OCTERA
Corporation

# AES 128 Encryption/Decryption

Version 1.0, December 2011

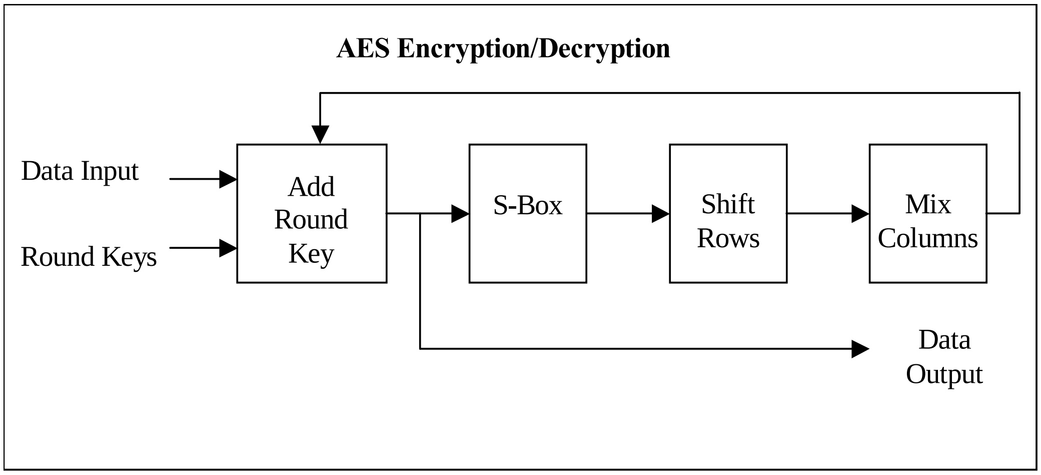
## Introduction

**Octera's AES-128 encryption/decryption IP provides better performance than competing IP. It also allows for flexibility in trading off performance for reduced resouce utilization. The high performance configuration is 30% faster than the ROM based configuration, while the ROM based configuration still out performs other available IP by 4% while offering a minimal foot-print.**

**The AES-128 encryption and decryption IP perform generic encryption/decryption of a 128-bit QWord. The round keys (which must be provided to the IP) are generally calculated by software rather than hardware, since high performance is seldom necessary for that purpose.**

## Features

- **ROM based versions for minimal foot-print.**
- **LUT based versions for maximum performance.**



**Representative data from an Altera Stratix IV EP4SGX230FF35C3 based design:**

| Encryption/ Decryption | Core | Clock Frequency | # of clocks required | Total time | LUTs | M9Ks |
|---|---|---|---|---|---|---|
| Encryption | ROM | 244MHz | 10 | 40.9ns | 322 | 8 |
| Encryption | logic | 305MHz | 10 | 32.8ns | 1228 | 0 |
| Encryption | 5-clock | 167MHz | 5 | 29.9ns | 2435 | 0 |
| Decryption | ROM | 207MHz | 10 | 48.2ns | 445 | 8 |
| Decryption | ROM-32 | 260MHz | 10 | 38.5ns | 256 | 16 |

## Deliverables

- **VHDL source code or encrypted source code depending on the type of license**
- **Round key generator as PERL script or executable**
- **User documentation**

**Product code: OCT-AES128**