

Features

- Inline symmetric cryptographic functions (as part of 802.16e-2005 PDU processing):
- AES-CBC and AES-CTR to NIST Special Publication 800-38A.
- AES-CCM to the NIST SP 800-38C specification
- Support for insertion and extraction of packet number in CCM mode
- Support for insertion and extraction of roll-over counter in CTR mode
- AES core supports 128 bit keys
- DES-CBC with 56 bit key
- Pin select mode for 802.16-2004 compatible operation
- NULL encryption mode support to flow through selected PDUs without performing any security processing.

Applications

- WiMAX SoCs in base station and subscriber applications

The IEEE has ratified the WiMAX/802.16 (802.16e-2005) security standard. It now requires an AES implementation capable of supporting multiple modes including -CBC, -CTR, and -CCM; as well as a DES algorithm supporting -CBC mode. The LLP-02 is an upgrade to the LLP-01 and is designed to incorporate the functionality required to meet the now ratified standard.

This core offers an inline processing engine which captures traffic, security associations and control words through a single FIFO and operates on them per the reference standard. This greatly simplifies the implementation of complex security functions such as those required for WiMAX and presents significant offload to the embedded processor in soft MAC implementations.

General Description

The LLP-02 offers a complete, drop-in solution to the link layer security requirement for 802.16/WiMAX. It is fully compliant to both the IEEE 802.16e-2005 standard which was ratified in December 2005, and through a pin select can also support the 802.16-2004 standard. The LLP-02 is recommended for new designs.

The LLP-02 accepts interleaved Security Associations (SA) and PDU data through a common FIFO, interprets the command sequence, establishes the context for the appropriate cipher block then does either the encryption or decryption operation required. The LLP-02 can therefore be inserted seamlessly into the upper layer of the MAC.

The draft standard of the WiMAX specification requires AES as a mandatory cipher with 128 bit key size and support for the following modes:

- Cipher Block Chaining (CBC)
- Counter Mode (CTR)
- CCM (Counter mode with CBC Message authentication)

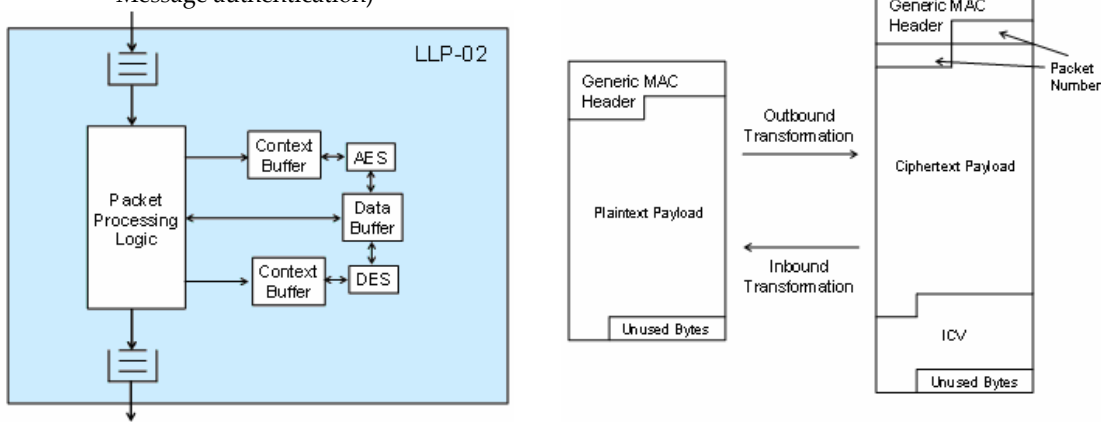
In addition, the core must support DES in CBC mode with 56 bit keys for legacy interoperability purposes.

The block diagram below illustrates the internal construction of the core.

The FIFOs in and out of the core are 34 bits wide. 32 bits are used for data and 2 bits for control. Control words indicate the type of data presented to or received from the FIFO, i.e the control bits select whether the associated data word contains PDU data, SA data, or control information to/from the core.

Any PDU in the stream may be tagged with the NULL encryption mode and will pass transparently through the core without application of the cryptographic functions. This feature can also be useful for debug during integration and application development..

As the specified cryptographic function is implemented, the PDU is transformed based upon the mode selected. A sample transformation is outlined in the diagram below.

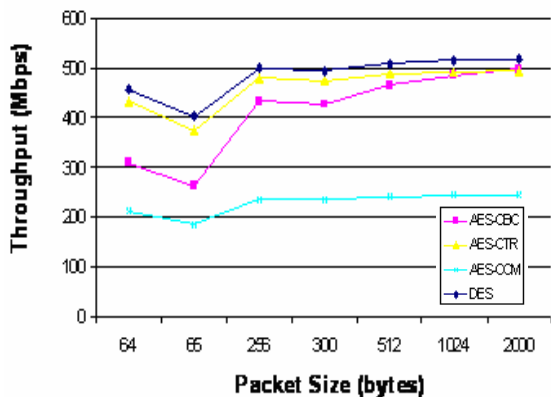


General Description cont'

Throughput

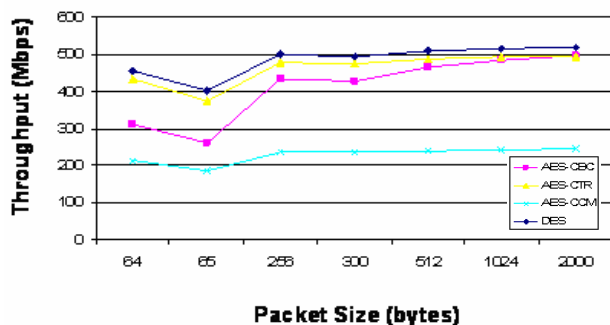
The graph below indicates the transmit performance with a core clock of 200MHz.

Receive Throughput vs Packet Size



The graph below presents the transmit throughput capability of the LLP-02

Transmit Throughput vs Packet Size



Elliptic has a full line of PDU Processors including:

- LLP-02 802.16/WiMAX PDU Processor
- LLP-03 WiMAX Forum Mobile Profile PDU Processor
- LLP-04 802.1AE/MACsec PDU Processor
- CLP-25 Configurable IPsec (ESP/AH) Offload Engine
- CLP-36 IPsec/SRTTP (ESP/AH) Offload Engine

Core Memory

The LLP-02 requires three internal memories or register files. There is context memory for the AES core, a context memory for the DES core and a data buffer. The following table specifies these requirements:

Memory	Size	Type
AES Context	72 x 32	Dual Port SRAM
DES Context	24 x 32	Dual Port SRAM
Data Buffer	48 x 32	Dual Port SRAM

As mentioned earlier, the input and output FIFOs are build time configurable by Elliptic. The standard configuration is implemented as 24 words deep – each word being 34 bits.

Availability

- The LLP-02 is available in soft IP form HDL Source. The deliverables available are:

HDL Source Licenses:

- Verilog HDL
- Testbench
- Sample synthesis script & constraints
- Sample simulation script
- Documentation