WPI1

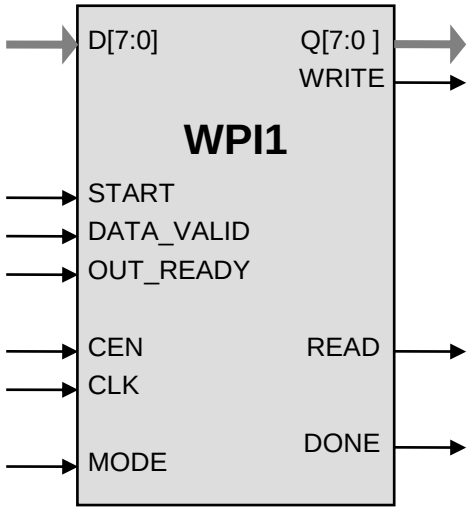
IEEE 802.11 WAPI Encryption Core

General Description

Implementation of the new Chinese security standard (WAPI) requires running the SMS4 cipher in the WPI mode for encryption and message authentication. The WPI1 core is tuned for WAPI applications and as such requires much smaller gate count than a full implementation.

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

Symbol



Key Features

Completely self-contained: does not require external memory

Includes encryption, decryption, key expansion and data interface

Support for WAPI WPI packet encapsulation

Automatic generation of key context from key data

Flow-through design

Test bench provided

Deliverables include test benches

Applications

- WAPI

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
DATA_VALID	Input	HIGH when valid data byte present on the input
WRITE	Output	Write to the output interface
OUT_READY	Input	HIGH when output interface is ready to accept data byte
D[7:0]	Input	Input Data
Q[7:0]	Output	Output Data
DONE	Output	Data processing completed

Function Description

The SMS4 algorithm is a data encryption standard as defined in the Chinese government specification 无线局域网产品使用的SMS4密码算法.

The WPI1 implementation fully supports the WPI packet encapsulation of the Chinese WAPI encryption standard for the IEEE 802.11 networks..

The core is designed for flow-through operation, with byte-wide input and output interfaces. SMS4 key and WPI initialization vector precede the frame in the flow of data. WPI1 supports encrypt and decrypt modes.

Data Formats

Core is designed to sit next to the modem in the data flow and so is able to pass through entire MPDU and A-MPDU data. It can recognize PLCP SIGNAL fields and MPDU Delimiters and extract and generate the MPDU length information. The core extracts the information from the WPI header and modifies the packet by appending or removing the 16-byte MIC.

.

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 script
- Synthesis script
- User Documentation

Netlist Licenses

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

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