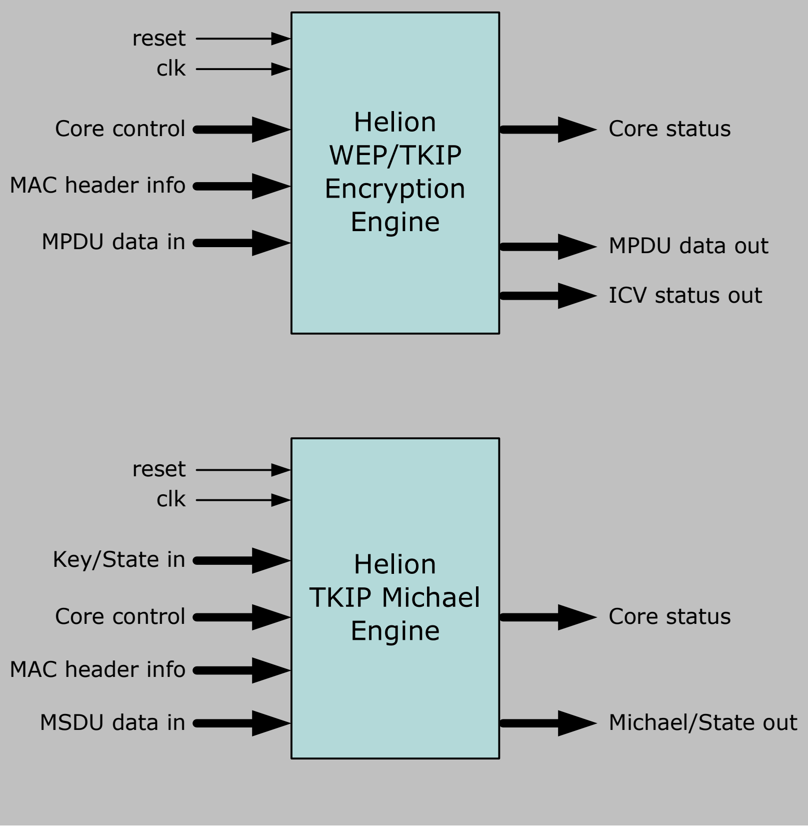
Helion Technology

FULL DATASHEET – 802.11i Wireless Security Cores for Xilinx FPGA



Features

- Implements WPA™ security protocol according to IEEE 802.11i standard
- Standalone WEP/TKIP encryption core intended to work at MPDU level
- WEP/TKIP encryption core supports key mix processing as well as MPDU payload encryption/decryption
- Standalone TKIP Michael authentication core intended to work at MSDU level
- TKIP Michael core has optional support for mid-message state unload/reload
- Supports high data throughputs
- Highly optimised for use in Xilinx FPGA technologies

Deliverables

- Target specific netlist or fully synthesisable RTL VHDL/Verilog
- VHDL/Verilog simulation model and testbench
- Comprehensive User documentation

Overview

These high performance cores have been designed to provide hardware acceleration of the underlying 802.11 WPA™ security algorithms, which in combination with the Helion AES-CCM core family, may be used to implement a full 802.11i WPA2™ security solution very efficiently in Xilinx FPGA. The security processing is split into two parts, since they are likely to be required at different points within the MAC subsystem.

The Helion WEP/TKIP Encryption engine is a standalone high-speed processing core which is designed to encrypt and decrypt 802.11 MPDU data, based on an underlying ARC4 stream cipher. It includes all the defined keymix processing as well as the MPDU payload encryption/decryption functionality.

The Helion TKIP Michael engine is a standalone high-speed processing core which is designed to accept 802.11 MSDU data and use it to generate a compliant “Michael” authentication tag. The Michael tag is typically appended to an outgoing MSDU for encryption, or compared with a decrypted incoming tag for authentication checking.

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

General Description - WEP/TKIP Encryption Core

To start processing for a new MPDU, the MAC header information must first be loaded into the core. This is used by the core at the start of processing only to generate the next WEP seed, and so can be loaded whilst the previous MPDU payload data is still being processed. A status output from the core indicates when it is safe to load the MAC header information for the next MPDU.

Once the MAC header information has been loaded, the core is ready to start processing the MPDU payload data. A process start is requested by the external logic, which at the same time must present a valid temporal key along with an indication of the WEP/TKIP mode, WEP keysize, and encrypt/decrypt mode to the core.

After the processing has started, and after a delay whilst the internal WEP seed is generated and initialised, the engine will be ready to accept MPDU payload data over its byte-wide interface. This is indicated by the core asserting the data ready output, which indicates that the next MPDU payload data byte may be loaded by the external logic, when available.

