MULTI-PROTOCOL ENGINES

inside secure

Packet-Engine IP Core Family for IPsec, SSL/TLS, DTLS and more

Highlights

Multi-Protocol Engine IPs offer acceleration of IPsec, MACsec, SSL/TLS/DTLS, sRTP and basic hash-crypto in architectures ranging from the look-aside engines to the more sophisticated, powerful inline packet engines.

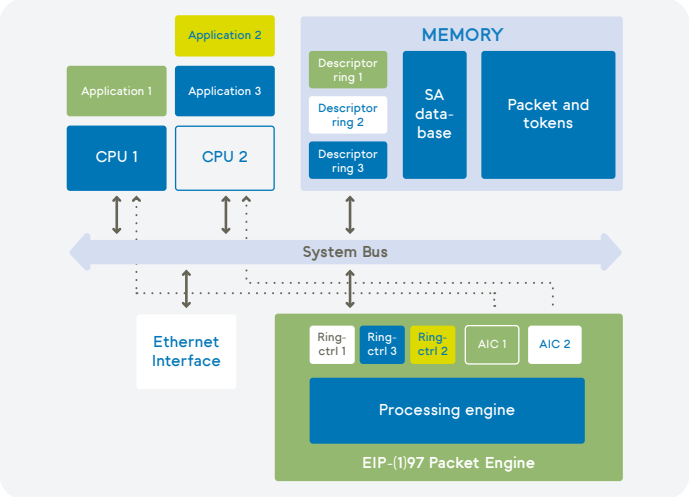
Engines Family

- **EIP-93** – Smallest Packet-Engine for Embedded/IoT GW
- **EIP-96** - Transform Engine for high-end NPU, Networking
- **EIP-97** – Multi-Protocol, Multi-Host, High Performance
- **EIP-197**- Adds inline flow with classification engine

Performance

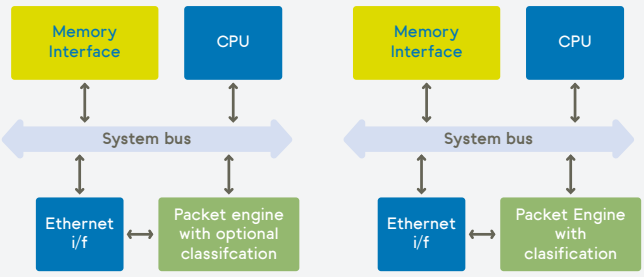
The EIP-197 configurations ranging from 5Gbps to 80Gbps and 100Gbps in modern 7nm processes.
At 1GHz the nominal performance is (large/small packets):

- **EIP-197b**: 10Gbps / 5Gbps,
- **EIP-197c**: 20Gbps / 10Gbps,
- **EIP-197d**: 40Gbps / 20Gbps,
- **EIP-197e**: 80Gbps / 40Gbps.



Architectures

- **Look-Aside/Hybrid**: connected as security co-processor to a SoC bus,
- **In-line Hybrid**: connected in between two streaming interfaces that are indirectly connect to either SoC or some external interface,
- **Bump in the Stack**: connected in between a SoC bus and Ethernet MAC,
- **Bump in the Wire**: connected in between two Ethernet MACs.



Interfaces

- **AXI master** Host bus interfaces (data width 128bits address width 56bits),
- **AXI slave** Host bus interfaces (data width 32bits address width 21bits),
- Virtualization support through bus sideband signals
- Internal scheduling of parallel descriptor-rings to avoid delays due to bus latency

Protocols

IPsec Classification

- Psec-ESP header parsing to look-up a flow,
- Fetch flow and corresponding transform record based on lookup result,
- Update flow statistics,
- Update transform statistics,
- Support for IPv4 and IPv6,
- For detailed L2, L3, L4 header parsing inforation is referred to the product documentation. Custom classification can be discussed.

IPsec transformation

- Full IPsec packet ESP transforms according to latest RFCs (2403, 2404, 2405, 2410, 2474, 3168, 3566, 3602, 3686, 4106, 4301, 4303, 4308, 4309, 4543, 4868, 4869, 6040, 6071, 7539 and 7634),
- Support for IPv4 and IPv6,
- Autonomous IPsec ESP packet classification and Security Association selection (both out- and inbound),
- IPsec ESP tunnel & transport mode,
- Complete IPsec Header/Trailer processing,
- Insert ESP header for outbound packets, strip and verify ESP header for inbound packets,
- Full sequence number processing, including ESN and full anti-replay check with various mask sizes, up to 384 bits
- Calculate and insert Integrity Check Value for outbound packets, strip and verify for inbound packets,
- Append (outbound) / strip and verify (inbound) padding up to 255 bytes.
- Support for processing packets for one SA on multiple processing engines, maintaining SA coherency.

SSLv3.0 / TLSv1.0 / TLSv1.1 / TLSv1.2

- Packet transforms according to latest RFCs (2246, 4346, 5246, 6101, 6655, 7905 and 8446),
- Header processing,
- Full autonomous single pass processing for stream and block cipher modes of operation,
- Padding insertion & removal up to 255 bytes,
- ICV/TAG insertion/verification.

DTLS v1.0 - v1.2

- Packet transforms according to latest RFCs (4347 and 6347),
- Header processing,
- Full autonomous single pass processing for stream and block cipher modes of operation,
- Padding insertion & removal up to 255 bytes,
- ICV/TAG insertion/verification
- Support for processing packets for one SA on multiple processing engines, maintaining SA coherency.

MACsec

- MACsec frame transforms according to IEEE 802.1AETM-2006 and 802.1AEbn,
- SecTAG insertion and removal,
- PN insertion, removal and verification,
- ICV generation, insertion, removal and verification
- Support for processing packets for one SA on multiple processing engines, maintaining SA coherency.

SRTP

- SRTP packet transforms according to RFC3711,
- ROC insertion and removal,
- MKI insertion and removal,
- TAG generation and insertion.

Wireless Algorithms

- Kasumi f8 and f9,
- SNOW 3G,
- ZUC.

Storage algorithms

- AES-XTS (including CTS mode)

Product webpage →

For further details on all of Inside's security solutions, visit www.insidesecure.com

inside secure