

# AES Cryptosystem Engine IP-AES-EP

February 20, 2008

Product Specification

## 開発・販売・サポート

株式会社 機械学習研究所

(Machine Learning Laboratory, Inc.)

〒228-0803 神奈川県相模原市相模大野 3-1-12

Phone: 042-705-0377

Fax: 042-705-0378

E-mail: ipcore@ml-labo.com

URL: <http://www.ml-labo.com/>

## 特徴

- VHDL IP コア
- AES Cryptosystem Engine
- 暗号鍵長: 128/192/256-bit
- 暗号鍵入力ポート幅: 32-bit
- データ入出力ポート幅: 128-bit
- オペレーションモード: ECB
  - IP-AES-EP は IP-AES-xP ファミリの Engine 部
- 最高動作周波数: 222MHz
  - Xilinx XC5V LX50-3 における評価値
- 最高データ速度: 1.8Gbps ~ 2.5Gbps
  - Xilinx XC5V LX50-3 における評価値
- スピード・ファクタ: 8.5 ~ 11.6
  - 最高データ速度/最高動作周波数

## 応用分野

- 通信システムの情報秘匿
- 記憶媒体やデータベースの情報秘匿
- 著作権保護
- 電子決済

表 1 : IP-AES-EP 仕様

設計パラメータ	
オペレーションモード <sup>1</sup>	ECB
暗号鍵入力幅(bit)	32
データ入出力幅(bit)	128
レイテンシー(clock)	10+1 (鍵長 128-bit 時) 12+1 (鍵長 192-bit 時) 14+1 (鍵長 256-bit 時)
スピードファクタ <sup>2</sup>	11.6 (鍵長 128-bit 時) 9.8 (鍵長 192-bit 時) 8.5 (鍵長 256-bit 時)
パフォーマンス <sup>3</sup>	
最高動作周波数 <sup>3</sup>	222MHz
最高データ速度 <sup>3</sup>	2.5Gbps (鍵長 128-bit 時) 2.1Gbps (鍵長 192-bit 時) 1.8Gbps (鍵長 256-bit 時)
パッケージ構成 <sup>4</sup>	
配布形式	VHDL ソースコード
検証方法	VHDL テストベンチ
添付ドキュメント	ユーザーズマニュアル

注:

1. IP-AES-EP は IP-AES-xP ファミリの Engine 部分ですので、対応するオペレーション・モードは ECB のみです。ECB 以外のオペレーション・モードが必要なお客様は、IP-AES-128P など、オペレーション・モード付きの製品をお選びください。
2. スピードファクタは、最高データ速度と最高動作周波数の比 (= 最高データ速度/最高動作周波数) です。
3. Xilinx XC5V LX50-3 における評価値です。
4. ファイルは CD-R に記録して提供されます。

## 概要

AES (Advanced Encryption Standard) は、米国商務省標準技術局(NIST)によって、米連邦情報処理標準 (FIPS)として選定された秘密鍵暗号です。AES は、通信システムの情報秘匿、記憶媒体やデータベースの情報秘匿、著作権保護、電子決済など、様々な分野で利用されています。

IP-AES-EP は、NIST の FIPS-197 に完全準拠するデータ入出力幅 128-bit の AES Engine です。IP-AES-EP では、部分的に並列&パイプライン処理を行うことによって、スピード・ファクタ 8.5 ~ 11.6 を達成しています。

なお、IP-AES-EP は IP-AES-xP ファミリの Engine 部分ですので、対応するオペレーション・モードは ECB のみです。ECB 以外のオペレーション・モードが必要なお客様は、IP-AES-128P など、オペレーション・モード付きの製品をお選びください。

## ブロック図

IP-AES-EP の Pinout は次のようになっています。

図 1 : Decoder の Pinout

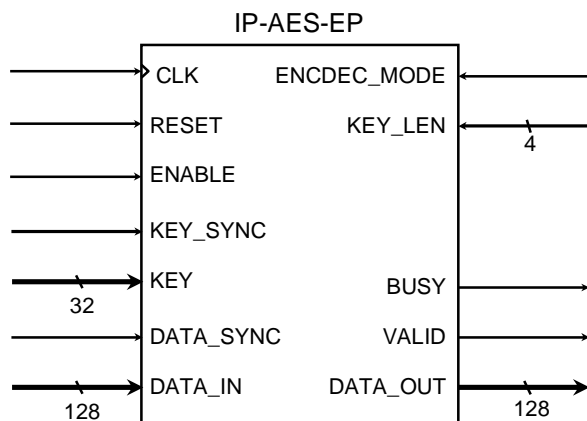


表 2 : I/O Description

信号名	I/O	Description
CLK	I	システムクロック
RESET	I	システムリセット (非同期)
ENABLE	I	システムイネーブル
ENCDEC_MODE	I	暗号化/復号化のモード指定 0 暗号化, 1 復号化
KEY_LEN	I	暗号鍵長を指定する (2bit) 0 128, 1 192, 2 256
KEY_SYNC	I	暗号鍵ワードが先頭の暗号鍵ワード
KEY_IN	I	暗号鍵ワード (32bit)
DATA_SYNC	I	入力データが有効
DATA_IN	I	入力データ (128bit)
BUSY	O	データ入力禁止
VALID	O	出力データが有効
DATA_OUT	O	出力データ (128bit)

なお、以上において、CLK は立ち上がりエッジでトリガされます。また、RESET, ENABLE などの制御信号は、すべてポジティブ・ハイです。

## ベンチマーク

例えば、Xilinx XC5V LX50-3 では、次のような特性が得られます。

表 3 : IP-AES-EP のベンチマーク

スライス数	BRAM 数	動作速度
833	4	222MHz

CLK にタイミング制約を付けて、ISEの Properties を Global Effort を High / Normal、Speed 優先にして、コンパイル。

## 注意事項

本製品に関する直接的かつ技術的な問題については、製品ご購入後 1 年間、無償でサポートいたします。

本製品や本製品搭載装置を海外に持ち出される場合には、輸出貿易管理令や外国為替令などの輸出規制をご確認のうえ、必要な手続きをお取りください。