

# DES Cryptosystem IP-DES-64P

September 30, 2004

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
- DES Cryptosystem
- 暗号鍵長: 64-bit
- 暗号鍵入力ポート幅: 64-bit
- データ入出力ポート幅: 64-bit
- オペレーションモード: ECB, CBC, CFB, OFB
- 最高動作周波数: 127MHz  
Xilinx XC2V1000-6 における評価値
- 最高データ速度: 508Mbps  
Xilinx XC2V1000-6 における評価値
- スピード・ファクタ: 4  
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-DES-64P 仕様

設計パラメータ	
オペレーションモード	ECB, CBC, CFB, OFB
暗号鍵入力幅(bit)	64
データ入出力幅(bit)	64
レイテンシー(clock)	16+1
スピードファクタ <sup>1</sup>	4
パフォーマンス <sup>2</sup>	
最高動作周波数 <sup>2</sup>	127MHz
最高データ速度 <sup>2</sup>	508Mbps
パッケージ構成 <sup>3</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. 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。
2. Xilinx XC2V1000-6 における評価値です。
3. ファイルは CD-R に記録して提供されます。

### 概要

DES (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。DES 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-DES-64P は、FIPS 46-2, FIPS 81 に完全準 拠するデータ入出力幅 64-bit の DES です。

### ブロック図

IP-DES-64P の Pinout は次のようになってい ます。

図 1 : Decoder の Pinout

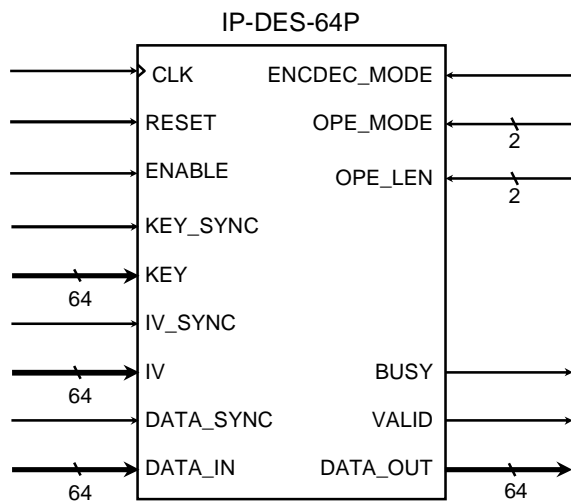


表 2 : I/O Description

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

OPE_MODE	I	オペレーションモードを指定する(2bit) 0 ECB, 1 CBC, 2 CFB, 3 OFB
OPE_LEN	I	オペレーションモード CFB,OFB 時におけるデータ 入出力幅を指定する(2bit) 0 1, 1 8, 2 32, 3 64
KEY_SYNC	I	暗号鍵が有効
KEY	I	暗号鍵(64bit)
IV_SYNC	I	初期化ベクトルが有効であ
IV	I	初期化ベクトル(64-bit)
DATA_SYNC	I	入力データが有効
DATA_IN	I	入力データ (64bit)
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 (64bit)

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 XC2V1000-6 では、次のような 特性が得られます。

表 3 : IP-DES-64P のベンチマーク

スライス数	BRAM 数	動作速度
1026	0	129 MHz

### 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製品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。