Advanced Encryption Standard (AES) (FIPS-197)

http://www.vocal.com

VOCAL Technologies, Ltd. software libraries include a complete range of ETSI / ITU / IEEE compliant algorithms, optimized for execution on ANSI C and leading DSP architectures (ADI, ARM, DSP Group, LSI Logic ZSP, MIPS and TI). This software is an example of VOCAL using MIPS Technologies CorExtend features to develop a custom solution to increase performance.

The Advanced Encryption Standard (AES) is a computer security standard that became effective on May 26, 2002 by NIST to replace DES. The cryptography scheme is a symmetric block cipher that encrypts and decrypts 128-bit blocks of data. Lengths of 128, 192, and 256 bits are standard key lengths used by AES.

The algorithm consists of four stages that make up a round which is iterated 10 times for a 128-bit length key, 12 times for a 192-bit key, and 14 times for a 256-bit key. The first stage "SubBytes" transformation is a non-linear byte substitution for each byte of the block. The second stage "ShiftRows" transformation cyclically shifts (permutes) the bytes within the block. The third stage "MixColumns" transformation groups 4-bytes together forming 4-term polynomials and multiplies the polynomials with a fixed polynomial mod (x^4+1). The fourth stage "AddRoundKey" transformation adds the round key with the block of data.

In most ciphers, the iterated transform (or round) usually has a Feistel Structure. Typically in this structure, some of the bits of the intermediate state are transposed unchanged to another position (permutation). AES does not have a Feistel structure but is composed of three distinct invertible transforms based on the Wide Trial Strategy design method.

The Wide Trial Strategy design method provides resistance against linear and differential cryptanalysis. In the Wide Trail Strategy, every layer has its own function:

The linear mixing layer: guarantees high diffusion over multiply rounds
The non-linear layer: parallel application of S-boxes that have the optimum worst-case non-linearity properties.
The key addition layer: a simple XOR of the round key to the intermediate state

Terminology:

- Plaintext refers to the data to be encrypted. Ciphertext refers to the data after going through the cipher as well as the data that will be going into the decipher.
- The state is an intermediate form of the cipher or decipher result usually displayed as a rectangular table of bytes with 4 rows and 4 columns.

Features:

- Key lengths of 128, 192, and 256 bits are supported. Each step in key size requires only two additional rounds.
- The decipher is simply the inverse of the cipher.
- Figure 1 shows the ShiftRows transformation where the first row remains untouched, while the second, third, and fourth rows perform a byte rotate by one, two, and three bytes respectively.
- Figure 2 shows the MixColumns transformation where each column is treated as a four-term polynomial over GF(2) and multiplied by $a(x) = \{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$.

Implementations:

- **Optimized Software Implementation.** The pure software implementation is bounded by the load/store behavior and byte arithmetic of the algorithm. The encryption requires 774 cycles per block on a MIPS32 processor and the decryption requires 837 cycles.

- **AES Primitives.** This is the simplest form of Vocal's hardware acceleration. The AES Primitives extend the capabilities of the MIPS32 processor by taking advantage of MIPS Technologies CorExtend capability to decrease the number of cycles to 393 cycles to encrypt and 460 cycles to decrypt per block on the MIPS32 processor.

VOCAL Technologies, Ltd.

Custom Product Design Division
200 John James Audubon Parkway
Buffalo, New York 14228
716-688-4675

http://www.vocal.com

- **AES Round Accelerator.** The Round Accelerator requires 1024 bytes of local memory, but increases the performance to 117 cycles per block to encrypt and 127 cycles per block to decrypt.

- **AES 32-bit Block Accelerator.** The Block Accelerator is designed to be a good mid-scale solution. It uses 2048 bytes of local memory. The number of cycles to process a block on a MIPS32 cpu falls to 64 cycles for both encryption and decryption using this implementation.

- **AES 32-bit Co-Processor.** The Co-Processor implementation uses 2048 bytes of memory to deliver performance of 45 cycles per block on the MIPS32.

- **AES 64-bit Co-Processor.** The same amount of the memory is required for the 64-bit implementation, but the performance increases to just 25 cycles per block on the MIPS32.

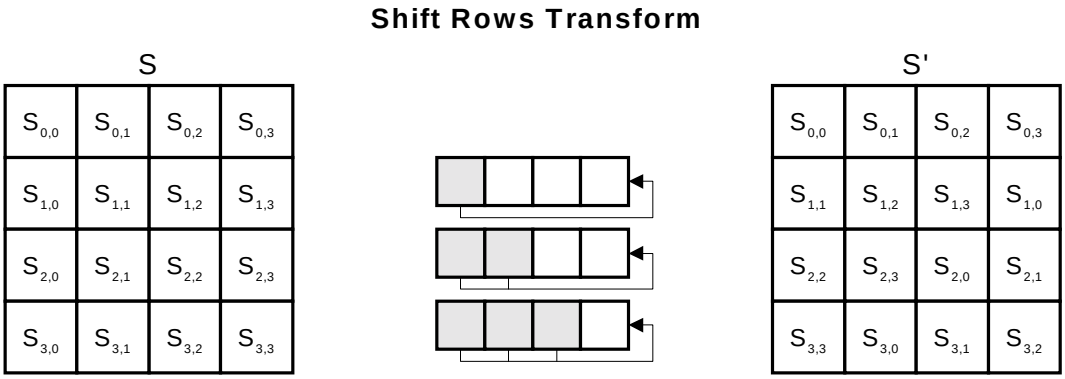

Figure 1.

Figure 2.

	Optimized Software (No Pro Instructions)	VOCAL Block Accelerator and Pro	TI C62x DSP	TI C64x DSP
AES Encrypt (128-bit key)	774 cycles per block	64 cycles per block	227 cycles per block	--
AES Decrypt (128-bit key)	837 cycles per block	64 cycles per block	268 cycles per block	--

Figure 3. Table of Benchmarks

Custom Product Design Division
200 John James Audubon Parkway
Buffalo, New York 14228
716-688-4675

http://www.vocal.com