DVB Common Scrambling Algorithm (Helion)

January 18, 2008 Product Specification

Helion Technology Limited

Ash House, Breckenwood Road,
Fulbourn, Cambridge CB21 5DQ, England
Phone: +44 1223 500 924
Fax: +44 1223 500 923
E-mail: helioncores@heliontech.com
URL: www.heliontech.com

AllianceCORE™ Facts	
Provided with Core	
Documentation	User Guide
Design File Formats	Xilinx netlist
Constraints Files	.ucf
Verification	Verilog test bench VHDL or Verilog simulation model
Instantiation Templates	VHDL ,Verilog
Reference Designs & Application Notes	
Additional Items	Example ModelSim scripts
Simulation Tool Used	
ModelSim PE 6.1e	
Support	
Support provided by Helion Technology Limited	

Features

- Implements ETSI DVB Common Scrambling Algorithm (DVB-CSA)
- Allows Scrambling/Descrambling of MPEG-2 Transport Streams for use in DVB Conditional Access
- Suitable for Digital Satellite News Gathering BISS Mode 1 and Mode E applications
- Available as separate Scrambler and Descrambler cores for maximum system flexibility
- Simple 8-bit data and 64-bit keying interfaces
- Highly optimised for efficient implementation in Xilinx FPGA
- Offers support for high data rates
  - up to 200Mbps in low-cost Spartan-3 devices
  - up to 400Mbps in high-end Virtex-5
- Available for all Xilinx FPGA technologies (including legacy device families)
- Available under terms of the SignOnce IP License

Table 1: Example Implementation Statistics – DVB-CSA Descrambler Core for Xilinx® FPGAs

Family	Example Device	Fmax[1] (MHz)	Slices	IOB[2]	GCLK	BRAM	MULT/ DSP48	DCM / CMT	MGT	Design Tools
Spartan™-3	XC3S1500-5	185	360	98	1	1	0	0	N/A	ISE™ 9.2.03i
Spartan™-3E	XC3S1600E-5	183	377	98	1	1	0	0	N/A	ISE™ 9.2.03i
Virtex™-4	XC4VLX25-11	296	371	98	1	1	0	0	N/A	ISE™ 9.2.03i
Virtex™-5	XC5VLX30-3	374	178	98	1	0	0	0	N/A	ISE™ 9.2.03i

Notes:

1) Fmax is quoted assuming all core inputs are sourced from flip-flops, and all core outputs drive flip-flops; this has been done to best represent real applications.

2) Assuming all core I/Os and clocks are routed off-chip

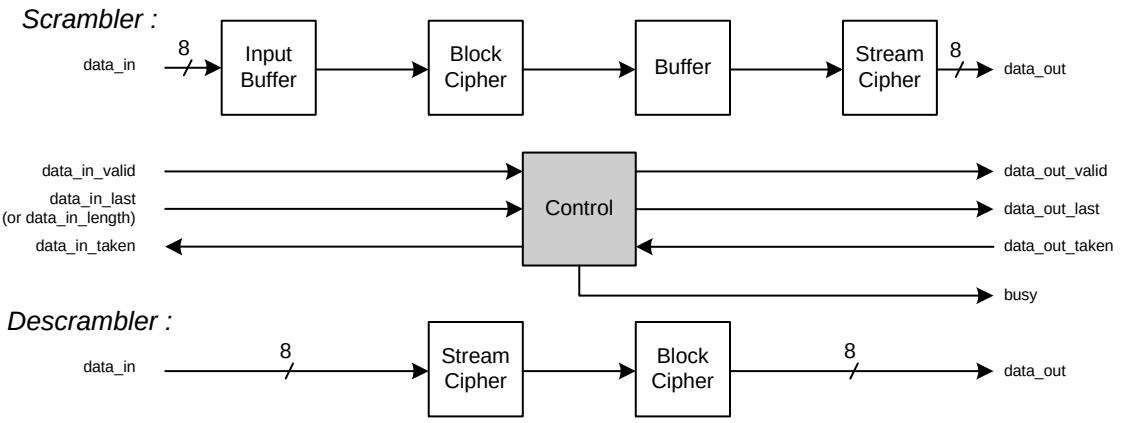

Figure 1: Helion DVB-CSA Scrambler and Descrambler Block Diagram

Table 2: Example Implementation Statistics – DVB-CSA Scrambler Core

Family	Example Device	Fmax[1] (MHz)	Slices	IOB[2]	GCLK	BRAM[3]	MULT/ DSP48	DCM / CMT	MGT	Design Tools
Spartan™-3	XC3S1500-5	198	393	91	1	3	0	0	N/A	ISE™ 9.2.03i
Spartan™-3E	XC3S1600E-5	189	395	91	1	3	0	0	N/A	ISE™ 9.2.03i
Virtex™-4	XC4VLX25-11	322	393	91	1	3	0	0	N/A	ISE™ 9.2.03i
Virtex™-5	XC5VLX30-3	364	193	91	1	2	0	0	N/A	ISE™ 9.2.03i

Notes:

1) Fmax is quoted assuming all core inputs are sourced from flip-flops, and all core outputs drive flip-flops; this has been done to best represent real applications.

