ISP1-12.8 Core

IPsec Security Processor IP Core

General Description

Implementation of the IPsec security standard at high data rates requires the cryptographic processing acceleration. The ISP1-12.8 core is tuned for applications with the data rates of 1-6 Gbps (less for TripleDES).

The design is fully synchronous and available in both source and netlist form.

Key Features

Support for IPv4 and IPv6 packets

Support for the ESP and AH protocols

- Insertion / removal of headers and trailers; internal padding
- Transport and tunnel modes of operation
- Integrity Check Value (ICV) insertion and validation

Support for ESP encryption algorithms per RFC 4835:

- NULL
- AES-CBC (128- and 256-bit keys)
- TripleDES-CBC

Support for ESP (and AH for –AH option) authentication algorithms per RFC 4835:

- HMAC-SHA1-96
- AES-XCBC-MAC-96

Additional cryptographic algorithms available upon request

Small size combined with high performance:

- Starting at less than 120K ASIC gates plus external memory sufficient to hold one packet
- Peak throughput of 12.8 bits per clock for 128-bit AES encryption (7.7 Gbps at 600 MHz), 9.1 bits per clock for 256-bit AES encryption (5.4 Gbps at 600 MHz)

FIFO-like interface with flexible bit width; simple integration into the datapath.

Supports encryption and decryption

Support for Galois Counter Mode Encryption and authentication (GCM), Galois Message Authentication (GMAC)

Flow-through design

Test bench provided

OpenSSL integration (integration with other packages upon request)

Uses an external Security Association (SA) database

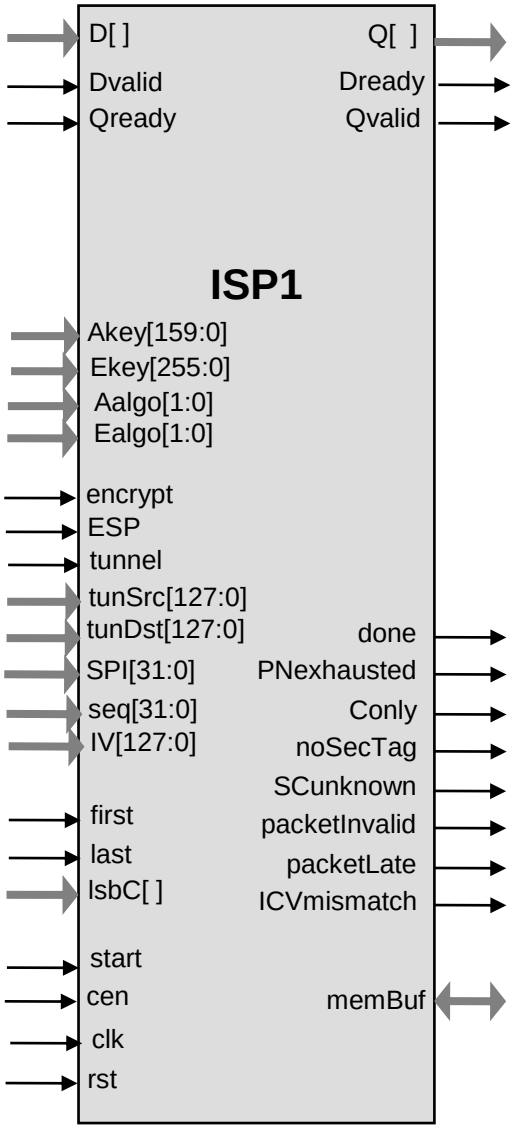
- No internal SA memory
- External database shall provide the replay protection

No segmentation/reassembly support in the transport mode

Applications

- IPsec accelerator

Symbol


D[ ]
Dvalid
Qready
Q[ ]
Dready
Qvalid
ISP1
Akey[159:0]
Ekey[255:0]
Aalgo[1:0]
Ealgo[1:0]
encrypt
ESP
tunnel
tunSrc[127:0]
tunDst[127:0]
SPI[31:0]
seq[31:0]
IV[127:0]
first
last
lsbC[ ]
start
cen
clk
rst
done
PNexhausted
Conly
noSecTag
SCunknown
packetInvalid
packetLate
ICVmismatch
memBuf

