WPA3

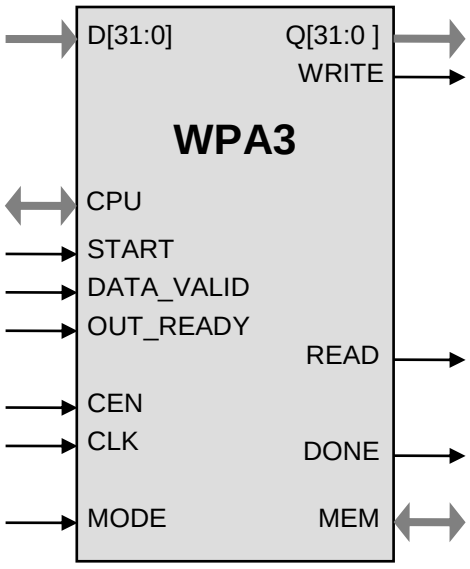
802.11i CCMP/TKIP Core

General Description

Implementation of the WLAN security standard (802.11i) requires the NIST standard AES cipher in CTR and CBC modes (a.k.a. CCM) for encryption and message authentication with the CCMP protocol and RC4/"Michael" cipher for the TKIP. The WPA3 core is tuned for high data rate 802.11i applications (up to 2 Gbps for the CCMP protocol for 802.11n/802.11ac). The core contains the base AES core AES1, base RC4 core ARC4 and is available for immediate licensing.

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

Symbol



Key Features

Small size:
Starting at 40K ASIC gates at 802.11a/g OFDM data speeds

Includes key lookup, encryption, decryption, header parsing and modification, key expansion and data interface

Uses external memory for key storage;

Configurable number of keys supported; 64 bytes are required per bidirectional link

Support for CCM AES-128 mode (Counter Mode with CBC MAC)

Support for RC4 and Michael ciphers, including the WEP Seed calculation

Legacy WEP mode supported, including pairwise keys

Flow-through design for data plane; microprocessor-friendly interface for configuration

Test bench provided

Deliverables include test benches

Applications

- WLAN 802.11i

Pin Description

Name	Type	Description
CLK	Input	Core clock signal
CEN	Input	Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored.
MODE	Input	Mode. When HIGH, transmit, when LOW receive
START	Input	HIGH starting input data processing
READ	Output	Read request for the input data byte
WRITE	Output	Write request for the output data byte
DATA_VALID	Input	HIGH when valid data byte present on the input
OUT_READY	Input	HIGH when output interface is ready to accept data byte
D[31:0]	Input	Input Data
Q[31:0]	Output	Output Data
DONE	Output	Data processing completed
CPU	I/O	Microprocessor bus for programming. Multiple interface versions available.
MEM	I/O	Local memory bus. Multiple memory configurations are available.

Function Description

The Advanced Encryption Standard (AES) algorithm is a NIST data encryption standard as defined in the FIPS-197 (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf). CCM mode is defined in NIST SP800-38C (http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C.pdf).

The WPA3 implementation fully supports the AES algorithm for 128 bit keys in Counter Mode (CTR) method of encryption with CBC message integrity check as required by the CCMP protocol of the 802.11i standard.

The core also supports ARC4 cipher with “Michael” authentication for the TKIP protocol as defined by the 802.11i standard.

The core is designed for flow-through operation (FIFO-like), with byte-wide input and output interfaces. The key and nonce information are stored in the local memory and automatically updated. PHY header precedes the packet in the data flow. Core performs all necessary per-packet calculations, parses and modifies the packet headers. The decryption results are indicated in the dataflow, including the replay protection.

WPA3 supports encrypt and decrypt modes

.

Export Permits

US Bureau of Industry and Security has assigned the export control classification number 5E002 to the core. The core is eligible for the license exception ENC under section 740.17(A) and (B)(1) of the export administration regulations. 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
- Simulation models
- User Documentation

Netlist Licenses

- Post-synthesis EDIF
- Testbench (self-checking)
- Vectors for testbenches
- Expected results
- Place & Route script
- Simulation models

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