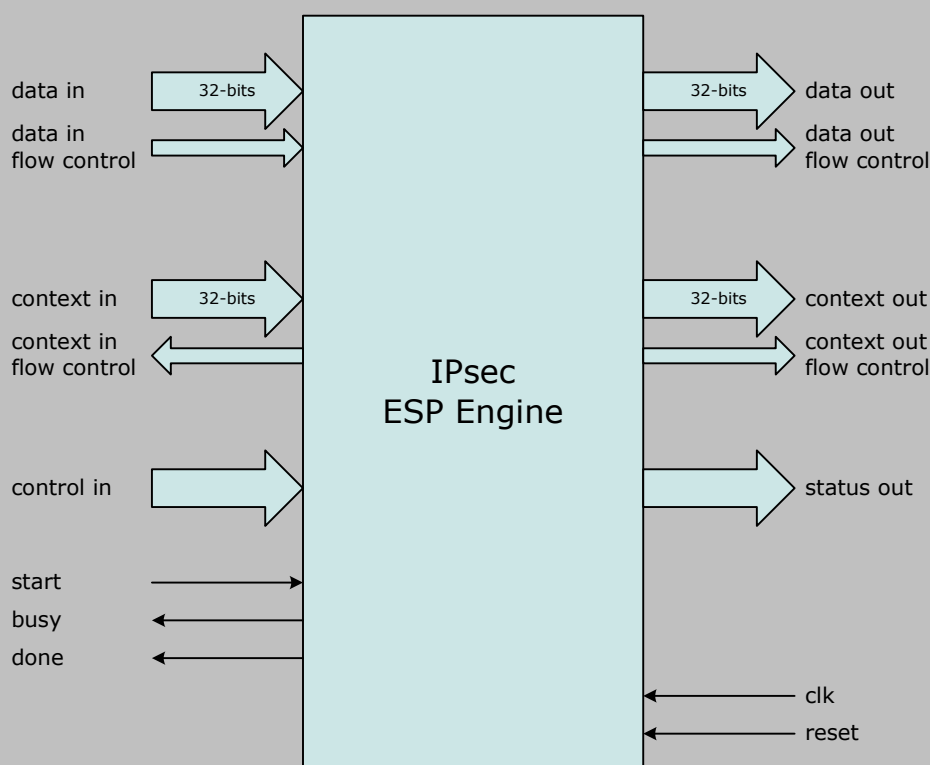


Helion Technology

DATASHEET - IPsec ESP Engine for Altera FPGA



Features

- Designed for hardware acceleration of IPsec ESP protocol
- Supports all mandatory and proposed IPsec ESP confidentiality and authentication algorithms
- Suitable for use in IPv4 and IPv6 IPsec Transport and Tunnel mode applications
- Extended (64-bit) Sequence Number support for IKEv2
- Supports all proposed ESP security service combinations
- Supports insertion of padding for Traffic Flow Confidentiality (TFC)
- Automatic ESP padding generation and checking
- Supports Gigabit/sec throughputs

Deliverables

- Target specific netlist or fully synthesisable RTL VHDL
- Verilog/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 computationally intensive algorithms 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 IPsec application to yield an optimum logic area and performance trade-off.

The ESP Engine is suitable for use in both IPv4 and IPv6 IPsec applications, and can support both Transport and Tunnel mode operation. It supports all mandatory ESP algorithms as defined in RFC4835 including 3DES-CBC, AES-CBC, AES-CTR, HMAC-SHA-1-96, and AES-XCBC-MAC-96, as well as the proposed combined mode algorithms such as AES-CCM and AES-GCM. In addition to cryptographic acceleration, the ESP Engine also performs padding generation and checking in accordance with RFC4303, and fully supports Traffic Flow Confidentiality padding generation.

Helion Technology Limited

Ash House, Breckenwood Road,
Fulbourn, Cambridge CB21 5DQ, England



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 in the output FIFO. A separate memory mapped context interface provides a means for the ESP Engine to access the Security Association 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 authentication 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.

Logic Utilisation and Performance

The table below shows typical logic resource and data throughput figures for three different configurations of the ESP Engine in Altera Stratix II. This illustrates how the ESP engine data throughput is dependent on both the type of IPsec security service selected and the maximum throughput of the underlying confidentiality and authentication algorithms. The maximum data throughput figures shown are for 1500 byte packets.

Helion can provide application specific ESP Engine wrappers to implement a basic flow-through IPsec ESP solution using packet FIFOs and context memories. The Helion ESP Engine is also available for other Altera FPGA families. Helion are able to provide a full range of consultancy and support services, and are happy to work with clients to achieve the maximum potential of our ESP Engine solution.

—Stratix II (EP2S15F672C3)—			
security type	3DES-CBC HMAC-SHA-1	AES-CBC HMAC-SHA-1	AES-CBC AES-XCBC-MAC
logic resource	3407 ALUTs 5 M4K 2 M512	5044 ALUTs 23 M4K 10 M512	5097 ALUTs 28 M4K 10 M512
max clock	202 MHz	200 MHz	192 MHz
auth only throughput	956 Mbps	946 Mbps	1920 Mbps
conf+auth throughput	463 Mbps	946 Mbps	1848 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