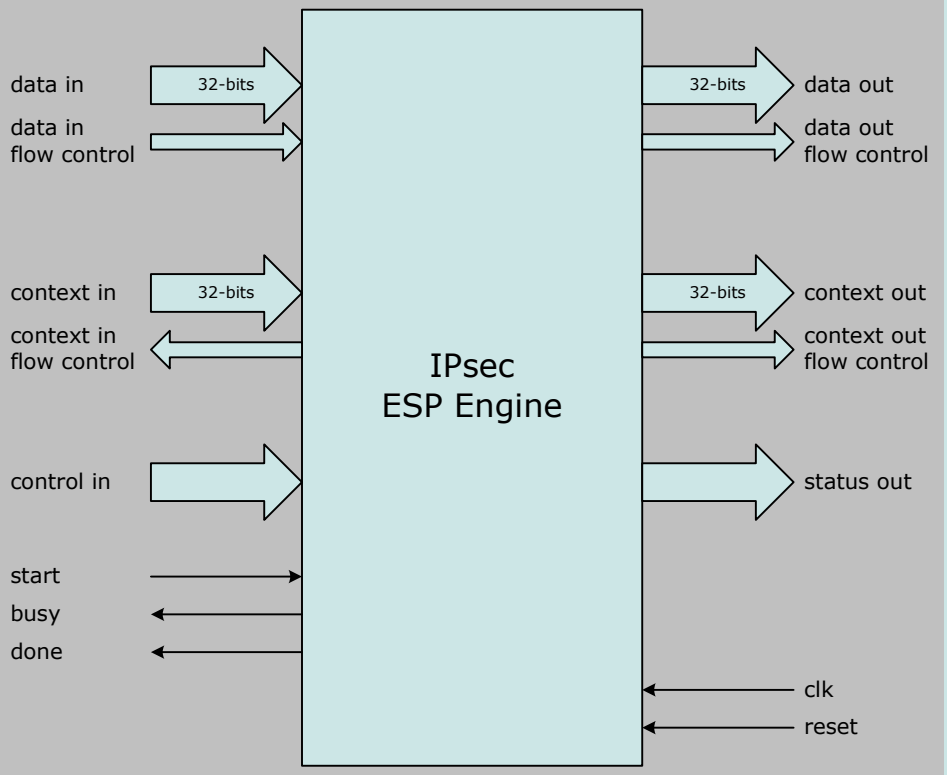
Helion Technology

PRODUCT BRIEF | **IPsec ESP IP core for FPGA**



Features

- Performs hardware acceleration of IPsec ESP protocol to RFC 4303
- Fully configurable to support all mandatory and proposed ESP-v3 confidentiality and integrity algorithms
- Suitable for use in IPv4 and IPv6 IPsec Transport and Tunnel mode applications
- Implements Extended (64-bit) Sequence Number for IKEv2 support
- Supports all ESP security service combinations
- Supports insertion of padding for Traffic Flow Confidentiality (TFC)
- Performs automatic ESP padding generation and checking
- Supports Gigabit/sec throughputs

Deliverables

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

Overview

Built on the success of Helion's industry proven cryptographic IP cores, the Helion ESP Engine provides hardware acceleration of the key cryptographic algorithms and packet processing required by the IPsec Encapsulating Security Payload (ESP) protocol. Its modular architecture provides the flexibility to support only those cryptographic algorithms required for a particular application to provide the optimum logic area and performance trade-off.

The Helion ESP Engine is suitable for use in securing both IPv4 and IPv6 IPsec traffic using either Transport or Tunnel mode operation. It supports all mandatory and proposed ESP-v3 confidentiality and integrity algorithms including **TripleDES-CBC**, **AES-CBC**, **AES-CTR**, **HMAC-SHA-1-96**, and **AES-XCBC-MAC-96**, as well as many optional algorithms such as the **AES-CCM** and **AES-GCM** combined mode algorithms. In addition to cryptographic acceleration, the Engine also performs mandatory ESP padding generation and checking in accordance with RFC4303 and fully supports Traffic Flow Confidentiality (TFC) padding generation.

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

Functional Description

Background
The Helion ESP Engine is designed to interface easily into a system datapath utilising external packet data FIFOs in a typical IPsec application. Data flow is controlled automatically by the ESP Engine using the number of data words available in the input FIFO, and the amount of free space available in the output FIFO, combined with the availability of the internal processing resources.

Security Association Context
A separate memory mapped context interface provides a means for the ESP Engine to access the Security Association (SA) information which must be provided for each packet to be processed by the external host that implements the IPsec Security Policy. The Security Association context includes all information required to provide ESP confidentiality and integrity services for the packet; cryptographic keys and IVs, ESP packet header SPI and Sequence Number fields etc.

In Operation
Once the appropriate context has been set up for the next packet by the host, the ESP Engine may be started. At this point a number of "per-packet" control inputs to the core (including ESP security service type, packet length and direction) are sampled, and loading of the context into the core will commence as the Engine pre-processes Keys and IVs for the cryptographic algorithms. Once pre-processing is complete, the Engine will commence with encryption/decryption of the input packet as it arrives at its input interface, before forwarding the resulting packet data to the output interface.

