

Triple-DES Cryptosystem IP-TDES-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
- Triple-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, CBC-I, CFB-P, OFB-I
- 最高動作周波数: 99MHz
Xilinx XC2V1000-6 における評価値
- 最高データ速度: 132Mbps (396Mbps)
Xilinx XC2V1000-6 における評価値
括弧内は、パイプラインモード時の値
- スピード・ファクタ: 1.33 (4)
最高データ速度/最高動作周波数
括弧内は、パイプラインモード時の値

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-TDES-64P 仕様

設計パラメータ	
オペレーションモード ¹	ECB, CBC, CFB, OFB, CBC-I, CFB-P, OFB-I
暗号鍵入力幅(bit)	64
データ入出力幅(bit)	64
レイテンシー(clock)	48+1
スピードファクタ ²	1.33 (4)
パフォーマンス ³	
最高動作周波数 ³	99MHz
最高データ速度 ³	132Mbps (396Mbps)
パッケージ構成 ⁴	
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	ユーザズマニュアル

注:

1. DES として動作させる場合には、ECB, CBC, CFB, OFB モードをサポートします。
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。括弧内は、パイプラインモード時の値です。
3. Xilinx XC2V1000-6 における評価値です。括弧内は、パイプラインモード時の値です。
4. ファイルは CD-R に記録して提供されます。

概要

Triple DES は、アメリカ規格協会(ANSI)によって、1981 年に ANSI X.3.92 として標準化された秘密鍵暗号です。Triple DES は、米連邦情報処理標準 (FIPS)としても選定され、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-TDES-64P は、ANSI X.3.92 に完全準拠したデータ入出力幅 64-bit の Triple-DES です。

ブロック図

IP-TDES-64P の Pinout は次のようになっています。

図 1 : Decoder の Pinout

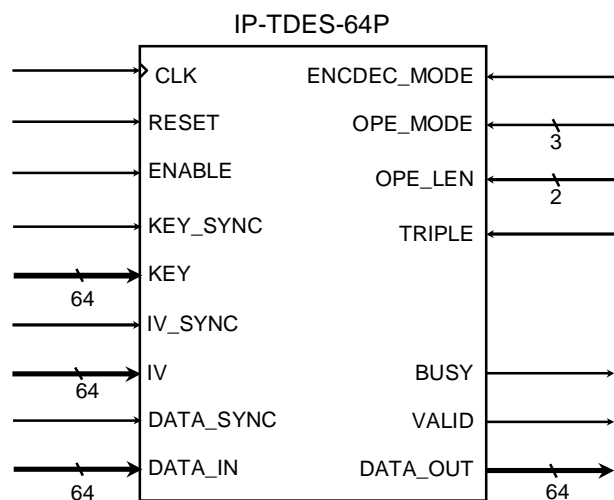


表 2 : I/O Description

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
ENCODEC_MODE	I	暗号化/復号化のモード指定

		0 暗号化, 1 復号化
TRIPLE	I	DES/TDES のモード指定 0 DES, 1 TDES
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, 5 CBC-I, 6 CFB-P, 7 OFB-I
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_IN	I	暗号鍵(64bit)
IV_SYNC	I	初期化ベクトルが有効である
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-TDES-64P のベンチマーク

スライス数	BRAM 数	動作速度
2,050	0	99 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。