Features

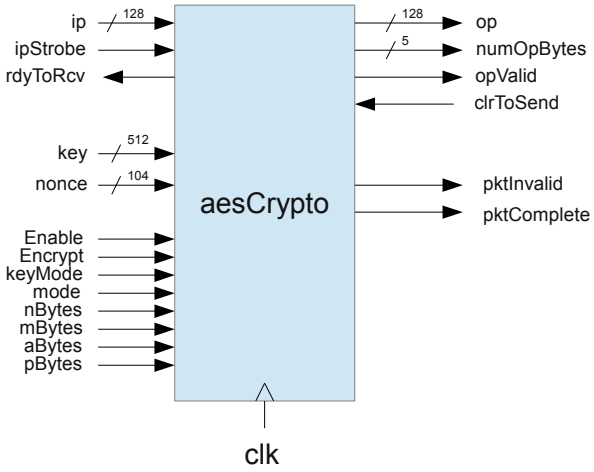
- Cryptography processor with one or more AES cores and, optionally, a GHASH core (for GCM).
- Nominal throughput of 1560MBPS @ 500MHz for a 128 bit key (4 cycles per round mode).
- Configurable number of cycles per round (4, 2 and 1) allowing even higher throughput per cycle.
- Full CCM, CMAC, GCM, GMAC encrypt/decrypt support.
- Basic AES modes of ECB, CTR and CBC also available.
- Low gate-count CCM configuration where a single AES core is time-shared between authentication and encryption.
- High throughput CCM configuration where separate AES cores are used for authentication and encryption.
- Configurable with an arbitrary number of AES cores in GCM mode, with throughput scaling in proportion.
- Presented as a core with 128-bit IO and simple control signal interface (processor agnostic).

Deliverables

- RTL (VHDL) block description and test harness with test vector files.
- C model.
- Vectors (collated from various standards docs).
- Detailed Functional Specification (to facilitate security reviews for export control).

General Description

This is an AES based encryption processor supporting the widely accepted protocols of CCM and GCM. CMAC (as specified in 802.11) is also supported.



The processor consists of one or more AES cores, a GHASH block (for the GCM option), scheduling controllers and datapath steering logic to manage the AES/GHASH resources to implement the required protocol (CCM, GCM etc).

IO is in the form of 128 bit blocks. External logic is required to map the blocks to the required system level bit-width.

Hardware signals provide the encryption key, nonce (or initialization vector) and byte counts for the nonce (N), MIC (M), additional (A) data and payload (P) data. A keyMode signal 0-2 selects a key size of 128, 256, 512 bits.

A mode signal selects the protocol (CCM, CMAC, GCM) and also allows selection of 'raw' AES modes (CBC, CTR, ECB). An encrypt signal selects between encryption and decryption (not supported for ECB and CBC modes).

The aforementioned signals are static and may easily be mapped to memory mapped registers in your system. A recommended mapping is provided however we leave the implementation to you as this is system-specific. Likewise the mapping of the 128-bit IO blocks to your internal data-path is architecture specific and also often requires standard-specific manipulation of headers (typically done in software).

Licence

The AES Crypto Processor may be licensed at the RTL level for a one-off licence fee that allows multiple uses in your own products (chips or FPGA based modules).

Full terms and conditions are provided with formal quotations.

The range of standards to be supported will typically be negotiated at the time of licensing as it is not practical to guarantee open ended support of all standards.

Product Selector

The following table shows this product (highlighted with *) alongside related products. Click the PDF icon to view the datasheets. The simplest product choice is to take only the RTL, however if you wish additional flexibility and the rights to modify the design then you can take the algorithm product as well.

Code	Description	
LDPCENC11NR	802.11n/ac LDPC Encoder RTL IP	
LDPCDEC11NR*	802.11n/ac LDPC Decoder RTL IP	
LDPCENCADR	802.11ad LDPC Encoder RTL IP	
LDPCDECADR	802.11ad LDPC Decoder RTL IP	
VITDEC11NR	802.11n/ac Viterbi Decoder RTL IP	
AESCRYPTO	AES Cryptography with CCM, and (optionally) CMAC and GCM.	

About Blue Rum Consulting

Blue Rum Consulting is a UK limited company offering the services and products of Michael Rumsey, a Wireless ASIC engineer with more than 30 years of experience. You can find him on linked-in and the company web-site at www.bluerum.co.uk .