Atomic Packets
Each packet is processed separately with no overlap. The external control of the ESP Engine uses a simple "start", "busy" and "done" sequence with status outputs provided. The status outputs are guaranteed valid on assertion of the done flag, and indicate the success or otherwise of the ESP packet processing including padding checking, ICV integrity checking, and the output packet length in bytes.

ESP Engine Usage

Taking as an example a user application implementing a typical Virtual Private Network (VPN) comprising an IPsec security gateway between a local private network and an open public network using tunnel mode:

For outbound packets - the ESP Engine performs all processing required to convert the outbound IP packet from the local private network into an ESP packet. The next layer within the user application then appends an outer IP header prior to the packets transmission onto the public network.

For inbound packets - the ESP Engine performs all processing required to convert the inbound ESP packet from the public network into an IP packet ready for forwarding to the local private network. In the process, the ESP Engine detects and reports any auditable events such as integrity check or padding failures to the user application.

The Helion ESP Engine can be used either standalone or in a load sharing arrangement where multiple ESP engines are used in parallel to provide ESP processing for IPsec applications capable of handling multi Gigabit per second data rates.

What does the ESP Engine not do?

The Helion ESP Engine is ideal for performing hardware acceleration of the key ESP protocol and cryptographic algorithms at the heart of any IPsec implementation. However, many of the protocol layers of IPsec do not map well to direct hardware implementation and are not required by all applications. As such these are best performed either wholly in software, or as an application specific combination of software and hardware. With this in mind there are a few IPsec requirements that the Helion ESP Engine does not perform:

- The Internet Key Exchange (IKE) which is a separate IPsec protocol used for the establishment and maintenance of IPsec Security Associations including the generation and exchange of suitable cryptographic IV, Nonce and Keys
- Any IPsec Database functions - Security Policy Database (SPD), Security Association Database (SAD) and Peer Authentication Database (PAD)
- The Anti-replay detection service for inbound packets
- Reassembly of inbound IP packet fragments, IP traffic header processing, or handling of ICMP traffic

HELION

ESP Engine Options

The Helion ESP Engine has been designed to be extremely flexible in order to offer a number of options to the user. Its modular architecture allows any combination of ESP confidentiality, integrity and/or combined mode algorithms to be efficiently implemented. This means it can be tailored to support only the ESP security algorithms required by your application and the modules matched closely to your performance goals; optimising device area and power.

As an example, the ESP Engine is available in versions with either high rate or low rate AES modules; allowing the performance and logic area to be ideally matched to your IPsec data rate requirement, be that a few Mbps or tens of Gbps. It can also be supplied in configurations that support optional extensions to the mandatory and proposed ESP algorithms, for example the NSA SuiteB IPsec extensions (RFC 4869) e.g. **AES-CBC**, **AES-GCM**, **AES-GMAC**, **HMAC-SHA-256**, and **HMAC-SHA-384**.

As standard the Helion ESP Engine performs both inbound and outbound packet processing. However, it can also be supplied in inbound-only or outbound-only versions. For certain configurations separate inbound and outbound engines can provide 2x the data rate of a single engine without using 2x the logic area. The ability to use separate unidirectional engines is also more efficient where physical separation of inbound and outbound traffic is a requirement.

The ESP Engine is configurable for all current IPsec ESP algorithms and easily extensible to support any future security algorithm requirements without the need for board level changes, e.g. the new SHA-3 hashing algorithm, something that current ASSPs cannot offer.

Core Throughput

IPsec ESP Core

Confidentiality Algorithm	Integrity Algorithm	Throughput (Mbps/MHz) 1536-byte packets
AES-CBC-128 (Hi rate)	AES-XCBC-MAC	9.78
AES-CBC-128 (Hi rate)	HMAC-SHA-1	5.18
AES-CBC-128 (Lo rate)	AES-XCBC-MAC	2.49
AES-CBC-128 (Lo rate)	HMAC-SHA-1	2.38

This table shows the maximum data throughput for an unencapsulated packet of length 1536-bytes, as a function of core clock frequency, for a selection of popular Confidentiality and Integrity algorithm pairs. For a given clock frequency, the maximum data throughput is dependent on the selected security algorithms, the packet length, and the throughput of the chosen cryptographic modules.

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

It is also important to take into account the inevitable per-packet overheads which may be incurred, which obviously become most dominant for shorter packet sizes. Full data on maximum supported frame rates with short packets is available on request from Helion.

Remember also that usable clock frequencies will depend on the exact FPGA type and speed grade being used. Please see below for guidance on this.

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 ~250MHz to ~300MHz in a mid speed grade part (depending on the exact version and device), whilst in lower cost FPGA devices this range may be closer to ~100MHz to ~150MHz. 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 IPsec ESP core web pages, at http://www.heliontech.com/ipsec.htm.

Ordering Information

Before ordering it is necessary to decide which confidentiality and integrity algorithms you want to support, and for any AES requirements, performance level and key size support is required. The other basic decision to be made is whether you need combined or separate inbound and outbound processing.

If some of these 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.

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.

ALTERA | LATTICE SEMICONDUCTOR | Microsemi | XILINX ALL PROGRAMMABLE ALLIANCE PROGRAM CERTIFIED MEMBER

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
fax: +44 (0)1223 500 923 web: www.heliontech.com