CoreAES128 v3.3 Release Notes

This is the production release for CoreAES128 v3.3. These release notes describe the features and enhancements. They also contain information about system requirements, supported families, implementations, and known issues and workarounds.

Features

CoreAES128 is a highly configurable core and has the following features:

- Compliant with Federal Information Processing Standards Publication (FIPS PUB) 197
- ECB implementation per NIST SP 800-38A
- Example source code provided for cipher block chaining (CBC), cipher feedback (CFB), output feedback (OFB), and counter (CTR) modes
- 128-bit cipher key
- Encryption and decryption possible with the same core
- 44-Clock cycle operation to encrypt or decrypt 128 bits of data
- Pause/resume functionality to continue encryption or decryption at will
- Provides redundant security

Delivery Types

CoreAES128 is licensed in two ways: Obfuscated and RTL.

Obfuscated

Complete RTL code is provided for the core, enabling the core to be instantiated with CoreConsole or SmartDesign. Simulation, Synthesis, and Layout can be performed with Libero® System-on-Chip (SoC). The RTL code for the core is obfuscated and some testbench source files are not provided as they are precompiled into the compiled simulation library.

RTL

Complete RTL source code is provided for the core and testbenches.

Supported Families

CoreAES128 supports the following families:

- IGLOO®
- IGLOOe
- ProASIC®3
- ProASIC3E
- ProASIC3L
- Fusion
- ProASICPLUS
- Axcelerator®
- RTAX-S
- SmartFusion®
- SmartFusion®2
- IGLOO®2
- RTG4™

Supported Tool Flows

This version of the core requires the following tools:

- Libero IDE v8.4 or Libero SoC v10
- CoreConsole v1.4 (optional)

Installation Instructions

The CoreAES128 CPZ file can be installed using SmartDesign or CoreConsole.

Libero SoC/SmartDesign Instructions

Within Libero SoC, click **Add Core** in the Catalog to locate and install a local CPZ file, or use the automatic web update feature in Libero SoC. Once the CPZ file is installed in Libero SoC, the core can be instantiated, configured, and generated within SmartDesign for inclusion in your Libero SoC project.

For the RTL release version of the core, the FlexLM license must be installed and Libero SoC restarted before the core can be configured and generated within SmartDesign. Refer to the Libero SoC online help for instructions about core installation and licensing.

Documentation

This release contains a copy of the CoreAES128 handbook. The CoreAES128 handbook describes the core functionality, gives step-by-step instructions on how to simulate, synthesize, and place-and-route this core, and provides implementation suggestions. The documentation can be viewed by right-clicking the Core Selection window in CoreConsole after the core has been installed.

For updates and additional information about the software, devices, and hardware, refer to the Intellectual Property pages on the Microsemi web site

Supported Test Environments

CoreAES128 supports the following test environments:

- VHDL user testbench
- Verilog user testbench

Release History

Table 1 provides the release history of CoreAES128.

Table 1 Release History of CoreAES128

Version	Date	Changes
3.3	November 2014	Added support for RTG4.
3.2	February 2014	Added support for IGLOO2.
3.1	December 2012	Added support for SmartFusion and SmartFusion2.
3.0	February 2009	Added a generic/parameter FAMILY to select specific RAM type for each family. Added a generic/parameter CFG_MODE to configure only Encryption/Decryption mode.
2.1	January 2005	Added support for ProASIC3 and ProASIC3E devices.
2.0	March 2003	First production release of the core.

Resolved Issues in the v3.3 Release

There are no resolved issues with the CoreAES128 v3.3 release.

Resolved Issues in the v3.2 Release

There are no resolved issues with the CoreAES128 v3.2 release.

Table 2 Resolved SARs in CoreAES128 v3.2 Release

SAR	Description
54754	Updated Installation Instructions section.

Resolved Issues in the v3.1 Release

There are no resolved issues with the CoreAES128 v3.1 release.

Resolved Issues in the v3.0 Release

There are no resolved issues with the CoreAES128 v3.0 release.

Known Issues and Workarounds

There are no known issues or workarounds with the CoreAES128 v3.3 release.

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
E-mail: sales.support@microsemi.com

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense and security, aerospace, and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs, and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; security technologies and scalable anti-tamper products; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif. and has approximately 3,400 employees globally. Learn more at **www.microsemi.com**.

51300004-4/11.14