MSP1-PON Core

IEEE 802.1ae (MACsec) Security Processor Core

General Description

Implementation of the new LAN security standard IEEE 802.1ae (MACsec) requires the NIST standard AES cipher in the GCM mode for encryption and message authentication, as well as header parsing and formatting operations on the transmitted and received packets. The MSP1-PON core is tuned for Passive Optics Networks (PON) IEEE 802.1ae applications at the data rates of 10-100 Gbps.

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

Key Features

Small size combined with high performance:

- Starting at less than 180K ASIC gates
- 16 Gbps performance at 250 MHz with 180K gates

Self-contained, uses two external memories for key storage and statistic counters

Very low latency

- 12 clocks input-to-output

Back-to-back packet processing

- 64 bytes shortest packet

Supports encryption and decryption

Provides MACsec header parsing and modification:

- Insertion and removal of the SecTag including the packet number (PN) and an optional SCI
- RX packet validation
- Insertion, validation and removal of the ICV
- Replay protection based on the PN windowing

Includes key storage, lookup, and expansion

- Key lookup is based on LLID (other option of packet classifications are available)
- Ability to lookup the key using built-in associative memory (parameterized size, default 16 entries) or using the LLID directly as an index

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

Flow-through design

Test bench provided

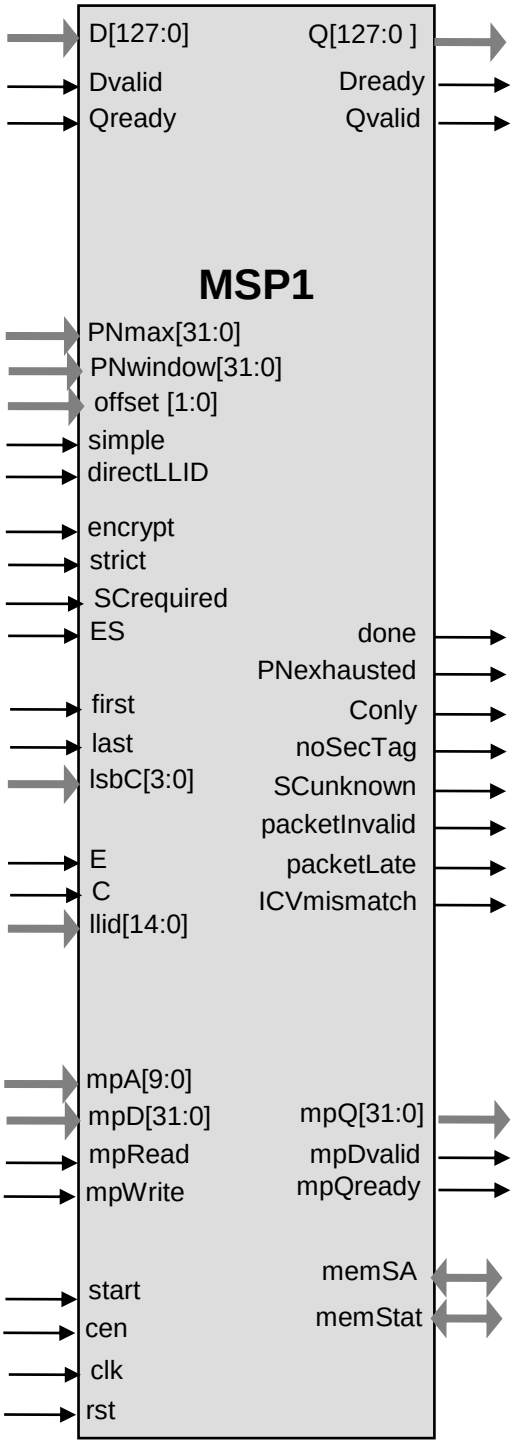
Sample software for 802.1X-2010 (a.k.a. 802.1af, KEYsec, 802.1x-REV) key agreement (MKA) is provided

