Enhanced AES (Rijndael) IP Core

Introduction

The Enhanced AES (Rijndael) IP Core provides numerous building blocks that are used to put together an encryption core for a variety of different applications. It provides both cypher and inverse cypher operations. High performance implementation, over 34 Gbit/sec in an 0.18u process.

Features

Fully FIPS-197 compliant. This enhanced implementation consists of several blocks that can be selected by the customer depending on his needs. These blocks include:

- Data Path Units
- Static Key Expansion Units
- Dynamic Key Expansion Units

It provides true single cycle cypher/inverse cypher operations.

Architecture

Data Path Unit

The data path units are available for 128, 192 and 256 bit keys, and comes in two flavors: Single and Double stage pipeline. Both can perform a full cypher/inverse cypher operation every clock cycle. The single stage pipeline has a latency of 12-16 cycles, the double stage pipeline of 22-26 cycles (depending on key size). The double stage pipeline allows the core to operate at higher speeds, but makes it larger. Both Data Path Units can be used with any key expansion module. Separate Data Path Units are used for cypher and inverse cypher operations.

Static Key Expansion Units

The static key expansion units are available for 128, 192 and 256 bit keys. They can expand a key every 12-14 cycles (depending on key size). They are best suitable for applications where the key does not change every clock cycle.

Dynamic Key Expansion Units

The dynamic key expansion units are available for 128, 192 and 256 bit keys. They can expand a key every clock cycle. The latency depends on the key size and weather it is cypher or inverse cypher unit. They are best suited for applications where the key changes every clock cycle.

Verification

All blocks have been verified against a vast variety of test vectors available on the Internet including the AES Algorithm Validation Suite (AESAVS) from National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Division.

Size And Speed

Sample Synthesis results for an 0.18u process. The goal was smallest and fastest implementation.

Function	*Gate Count*	*Fmax*	*Throughput*
Data Path Unit, 128 bit, cypher	310K	266 Mhz	34Gbps
Data Path Unit, 192 bit, cypher	372K	266 Mhz	34Gbps
Data Path Unit, 256 bit, cypher	430	266 Mhz	34Gbps
Key Module 128 bit, dynamic	84K	400 Mhz	400M keys/s
Key Module 256 bit, static	130K	300 Mhz	16M Keys/s

*All Gate Counts include ROMs.

These synthesis results are provided for *reference only*. Please contact us for estimates for your application.