2) Assuming all core I/Os and clocks are routed off-chip

3) For Virtex-5™ the number of Block RAMs given is for RAMB18 primitives

Applications

The Helion DVB-CSA scrambler and descrambler cores are intended for use in implementing the DVB Conditional Access specification (DVB-CA) commonly used in Pay-TV systems, as well as BISS Mode 1 and BISS Mode E implementations used for Digital Satellite News Gathering applications.

General Description

The Helion DVB-CSA cores efficiently implement the ETSI specified Common Scrambling Algorithm in all Xilinx FPGA technologies. The cores are capable of scrambling and descrambling MPEG-2 Transport Stream payloads at data throughputs up to 400 Megabits per second (Mbps) in Xilinx FPGA.

Functional Description

Figure 1 is a block diagram showing the datapath of the Helion DVB-CSA Scrambler and Descrambler cores. Note that the control block is shown only to illustrate the input and output control interfaces and is

functionally different for the two cores. For clarity, the parallel key interface is not shown, but the 64-bit key is used by both the stream and block ciphers.

Due to the asymmetrical nature of the Common Scrambling Algorithm, the descrambling process is simpler than the scrambling process. This is because the scrambler has to operate on complete payloads and hence requires internal Block RAM buffers to store intermediate cipher results. However, the pipelining introduced by the buffering allows scrambling of up to three different payloads to be in progress at any one time, thus maximising the scrambler data throughput.

The scrambling process consists of applying a block cipher followed by a stream cipher to the input data to produce a scrambled payload. For DVB-CA applications, the user simply appends a MPEG-2 packet header before forwarding the scrambled payload.

The descrambling process consists of applying the ciphers in the reverse order i.e. the stream cipher followed by the block cipher to produce a descrambled payload. For DVB-CA applications, the user simply appends a MPEG-2 packet header before forwarding the descrambled payload.

Data Throughput Capability

The Helion CSA Scrambler and Descrambler cores have a maximum data throughput of approximately one bit per clock for a typical 184 byte MPEG-2 Transport Stream payload i.e. for a 100MHz clock the maximum data throughput would be approximately 100 Mbps. For smaller payloads the maximum data throughput is slightly reduced due to per-payload overheads. Please contact Helion for further details.

Core I/O Signals

The core signal I/O have not been fixed to specific device pins to provide flexibility for interfacing with user logic. Descriptions of all signal I/O are provided in Table 4.

Table 4: Core I/O Signals.

Signal	Width	Signal Direction	Description
clk	1	Input	Master clock
reset	1	Input	Master asynchronous reset; 1 = “reset”
Control & Status			
busy	1	Output	Core is busy; 1 = “busy”
Key interface			
key_data	64	Input	Key input
key_data_valid	1	Input	Key input valid
key_data_taken	1	Output	Key input taken by core
Input data interface (8-bit data & handshaking)			
data_in	8	Input	Data input byte
data_in_length	8	Input	Data input length in bytes (descrambler only)
data_in_last	1	Input	Data input last byte marker (scrambler only)
data_in_valid	1	Input	Data input valid
data_in_taken	1	Output	Data input taken by core
Output data interface (8-bit data & handshaking)			
data_out	8	Output	Data output byte
data_out_last	1	Output	Data output last byte marker
data_out_valid	1	Output	Data output valid
data_out_taken	1	Input	Data output taken from core

Verification Methods

The Helion CSA cores have been thoroughly verified in simulation using ETSI supplied test vectors.

Recommended Design Experience

Users should be familiar with HDL methodology and Xilinx design flows including VHDL/Verilog component instantiation, synthesis, implementation and simulation.

Ordering Information

The use of the Common Scrambling Algorithm is licenced by the Electronic Telecommunications Standards Institute (ETSI) on behalf of the companies which originally developed the algorithm. Accordingly, the Helion CSA cores can only be provided to users that have already obtained a licence to use the DVB CSA algorithm. Details of the relevant licence and non-disclosure agreements to permit the use of CSA are available from the ETSI website (www.etsi.org).

This product is available directly from Xilinx AllianceCORE member Helion Technology under the terms of the SignOnce IP License. Please contact Helion Technology for pricing and additional information about this product. Contact information for them is on the front page of this datasheet. To learn more about the SignOnce IP License program, contact Helion Technology or visit the web:

Email: commonlicense@xilinx.com
URL: www.xilinx.com/ipcenter/signonce

Related Information

ETSI DVB CSA algorithm home page :
http://www.etsi.org/WebSite/OurServices/Algorithms/dvbalgorithms.aspx

Xilinx Programmable Logic

For information on Xilinx programmable logic or development system software, contact your local Xilinx sales office, or:

Xilinx, Inc.
2100 Logic Drive
San Jose, CA 95124
Phone: +1 408-559-7778
Fax: +1 408-559-7114
URL: www.xilinx.com