Pin Description

Name	Type	Description
Generic		
Clk	Input	Core clock signal
Rst	Input	Core reset signal
Cen	Input	Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored.
Start	Input	HIGH level starts the core operation
Configuration. The signals in this group typically have constant values during the core operation		
Encrypt	Input	When HIGH, core is encrypting, when LOW core is decrypting
ESP	Input	When HIGH, core is performing ESP processing. When LOW, AH processing
Tunnel	Input	Tunnel/transport switch. HIGH indicates tunnel.
Packet information. The signals in this group are to be asserted with the first or last word of the packet		
First	Input	Indicates the first word of a new packet on the D interface
Last	Input	Asserted with the last word of the packet
lsbC[ ]	Input	Number of valid bytes in the last word (unused if the D and Q buses are 8 bit wide)
Ealgo[1:0]	Input	Encryption algorithm for ESP. Asserted with the first word of the packet: • 00 – NULL • 01 – 3DES • 10 – AES-128-CBC • 11 – AES-256-CBC
Aalgo[1:0]	Input	Authentication mode for ESP or AH. Asserted with the first word of the packet: • 00 – None • 01 – HMAC-SHA1-96 • 10 - AES-XCBC-MAC-96
Ekey[255:0]	Input	Encryption key (shorter AES-128 and 3DES keys are in the MSB). Asserted with the first word of the packet.
Akey[159:0]	Input	Authentication key (shorter AES-128 key is in the MSB). Asserted with the first word of the packet.
tunSrc[127:0]	Input	Tunnel outer header information (source IP address). The IPv4 32-bit address is in the MSB (encryption in tunnel mode only). Asserted with the first word of the packet.

Name	Type	Description
tunDst[127:0]	Input	Tunnel outer header information (destination IP address). The IPv4 32-bit address is in the MSB (encryption in tunnel mode only). Asserted with the first word of the packet.
SPI[31:0]	Input	SPI value (encrypt only). Asserted with the first word of the packet.
seq[31:0]	Input	Sequence number (encrypt only). Asserted with the first word of the packet.
IV[127:0]	Input	Initialization vector for the ESP (shorter 3DES IV is in the MSB). Asserted with the first word of the packet.
Datapath		
D[ ]	Input	Input packet data
Dvalid	Input	When high, data on the D bus is valid
Dready	Output	When HIGH, core is ready to accept next data word on the D bus
Q[ ]	Output	Output encrypted or decrypted packet
Qvalid	Output	When high, data on the Q bus is valid
Qready	Input	When HIGH, external circuitry is ready to accept next data word on the Q bus
Completion signals. Asserted after the packet processing		
Done	Output	HIGH when data processing is completed, gate for the rest of completion signals
ICVmismatch	Output	On decryption: Packet authentication has failed
Memory interfaces		
memBuf		Memory buffer. Used as a ring buffer to delay a packet so its header can be modified. Single-port memory interface with data width twice larger than the D and Q buses

Function Description

The ISP1 implementation supports the IPsec protocol acceleration for cryptographic algorithms.

The core is designed for flow-through operation. ISP1 supports encryption and decryption modes (encrypt-only and decrypt-only options are available).

Tx Processing for ESP

On encryption, for each frame the core:

- Reads the header and key information from the inputs
- Prepends the ESP header (and, optionally, the outer tunneling header) to the packet
- Encrypts the packet
- Computes and stores the ICV in the packet
- Pads and appends the ESP trailer to the packet

Rx Processing for ESP

On decryption, for each frame the core:

- Reads the key information from the inputs
- Removes the ESP header (and, optionally, the outer tunneling header) from the packet
- Decrypts the packet
- Calculates the authentication value ICV and compares against the ICV in the packet
- Removes the ESP trailer

Tx Processing for AH

On encryption, for each frame the core:

- Reads the header and key information from the inputs
- Inserts the AH header (and, optionally, the outer tunneling header) into the packet
- Computes and stores the ICV in the packet

Rx Processing for AH

On decryption, for each frame the core:

- Reads the key information from the inputs
- Removes the AH header (and, optionally, the outer tunneling header) from the packet
- Calculates the authentication value ICV and compares against the ICV in the packet

Implementation Results

Area Utilization and Performance

Representative area/resources figures are shown below.

Technology	Area / Resources	Frequency	Throughput
TSMC 65 nm G+	100K gates	400 MHz	5 Gbps

Export Permits

The core can be a subject of the US export control. It is the customer's responsibility to check with relevant authorities regarding the re-export of equipment containing the AES encryption technology. See the IP Cores, Inc. licensing basics page, http://ipcores.com/exportinformation.htm, for links to US government sites and more details.

Deliverables

HDL Source Licenses

- Synthesizable Verilog RTL source code
- Source code for OpenSSL integration
- Testbench (self-checking)
- Vectors for testbenches
- Expected results
- User Documentation

Netlist Licenses

- Post-synthesis EDIF
- Testbench (self-checking)
- Vectors for testbenches
- Expected results

Contact Information

IP Cores, Inc.
3731 Middlefield Rd.
Palo Alto, CA 94303, USA
Phone: +1 (650) 815-7996
E-mail: info@ipcores.com
www.ipcores.com