ISP1-128 Core

IPsec Security Processor IP Core

General Description

Core implements the IPsec and SSL/TLS security standard at high data rates that require the cryptographic processing acceleration. The ISP1-128 core is tuned for applications with the data rates of 10-100 Gbps in advanced ASIC geometries.

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

Key Features

Support for IPv4 and IPv6 packets

Support for the IPsec 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
- Transport and Tunnel Adjacency (AH+ESP combination) support

Support for IPsec ESP encryption algorithms per RFC 4835:

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

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

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

Optional support for SSL 2.0, 3.0 and TLS 1.0. 1.1, and 1.2 (-SSL option). Capable of supporting simultaneous SSL/TLS and IPsec data flows. SSL/TLS cipher support includes:

- Block ciphers with hash-based authentication
- AEAD ciphers

Support for SSL / TLS block ciphers:

- RC4
- TripleDES-CBC
- AES-CBC (128-, 192- and 256-bit keys)
- AES-GCM (128- and 256-bit) (-GCM option)

Support for SSL / TLS hashes:

- MD5
- SHA-1
- SHA-256
- SHA-384
- SHA-512

Additional cryptographic algorithms available upon request

Built-in cryptographically secure pseudorandom number generator

Replay protection

Scalable high performance. Scaling is achieved through adjustable number of encryption engines inside and configurable throughput of the connection parameters memory .

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

Dedicated encryption and decryption configurations, duplex option with shared connection context memory available.

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

Flow-through design

Built-in connection parameters database and lookup engine

OpenSSL integration (integration with other packages upon request)

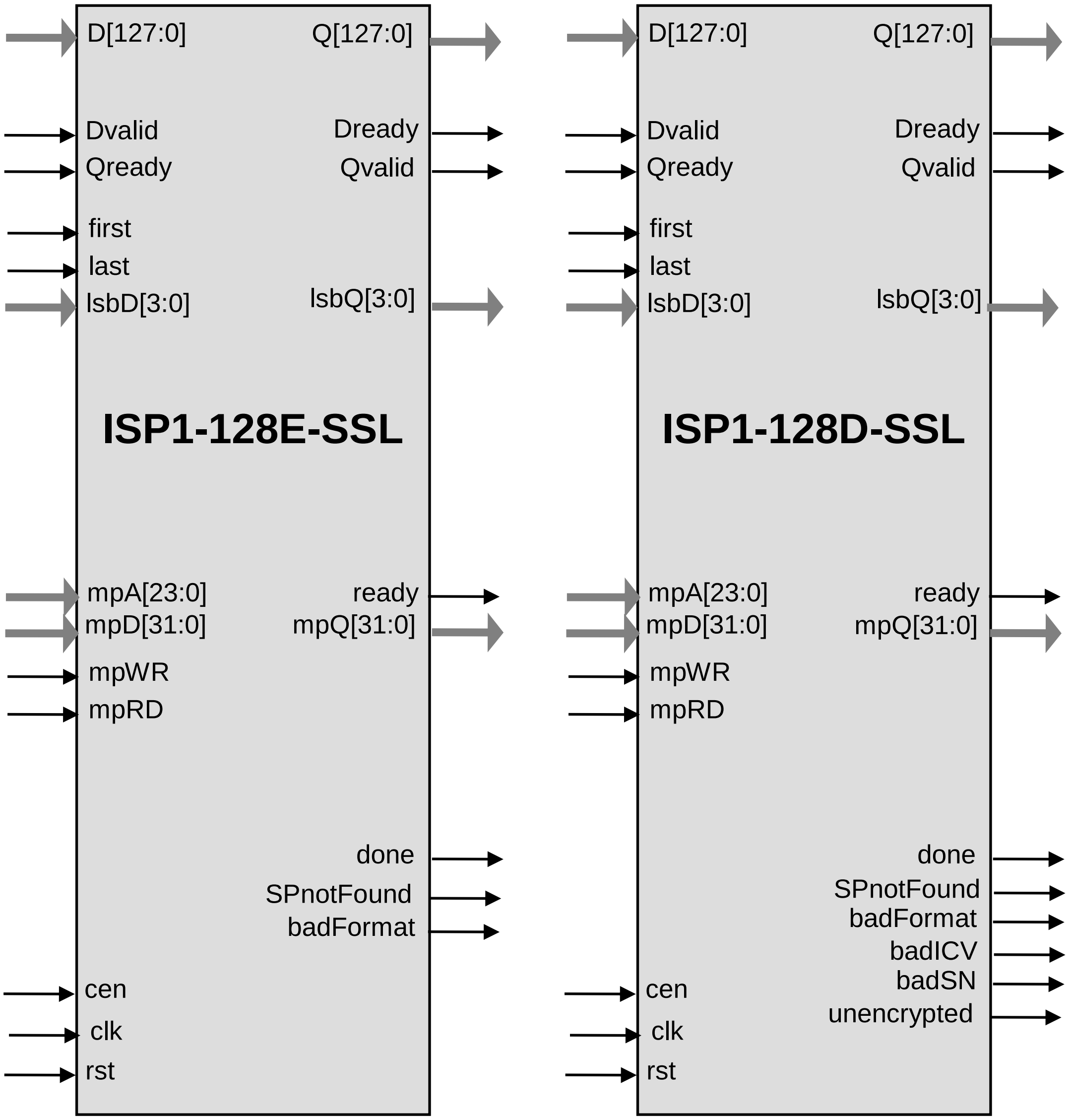
Optional statistics block

No segmentation/reassembly support in the IPsec transport mode

Applications

- IPsec accelerators
- SSL/TLS accelerators
- High performance routers

Symbol


D[127:0]
Q[127:0]
Dvalid
Dready
Qready
Qvalid
first
last
lsbD[3:0]
lsbQ[3:0]
ISP1-128E-SSL
mpA[23:0]
ready
mpD[31:0]
mpQ[31:0]
mpWR
mpRD
done
SPnotFound
badFormat
cen
clk
rst
D[127:0]
Q[127:0]
Dvalid
Dready
Qready
Qvalid
first
last
lsbD[3:0]
lsbQ[3:0]
ISP1-128D-SSL
mpA[23:0]
ready
mpD[31:0]
mpQ[31:0]
mpWR
mpRD
done
SPnotFound
badFormat
badICV
badSN
unencrypted
cen
clk
rst

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.
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
Datapath		
D[127:0]	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
lsbD[3:0]	Input	Number of valid bytes minus 1 in the last word
Q[127:0]	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
lsbQ[3:0]	Input	Number of valid bytes minus 1 in the word on Q bus (FF for all words but the last one)
Completion signals. Asserted after the packet processing		
done	Output	HIGH when data processing is completed, gate for the rest of completion signals
SPnotFound	Output	Secure parameters for the packet were not found
badFormat	Output	Packet was not correctly formatted
badICV	Output	Calculated ICV (IPsec) or MAC (SSL/TLS) does not match the one in the packet
badSN	Output	Sequence number for IPsec packet is outside the replay window
unencrypted	Output	The input packet was unencrypted

CPU interface		
mpA[23:0]	Input	Internal core address
mpD[31:0]	Input	Write data
mpQ[31:0]	Output	Read data
mpRD	Input	CPU read
mpWR	Input	CPU write
ready	Input	mpQ data is valid

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 NETKEY IPsec stack and 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