TI Software

Advanced Encryption Standard (AES)

Release Notes

Applies to Release: 1.0
Publication Date: July 7, 2008

Texas Instruments, Incorporated
20450 Century Boulevard
Germantown, MD 20874 USA

Contents

Release Notes

AES 1.0

Introduction

The AES component provides block cipher encryption and decryption for little and big endian processors. The component supports key sizes of 128, 192, and 256 bits, input text in 128 bit blocks and output text in 128 bit blocks.

Documentation

AES Doxygen API Document:
ti/mas/aes/docs/doxygen/AESAPI.chm

AES Test Module Doxygen Document:
ti/mas/aes/test/docs/doxygen/AES_TEST.chm

AES Standard:
http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

New This Release

Initial release

- AES Encryption
  - Optimized c64x+ encryption
    - Big endian
    - Little endian
- AES Decryption
  - c64x+ decryption
    - Big endian
    - Little endian
- Support for 128, 192, 256 bit keys
- C model (un-optimized) encryption supports small encryption table for memory savings (~3k bytes)

Upgrade and Compatibility Information

The integrator should be aware an extra input parameter, over open source implementations, has been added to AES encrypt and decrypt functions. The input parameter passes the number of rounds, output by the key expansion function, to the encrypt/decrypt function. More information can be found in the AES Doxygen API document.

Device Support

C64x+ Targets
- Tomahawk (TCI 6486)
  - Big endian
  - Little endian
- Himalaya (TCI 6482, 6455) [not tested]
  - Big endian
  - Little endian

Validation Information

Component Dependencies

AES
- ti.mas.types 4.1.0.1 (Common data type definitions)
- ti.mas.asm 2.0.0.1 (Common assembly utilities)
- ti.mas.secutil 1.0.0.0 (Common security utilities)
- ti.mas.swtools 3.1.0.2 (Internally used s/w tools)

AES Test Simulation
- ti.mas.types 4.1.0.1 (Common data type definitions)
- ti.mas.secutil 1.0.0.0 (Security utilities)
- ti.mas.util 3.1.0.0 (Common utilities)
- ti.mas.fract 1.3.0.9 (Common fractional arithmetic macros)
- ti.mas.aes 1.0.0.0 (Advanced Encryption Standard unit to be tested)
- ti.mas.sdk 1.2.0.1 (test infrastructure software)

Tool Dependencies

- XDCVERSION = xdc_3_00_04
- COVERITY VERSION = prevent-mingw-3.8.0
- C54 CODEGENVERSION = 4-10
- C55 CODEGENVERSION = cgen401
- C64 CODEGENVERSION = cgen6_0_15
- SDO ARCHITECTURE = sdoarch_standards_1_00_00_05
- XDAISVERSION = xdais_5_21
- XDCCGROOT = C:/tools/
- DOXYGENVERSION = 1.5.1-p1

- GRAPGVIZVERSION = 2.12
- HTMLHELPWORKSHOP = 10-01-2007
- TITEMPLATES = 10-01-2007

Compiler Options

Please view the AES package.bld file located in ti/mas/aes directory.

Known Issues

AES c64x+ little endian optimized encrypt does not work in conjunction with the decrypt. If the user would like to use a little endian encrypt together with decrypt, then must use the C model for the encrypt.

Benchmarks

Benchmarks can be found in the AES test simulation documentation located in the ti/mas/aes/test/docs/doxygen/ directory. Memory and MIPS information can be found under the 'Related Pages" tab.

Versioning

The component version definition can be found at the following site under section 'Compatibility Keys and Version Numbers':
https://twiki.dal.design.ti.com/twiki/bin/view/ASP/DSPS/Germantown/GTComponentGuidelinesC2

Technical Support and Product Updates

Contact local TI Field Application Engineer for technical support.

AES component information can be found at the following location:
https://twiki.dal.design.ti.com/twiki/bin/view/ASP/DSPS/Germantown/TiMasAes