ASICS.ws

Product Overview

AES Crypt IP Core

Introduction

This is a high performance, small footprint crypt/decrypt IP Core. It features up to 8 independent crypt engines. Three DMA engines make sure the core is always provided with a constant data stream. The crypt engines run of a dedicated clock, separate from AXI interfaces.

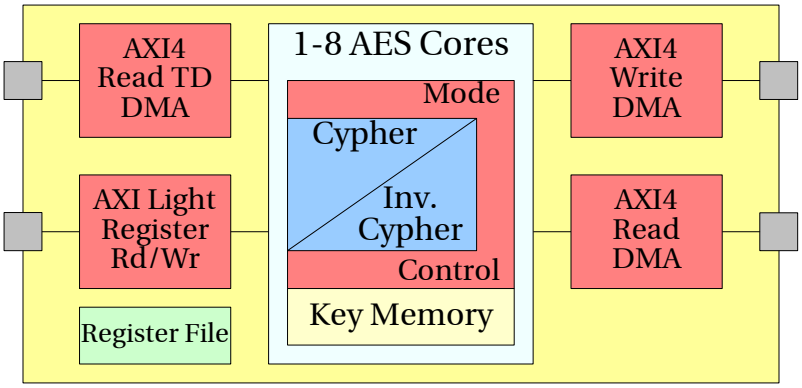
Features

The AES Crypt IP Core includes the following features:

- *100% AES compatible*
- *>2.4 GB/sec max throughput*
- *Up to 8 engines in parallel (configurable)*
- *Supports ECB, CBC and XTS/XEX modes*
- *Supports BitLocker acceleration*
- *Supports Encryption and Decryption*
- *Supports 128, 192 and 256 key sizes*
- *4/8 keys can be stored in each engine*
- *Verified against FIPS test vectors*
- *Task Based DMA engine*
- *Configurable Data Path 32, 64 or 128 bit*
- *Fully AXI4 compatible (data interface)*
- *AXI Light for register Interface*
- *Separate clocks for AES engines and AXI interface*

Architecture

Separate DMA engines for reading and writing data, as well as for fetching the task descriptor. All master interfaces are AXI4 compatible. The register file interface utilizes a AXI Light interface.



Size And Speed

Sample Synthesis results for AES IP Core. The goal was smallest and fastest implementation.

Technology	*Gate Count*	*Fmax*
Virtex UltraScale+ Virtex UltraScale Kintex 7, Virtes 7	10,200 LUTs, 11,500 Registers 64 BRAMs	AXI Interface: >200 MHz Engines: >300 MHz
This IP Core can be implemented in any technology. There are no special/dedicated FPGA (or other) components in this IP Core.		

Synthesis results for an implementation with 4 Crypt Engines. These synthesis results are provided for reference only.