Deliverables include test benches and optional NIST algorithm validation

Applications

- WLAN 802.1ae MACsec
- RFC 4869

Symbol


D[127:0]
Dvalid
Qready
Q[127:0]
Dready
Qvalid
MSP1
PNmax[31:0]
PNwindow[31:0]
offset [1:0]
simple
directLLID
encrypt
strict
SCrequired
ES
first
last
lsbC[3:0]
E
C
llid[14:0]
done
PNexhausted
Conly
noSecTag
SCunknown
packetInvalid
packetLate
ICVmismatch
mpA[9:0]
mpD[31:0]
mpRead
mpWrite
mpQ[31:0]
mpDvalid
mpQready
start
cen
clk
rst
memSA
memStat

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
offset[1:0]	Input	Confidentiality offset: • 00 – 0 bytes • 01 – 30 bytes • 10 – 50 bytes
PNmax[31:0]	Input	Threshold for PN exhaustion. When PN for an SA > PNmax, PNexhausted is asserted
PNwindow[31:0]	Input	Size of the PN window for replay protection
strict	Input	Strict fame verification. When HIGH, Tx frames for which SC cannot be found are suppressed
SCrequired	Input	If HIGH, Tx frames will include SCI
ES	Input	If HIGH, Tx frames will have ES set
directLLID	Input	If HIGH, LLID number is directy used as an index for the key lookup. If LOW, LLID is translated into key index using built-in associative storage.
simple	Input	Support for non-MACsec legacy encryption mode
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[3:0]	Input	Number of valid bytes in the last word
E	Input	If HIGH, the packet shall be encrypted/decrypted
C	Input	If HIGH, the packet shall be authenticated
llid[14:0]	Input	LLID of the packet
CPU interface		
mpA[9:0]	Input	Address

Name	Type	Description
mpD[31:0]	Input	Write data
mpQ[31:0]	Output	Read data
mpRead	Input	When HIGH, read operation
mpWrite	Input	When HIGH, write operation
mpDvalid	Output	When HIGH, valid data are available on the RD bus
mpQready	Output	When HIGH, CPU can write to the WD bus
Datapath		
D[127:0]	Input	Input packet data: additional authenticated data (AAD, A), followed by the plain or cipher text
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[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
Completion signals. Asserted after the packet processing		
done	Output	HIGH when data processing is completed, gate for the rest of completion signals
PNexhausted	Output	On Tx: PN number for the last packet is too high, time to re-key
Conly	Output	On Rx: The packet had C flag set, and E clear. These packets require KaY processing
noSecTag	Output	On Rx: The packet had no SecTag field (not a MACsec packet)
SCunknown	Output	On Rx or Tx: Unable to locate an SC for the packet
packetInvalid	Output	On Rx: Packet is not a proper MACsec frame
packetLate	Output	On Rx: Packet PN is outside the PN window
ICVmismatch	Output	On Rx: Packet authentication failed
Memory interfaces		
memSA		SA storage. For N SA, a single-port memory of 3N x 128 bits
memStat		(Only for statistics option) Statistics storage. For N SA, a single port memory of 12Nx64 bits

Function Description

The MSP1 implementation fully supports the IEEE 802.1ae (MACsec) algorithm for 128-bit bit keys, including AES support in Galois Counter Mode (GCM) per NIST publication SP800-38D http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf.

The core is designed for flow-through operation. MSP1 supports encryption and decryption modes (encrypt-only and decrypt-only options are available.

Tx Processing

On encryption, for each frame the core:

- Obtains the SC index from the LLID and looks up the current SA key
- Inserts the SecTag, including the PN and an optional SCI
- Encrypts and authenticates the frame, based on the values on the E and C inputs
- Appends the ICV tag to the packets
- Updates the PN
- Updates the statistics counters

Rx Processing

On decryption, for each frame the core:

- Obtains the SC index from the LLID and looks up the current SA key
- Allows pass-through fro KaY frames
- Validates the SecTag and SCI, if present
- Checks that the packet number PN is within the PN window
- Decrypts the frame, if encrypted
- Calculates the ICV tag, if the frame is authenticated, and compares to the one in the frame
- Removes the ICV tag, appended to the frame
- Updates the PN window
- Updates the statistics counters

Implementation Results

Area Utilization and Performance

Representative area/resources figures are shown below.

Technology	Area / Resources	Frequency	Throughput
TSMC 65 nm G+	180K gates	250 MHz	16 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
- Testbench (self-checking)
- Vectors for testbenches
- Expected results
- User Documentation
- Optional GCMVS NIST validation

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