At the end of the MPDU payload, the external logic must indicate to the core when the last payload data byte is being loaded by asserting the last payload byte flag. This places the core into its completion cycle, which will either generate a suitable ICV in encrypt mode, or will check the received ICV and indicate pass or fail status in decrypt mode.

General Description - TKIP Michael Authentication Core

To start processing a new MSDU, the MAC header information must first be loaded into the core. This is used by the core at the start of processing only, and so can be loaded whilst the previous MSDU payload data is still being processed. A status output from the core indicates when it is safe to be load the MAC header information for the next MSDU.

Once the MAC header information has been loaded, the core is ready to start processing the MSDU payload data. A process start is requested by the external logic, which at the same time must present a valid Michael key to the core. This will start the processing of the MSDU, initially using the previously loaded header information. Some time after processing has started, the core will be ready to accept MSDU payload words via a 32-bit data port, as indicated by the core asserting its data ready output. When this is asserted, the next MSDU payload word may be loaded by the external logic when available.

At the end of the MSDU payload, the external logic must indicate to the core that the last payload data word is being loaded by asserting the last payload word flag along with an index value which indicates the number of valid bytes in the final word. This will put the engine into its completion cycle, which will result in the generation of a final 64-bit Michael result. When all processing is complete, the core asserts the valid status output to indicate that the Michael result on the output port is valid.

The TKIP Michael core also supports context unloading and reloading at 32-bit MSDU payload boundaries, so that a complete MSDU does not necessarily have to be processed in one continuous process.

Logic Utilisation and performance

	WEP/TKIP core			**TKIP Michael core**		
technology	Spartan3 -5	Virtex4 -11	Virtex5 -3	Spartan3 -5	Virtex4 -11	Virtex5 -3
logic resource	499 slices 2 RAMB16	554 slices 2 RAMB16	238 slices 2 RAMB18	260 slices	271 slices	126 slices
max clock	120 MHz	163 MHz	222 MHz	188 MHz	308 MHz	348 MHz
throughput (2k byte payload)	290 Mbps	395 Mbps	535 Mbps	650 Mbps	1050 Mbps	1200 Mbps

The tables above cover the Helion WEP/TKIP encryption and the Helion Michael Authentication cores, each targeting three of the most popular Xilinx device families. Note that full support is available for all Xilinx families (both old and new) – full details are available from Helion on request.

Ordering Information

The Helion WEP/TKIP Encryption and Michael Authentication cores are available to support almost all Xilinx FPGA device families, so the main decision at time of order is what technology should be supported. The IP cores are usually delivered in the form of technology specific netlists together with a choice of VHDL or Verilog simulation models, so knowledge of device type plus your choice of HDL language is all that is required at time of order.

Helion AES-CCM IP cores for WPA2™

For a fully compliant WPA2™ solution, the Helion WEP/TKIP Encryption and Michael Authentication cores could be teamed up with one of Helion's highly efficient AES-CCM cores. Whereas the cores described in this datasheet offer support for the legacy WPA™ security function, the later WPA2™ standard makes use of the more secure AES-based CCM mode.

Helion offer a suite of AES-CCM cores which have been designed to be extremely area efficient in Xilinx FPGA, and offer full compliance with the requirements of the IEEE 802.11i standard. These cores are available in a choice of versions offering differing area/throughput balances, so the user can choose the most appropriate for their application. Please contact Helion directly for more information on these solutions.

About Helion

Founded in 1992, Helion is a well established British company based in Cambridge, England, offering a range of product-proven Data Security IP cores backed up by 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.

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.

In addition, our Design Services team have an impressive track record in the development of real security products for our customers; we are proud to have been involved in the design of numerous highly acclaimed security products. This knowledge and experience is fed back into our IP cores, to ensure that they are easy to integrate into real systems, and perform appropriately for real engineering applications.

Helion is also a member of the Xilinx AllianceCORE IP program, and a certified Xilinx Alliance Partner. We therefore take our Xilinx implementations very seriously indeed. Our cores have been designed from the ground up to be highly optimal in Xilinx FPGA; they are not simply based on a generic ASIC design like much of the competition.

Most Helion IP cores make use of Xilinx-specific architectural features; in fact in many cases we build-up custom internal logic structures by hand, in order to achieve the very highest performance and most efficient logic resource utilisation. The benefits of this dedicated approach can be clearly demonstrated by direct comparison between Helion data security IP cores and the equivalents from other vendors.

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