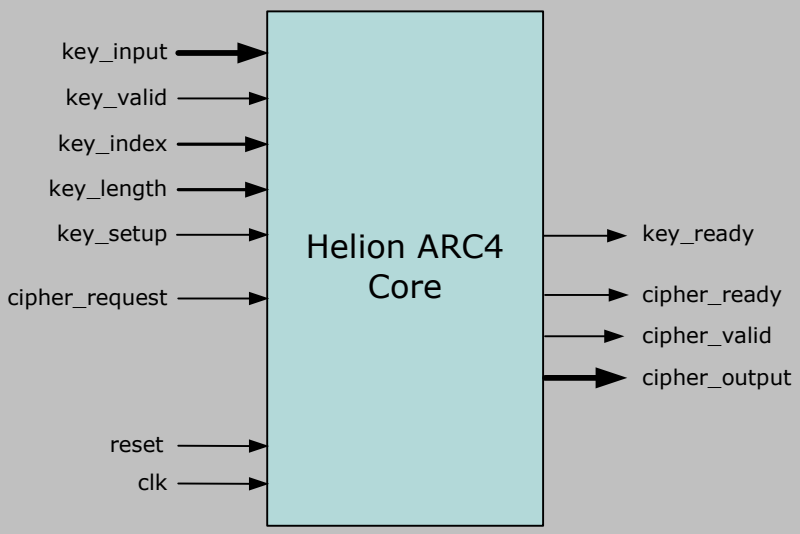
Helion Technology

FULL DATASHEET – ARC4 Core for Xilinx FPGA



Features

- Implements ARC4 stream cipher algorithm
- Fully compliant with the requirements of 802.11i WPA™ (WEP/TKIP) and SSL/TLS
- High speed operation – processes at a rate of 3 clocks per data byte
- Supports variable length keys up to 16 bytes long
- Efficient re-keying to minimise effective key setup time
- Simple external interface
- Highly optimised for use in Xilinx FPGA technologies

Deliverables

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

Overview

The Helion ARC4 core implements the Alleged RC4 stream cipher algorithm. The RC4™ algorithm itself was developed by Ron Rivest in 1987 and was originally a trade secret of RSA Security. However, a description of the algorithm became widely available on the Internet in 1994 and so the algorithm is no longer considered a trade secret, although the name RC4™ itself is still trademarked. Legal third party implementations are therefore often referred to as Alleged RC4™, which is usually abbreviated to ARC4.

The Helion ARC4 core generates a byte-wide keystream which is used to perform encryption and decryption when XOR'ed with either plaintext or ciphertext. It supports variable length key sizes of up to 16 bytes long. Applications include hardware implementations of the WEP and WPA™ 802.11i wireless security protocols, as well as TLS/SSL (Transport Layer Security, formerly Secure Sockets Layer) applications.

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

Operation, Logic Utilisation and Performance

Initially the key is loaded into the core using the key_valid, key_input, and key_index inputs. The key_length input indicates the size of the key in bytes. Once the key has been loaded the user starts the key initialisation process by asserting key_setup.

The core asserts the key_ready output when initialisation is complete, whereupon the user is able to request generation of keystream bytes using the cipher_request input. Using an external byte-wide XOR function the keystream may be used to perform either encryption or decryption at any rate up to one byte per three clocks.

The table opposite shows the logic resource and maximum data throughput for the core in popular Xilinx device families. Note that this core is also available to support most Xilinx technologies both past and present.

	ARC4		
technology	Spartan3 -5	Virtex4 -11	Virtex5 -3
logic resource	87 slices 1 RAMB16	87 slices 1 RAMB16	35 slices 1 RAMB18
max clock	111 MHz	181 MHz	244 MHz
throughput	296 Mbps	482 Mbps	650 Mbps

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