Fraunhofer IPMS

MAC-SEC

MACsec Controller IP Core

Media Access Control Security

The MACsec Controller IP Core MAC-SEC for data rates up to 10G implements the Layer 2 security standard specified in IEEE 802.1AE-2018, which provides authentication, confidentiality, and integrity between hosts in a Local Area Network (LAN). MACsec ensures that only authorized nodes on the LAN are allowed to communicate, provides confidentiality by encrypting transmitted data, and provides cryptographic mechanisms that ensure data integrity. It can be used with the Fraunhofer IPMS LLEMAC IP core, any other Ethernet MAC IP core or in standalone operations.

Features

- Fully synchronous and synthesizable HDL design (System Verilog)

- Supports MACsec specification (IEEE 802.1AE-2018) and IEEE Std802.1AEbw
  - GCM-AES-128/192/256
  - GCM-AES-XPN-128/192/256

- Supports NIST encryption Standards
  - Advanced Encryption Standard (AES) FIPS PUB 197
  - Galois Counter Mode (GCM) RFC 5647
  - Key size of 128, 192, or 256 bits
  - Verified with Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)

- Supports up to 2^16 (per synthesis parameter) secure associations
- Detailed error reporting

MAC Data Interface

- AXI stream interface for MAC data
  - Full duplex usage possible

Host Controller Interfaces

- 32 bit synchronous host controller interface; wrapper for 8 bit hosts
- 32 bit AMBA APB Protocol Specification v2.0
- 32 bit AMBA 3 AHB-Lite Protocol v1.0
- 32 bit Avalon-MM version 2018.09.26, simple interface (no pipelining)
- 32 bit Wishbone
- Optional application specific interface to the host-controller on request

Deliverables

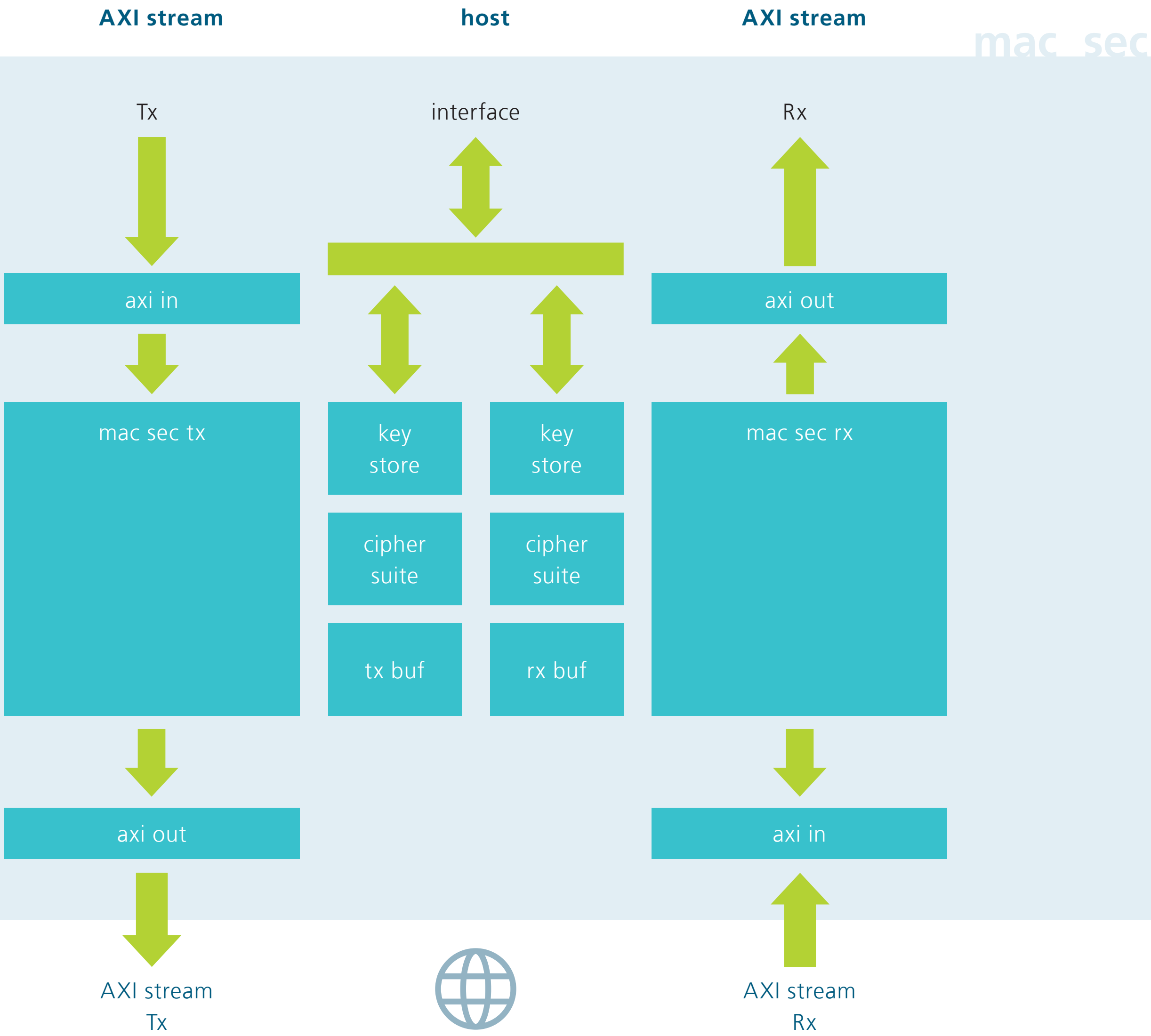
- Source code system Verilog RTL or targeted netlist
- Testbench
- Sample synthesis and simulation scripts
- Comprehensive documentation

Easy System Integration

- Platform independent implementation into any FPGA and any foundry technology
- Responsive implementation support

Low Latency Ethernet MAC Controller Core

Fraunhofer IPMS offers an IP core that implements an Low Latency Ethernet Media Access Controller (LLEMAC) that is compatible with the IEEE 802.3 and IEEE 802.3- 2002 specifications at 10/100 Mbps and 1Gbps. It has extremely low input and output latency. It is certified as ASIL-D-ready according to ISO 26262 for functional safety.



Contact

Monika Beck
+49 351 88 23 - 274
monika.beck@ipms.fraunhofer.de
Fraunhofer Institute for
Photonic Microsystems IPMS
Maria-Reiche-Str. 2
01109 Dresden
Germany
www.ipms.fraunhofer.de