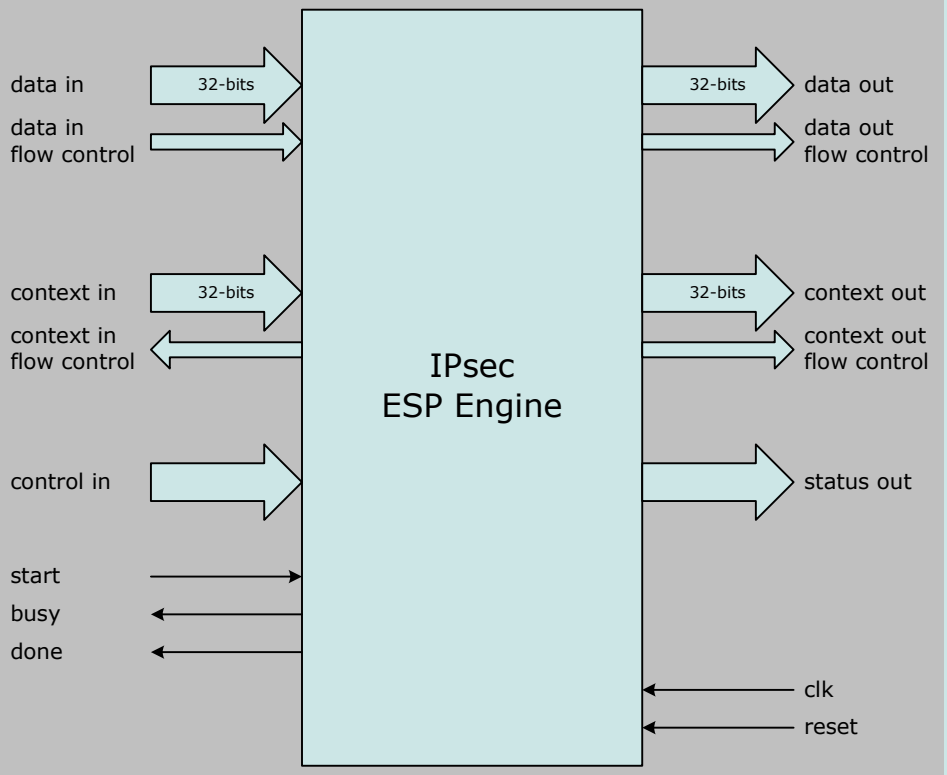
Helion Technology

DATASHEET - IPsec ESP Engine for Altera 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 VHDL 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

Copyright © 2004-2010 Helion Technology Limited. Revision 1.2 (14/07/2010)

Functional Description

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. A separate memory mapped context interface provides a means for the ESP Engine to access the Security Association (SA) information which must be provided 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.

Once the context has been setup by the host the ESP Engine may be started. At this point a number of per packet control inputs (including ESP security service type, packet length and direction) are sampled and loading of the context will commence as the Engine pre-processes Keys and IVs for the cryptographic algorithms. Once pre-processing is complete, the Engine will encrypt/decrypt the input packet as it arrives at its input interface before forwarding the resulting packet to the output interface.

External control of the ESP Engine uses a simple start, busy and done interface with status outputs. The status outputs are guaranteed valid on assertion of done 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 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, including configurations that support 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 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. Helion will be fully supporting the new SHA-3 hashing algorithm when the standard is published in 3Q 2012, something that current ASSPs cannot offer.

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.

HELION

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

Logic Utilisation and Performance

The Helion ESP Engine makes extensive use of Altera-specific architectural features in order to achieve high performance and extremely efficient logic resource utilisation. It can be configured at time of order to offer any combination of confidentiality and integrity algorithms. Various performance options are available which allow throughput and area to be matched to the user application requirements.

The tables below shows typical logic area and maximum performance figures for two ESP Engine configurations containing high rate AES modules; the first supporting **AES-CBC** and **AES-CTR** confidentiality algorithms with the **HMAC-SHA-1-96** integrity algorithm; the second supporting **AES-CBC** and **AES-CTR** confidentiality algorithms with the **AES-XCBC-MAC-96** integrity algorithm. The maximum data throughput figures shown are for an ESP security service with both data confidentiality and integrity for a 1536 byte unencapsulated packet length.
NB. For a given clock frequency, the maximum data throughput is dependent on the selected security service, the packet length, and the maximum throughput of the chosen cryptographic modules.

	——AES-CBC/CTR + HMAC-SHA-1——			**—AES-CBC/CTR + AES-XCBC-MAC—**		
technology	Arria II GX C4	Stratix III C2	Stratix IV C2	Arria II GX C4	Stratix III C2	Stratix IV C2
logic resource	3334 ALMs 19 M9Ks	3307 ALMs 19 M9Ks	3311 ALMs 19 M9Ks	3512 ALMs 29 M9Ks	3428 ALMs 29 M9Ks	3378 ALMs 29 M9Ks
max clock	236 MHz	259 MHz	251 MHz	230 MHz	255 MHz	248 MHz
max throughput (conf+integ)	1222 Mbps	1342 Mbps	1300 Mbps	2249 Mbps	2494 Mbps	2425 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

Copyright © 2004-2010 Helion Technology Ltd; All rights reserved. This document contains Proprietary Trade Secrets of Helion Technology Limited; its receipt or possession does not convey any right to reproduce, disclose its contents, or to use its contents to manufacture, use, or sell anything that it may describe without the written authorisation of Helion Technology Limited. The products described in this document are subject to continuous development and all information is supplied strictly "as is" with no warranties implied or expressed and Helion Technology Limited shall not be liable for any loss or damage arising from the use of any information contained in this document.