AKW1 Core

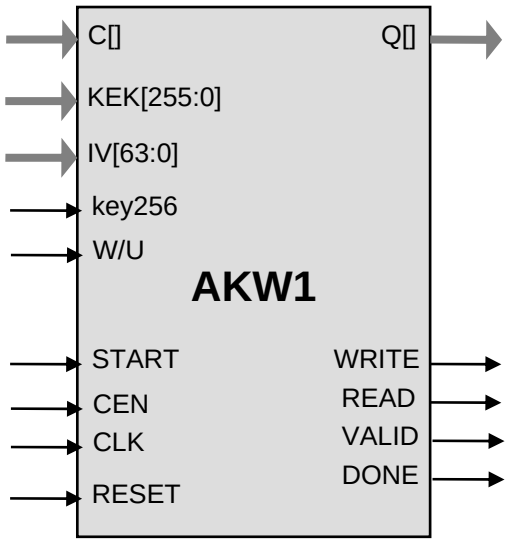
AES Key Wrap Core

General Description

AKW1 implements the NIST standard AES key wrap for encryption and decryption. Core contains the base AES core AES1 and is available for immediate licensing.

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

Symbol



Key Features

Small size: AKW1 starts from less than 8,000 ASIC gates

Completely self-contained: does not require external memory

Supports both encryption (wrap) and decryption (unwrap). Encryption-only and decryption only versions available.

Includes AES key expansion

128 and 256 bit AES key encryption keys (KEK) supported.

Flow-through design

Test bench provided

Applications

- AES key wrap per NIST key wrap specification

  and RFC 3394

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.
RESET	Input	HIGH level asynchronously resets the core
START	Input	HIGH level starts the input data processing
key256	Input	HIGH indicates 256-bit KEK key
W/U	Input	HIGH indicates key wrap, LOW – key unwrap
READ	Output	Read request for the input data byte
WRITE	Output	Write signal for the output interface
VALID	Output	HIGH level indicates a successful key integrity check
DONE	Output	HIGH level indicates a completion of key unwrapping
C[]	Input	Input Data
KEK[255:0]	Input	Key Encryption Key (128 bit KEK uses bits [255:128])
IV[63:0]	Input	Initial Value for A_0 per NIST standard
Q[]	Output	Output Key Data

Function Description

The Advanced Encryption Standard (AES) algorithm is a new NIST data encryption standard as defined in the http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

The AKW1 implementation fully supports the AES key wrap per NIST specification for 128 and 256 bit KEK, http://csrc.nist.gov/CryptoToolkit/kms/key-wrap.pdf.

The core is designed for flow-through operation, with 8/16/32/64/128-bit wide input and output interfaces. AKW1 supports both encryption (wrap) and decryption (unwrap) modes.

Implementation Results

Area Utilization and Performance

Representative area/resources figures are shown below.

Core Type	Technology	Area / Resources	Max Frequency	Throughput
AKW1-8D	TSMC 0.09 µ LV	8,000 gates	250 MHz	23 Kwraps/sec
AKW1-64D	TSMC 0.09 µ LV	14,000 gates	250 MHz	186 Kwraps/sec
AKW1-128D	TSMC 0.09 µ LV	16,000 gates	250 MHz	372 Kwraps/sec

Export Permits

US Bureau of Industry and Security has assigned the export control classification number 5E002 to the AES1 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/export_licensing.htm, for links to US government sites and more details.

Deliverables

HDL Source Licenses

- Synthesizable Verilog RTL source code
- Verilog testbench (self-checking)
- Vectors for testbench
- Expected results
- User Documentation

Netlist Licenses

- Post-synthesis EDIF
- Testbench (self-checking)
- Vectors for testbench
- Expected results

Contact Information

IP Cores, Inc.
3731 Middlefield Rd.
Palo Alto, CA 94303, USA
Phone: +1 (650) 814-0205
E-mail: info@ipcores.com
www.ipcores.com