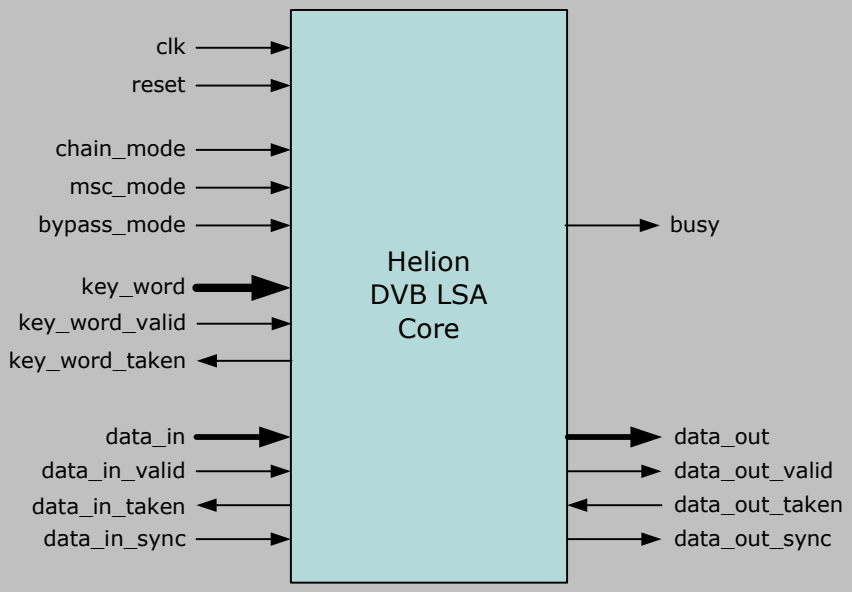
Helion Technology

FULL DATASHEET – DVB Local Scrambling Algorithm Cores for Altera FPGA



Features

- Implements DVB Local Scrambling Algorithm as required to provide content protection within DVB-CPCM
- Provides MPEG-2 Transport Stream packet scrambling/descrambling for DVB-CPCM compliant systems
- Supports both AES CBC and RCBC chaining modes
- Supports both MDI and MDD "Must Stay Clear" Data modes
- Bypass mode provides seamless handling for unscrambled PIDs
- Available as separate Scrambler and Descrambler cores
- Highly optimised for use in Altera FPGA technology

Deliverables

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

Overview

The Helion DVB LSA Scrambler and Descrambler cores implement the Local Scrambling Algorithm as specified to provide MPEG-2 Transport Stream packet security within DVB Content Protection and Copy Management (DVB-CPCM) compliant systems. Both cores provide all operations required to scramble or descramble MPEG-2 TS packets, including IV generation using either MSC Data Independent (MDI) or MSC Data Dependent (MDD) mode, and payload protection using either AES-CBC or AES-RCBC cipher chaining modes.

Both Helion LSA cores have been designed especially for use in Altera FPGA technology to provide high performance combined with the lowest possible logic resource utilisation. They can support DVB-CPCM content scrambling and descrambling applications capable of data throughputs in excess of 200 Mbps using even the lowest cost Cyclone family devices.

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

Functional Description

Both Helion LSA cores use a simple synchronous handshaking protocol using data valid and taken signals to transfer 188-byte Transport Stream (TS) packets at their byte-wide data input and output interfaces. A sync signal is used to indicate the presence of the TS packet sync byte (47 hex) at either interface. As soon as the sync byte is accepted at the input to the core, the busy output is asserted to indicate TS packet scrambling or descrambling is in progress. Only when the 188th output byte is successfully transferred to the user application is the busy output de-asserted to indicate that the core is ready to process the next packet.

The TS packet header and adaptation fields are never scrambled, and so are passed through the core directly from input to output. However, when MDD mode is selected (by the user serting the *msc_mode* input to high) they are used to generate the Initialisation Vector (IV) used to scramble or descramble the TS packet payload. A further control input, *chain_mode*, selects either the AES-CBC or AES-RCBC cipher chaining modes for this task.

For maximum system efficiency, the *bypass_mode* input allows PIDs which do not require scrambling or descrambling (as a result of user PID filtering) to be handled seamlessly within the user application. In bypass mode, the packet is passed directly through the core without any scrambling or descrambling of the payload taking place.

A separate 32-bit key interface is used to load the 128-bit Key Encryption Key (KEK) into the core when it is not busy.

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 LSA Scrambler and Descrambler cores have been specifically designed to be highly optimal in Altera FPGA designs to yield high functionality and performance for the logic resources used. Both cores are available for all current Altera FPGA device families and the table below shows some typical resource and performance figures for each core. Please free free to contact Helion if you require typical figures for any other device family or speed grade.

	Scrambler			**Descrambler**		
technology	Cyclone II C6	Cyclone III C6	Stratix II C3	Cyclone II C6	Cyclone III C6	Stratix II C3
logic resource	1245 LEs 6 M4Ks	1249 LEs 6 M9Ks	574 ALMs 3 M4Ks/6 M512s	1938 LEs 9 M4Ks	1943 LEs 9 M9Ks	886 ALMs 6 M4Ks/6 M512s
max clock	149 MHz	182 MHz	236 MHz	125 MHz	161 MHz	205 MHz
max throughput *Chain mode = CBC* *MSC mode = MDI* *Payload =184 bytes*	334 Mbps	408 Mbps	530 Mbps	270 Mbps	348 Mbps	443 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