TI Software

Advanced Encryption Standard (AES)

Release Notes

Applies to Release: 1.0
Publication Date: July 23, 2008

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

Contents

Introduction 1
Known Issues 1
Documentation 1
New This Release 2
Upgrade and Compatibility Information 2
Device Support 3
Validation Information 3
Benchmarks 4
Versioning 4
Technical Support and Product Updates 4

Release Notes

AES 1.0

Introduction

The AES component provides block cipher encryption and decryption for little and big endian c64x+ 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.

Known Issues

None.

Documentation

The following documentation is available:

- AES API Document
  aes/docs/doxygen/AESAPI.chm
- AES Test Module Document
  aes/test/docs/doxygen/AES_TEST.chm
- AES FIPS Standard
  http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

New This Release

Current Changes

The following changes have been made in release 1.0.0.1:

- Optimized c64x+ decryption
  - Big and little endian supported
  - ~35% improvement over C model for decryption key expansion function
  - ~29% improvement over C model for decryption function
- Improved performance of c64x+ encryption functions
  - ~2% for encryption key expansion function
  - ~5% for encryption function
- Reworked AES unit test to provide more accurate cycle profiling numbers.

Previous Changes

Release 1.0.0.0 provides the following:

- 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 encryption supports small encryption table for memory savings (~3k bytes)

Upgrade and Compatibility Information

Warning: Beginning with AES 1.0.0.1 the aes_c.a* library is no longer provided. All functions have been optimized and moved within the aes_a.a* library. All C model function counterparts have been moved within the aes_cm.a* library.

Compatibility Key Definitions

Compatibility keys are intentionally independent of Marketing product numbers and are intended to:

1. Enable tooling to identify incompatibilities between components, and
2. Convey a level of compatibility between different releases to set end user expectations.

Compatibility keys are composed of 4 comma-delimited numbers - M,S,R,P - where:

- **M = Major**. A difference in M indicates a break in compatibility.
- **S = Source**. A difference in S indicates source compatibility. That is, the user's source doesn't require change, but *does* require rebuilding.

- **R = Radix**. A difference in R indicates an introduction of new features, but compatibility with previous interfaces has not broken. If libraries are provided by the package, an application must re-link with the new libraries, but not rebuild from source.
- **P = Patch**. A difference in P indicates that only bugs have been fixed in the latest package and no new features have been introduced. If libraries are provided by the package, an application must re-link with the new libraries, but is not required to recompile its source.

Device Support

This release supports the following device families:

- C64P

Validation Information

This release was built and validated using the following:

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.util 3.0.0.0 (Common 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.aes 1.0.0.0 (Advanced Encryption Standard unit to be tested)
- ti.mas.sdk 1.2.0.1 (test infrastructure software)

Tool Dependencies for Source Release

- XDCVERSION = xdc_3_00_04
- COVERITY VERSION = prevent-mingw-3.8.0
- 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

Benchmarks

The following benchmarks were taken for the release:

- For cycle and memory benchmarks of the AES algorithms please refer to the AES test simulation documentation link provided in the 'Documentation' section of this document. The cycle and memory data can be found under the 'Related Pages" tab.

Versioning

Version Information:

Version Information is composed of 4 comma-delimited numbers – V, R, X, P - where:

- **V = Version -** Substantial difference from the last release.
- **R = Revision** – Minor difference from the last release.
- **X = External Vertical –** Vertical specific release.
- **P = Patch -** For any release other than mentioned above.

Technical Support and Product Updates

Contact local TI Field Application Engineer for technical support.