in terms of the encryption algorithm you are using, it may be worth looking at something based on AES. These offer more performance scalability, improved security and highly efficient implementations. Please take a look at our AES webpage at http://www.heliontech.com/aes.htm, or contact Helion for more information on faster AES based solutions.

Ordering Information

Before ordering it is necessary to decide which of our DVB-CSA cores will best fit your application. Simply decide between the **Scrambler** and **Descrambler** cores according to the function you require. In addition, you may like to consider including the optional **Transport Stream Packet Wrapper**, as described on the previous page. These decode the basic header information, and process only the parts of the payload that require it, hence simplifying deployment.

If any of the choices are unclear, or you would just like to go over the options available, we are always happy to discuss the alternatives and help select the best solution for your application.

SISVEL Licenses

IMPORTANT NOTE: We are only able to license these cores to customers that have signed the SISVEL Non-Disclosure Agreement and are in possession of a valid license to use the Common Scrambling Algorithm. This is a requirement on all users of this technology, applied by the consortium who own the rights to the algorithm, and is managed by the custodians SISVEL. Please feel free to contact Helion for more information on this requirement, or see the SISVEL CSA page at www.sisvel.com.

FPGA Technology Support

Helion has a long history in high-end FPGA design, and takes a great deal of care when implementing IP cores. As a result, these cores 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. Helion cores always make use of the architectural features available in each FPGA technology to achieve the highest performance combined with the most efficient logic resource utilisation.

Helion is an accredited IP partner with **Altera, Lattice, Microsemi (Actel)** and **Xilinx**, and supports all current and many legacy FPGA technologies from these vendors. Please feel free to contact Helion if your FPGA technology of choice is not listed here.

About Helion

Founded in 1992, Helion is a long established British company based in Cambridge, England. We offer a range of product-proven Data Security and Lossless Compression IP cores, backed by a team of highly experienced engineers, proudly developing and supporting a world-class portfolio.

Our aim is to offer our customers…

Innovation
Helion works hard to anticipate, understand and then deliver great solutions for its customers. As an example, Helion offered the world's first commercial AES core back in 2001, even before the industry had fully adopted the algorithm. This process continues unabated today, with new products in development that will lead the field.

High Performance
Helion IP is specially designed and optimised for each target technology. This means lots of work for us, but this approach yields amazing results for our customers. We always aim for the best in class performance and lowest utilisation in any given ASIC or FPGA target.

High Quality
IP should be problem free, so we always go the extra mile to ensure a smooth and trouble free integration phase for our products. We realise that our customers are putting their faith in us, and want to repay that with an outstandingly easy deployment.

Ease of Use
Helion engineers have many years of real product development experience, and so our IP is designed to be used in realistic situations. It is flexible and well thought through - the result being that it is simple to drop into your system.

See how we achieve all this by visiting our Clients page at http://www.heliontech.com/clients.htm

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
web: www.heliontech.com