

SHA-2 Hash Function (64-bit) IP-SHA2-64

June 30, 2007

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
- Hash Function
- データ入力ポート幅: 64-bit
- データ出力ポート幅: 384-bit (SHA-384),
512-bit (SHA-512)
- レイテンシー: $2T+1\sim 2T+16$
データ系列の入力が完了してからハッシュ関数の出力が確定するまでのクロック数。
データ系列の長さによって、変動します。
 $T=161$
- 最高動作周波数: 196MHz
Xilinx XC5V LX30-3 における評価値
- 最高データ速度: 1,132Mbps
Xilinx XC5V LX30-3 における評価値
- スピード・ファクタ: 5.78
最高データ速度/最高動作周波数

応用分野

- ユーザー認証
- 著作権保護
- 電子決済

表 1 : IP-SHA2-64 仕様

設計パラメータ	
データ入力幅(bit)	64
データ出力幅(bit)	384 (SHA-384) 512 (SHA-512)
レイテンシー(clock)	$2T+1\sim 2T+16$ where: $T=161$
スピードファクタ ¹	5.78
パフォーマンス ²	
最高動作周波数 ²	196 MHz
最高データ速度 ²	1,132 Mbps
パッケージ構成 ³	
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です。
2. Xilinx XC5V LX30-3 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

SHA-2 は、米国標準技術局 (NIST) が規格化した米国政府標準ハッシュ関数 (FIPS 180-2) です。これは、SHA-1 の上位規格であり、SHA-1 に加えて、ハッシュ関数 SHA-256、SHA-384、SHA-512 が新たに規格化されています。

IP-SHA2-64 は、FIPS 180-2 の SHA-384 と SHA-512 に完全準拠する SHA-2 IP コアで、64-bit ずつ入力されるデータストリームに対して、 $6 \times 64 = 384\text{-bit}$ あるいは $8 \times 64 = 512\text{-bit}$

SHA-2 Hash Function (64-bit) IP-SHA2-64

のハッシュ値を出力します。IP-SHA2-64 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 5.78 を達成しています。

ブロック図

IP-SHA2-64 の Pinout は次のようになっています。

図 1 : IP-SHA2-64 の Pinout

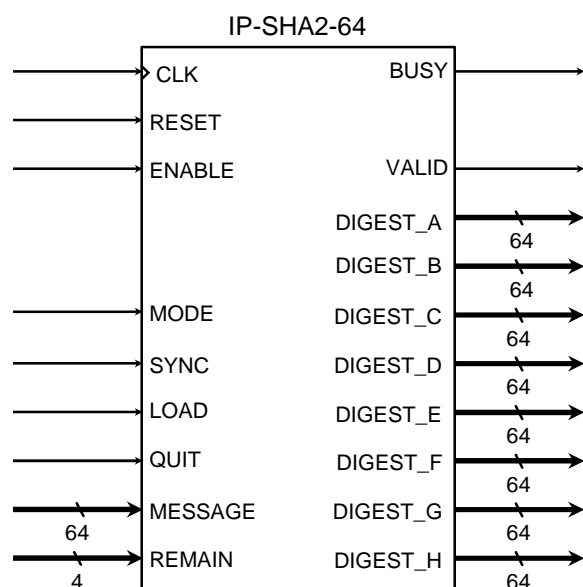


表 2 : IP-SHA2-64 の I/O Description

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
MODE	I	ハッシュ関数の選択
SYNC	I	MESSAGE がデータ系列の先頭にある
LOAD	I	MESSAGE を入力する
QUIT	I	MESSAGE がデータ系列の末尾にある
MESSAGE	I	入力データ (64-bit)
REMAIN	I	MESSAGE で使われていないバイト数
VALID	O	出力データが有効である
DIGEST_A	O	出力データ (ハッシュ値 A)

DIGEST_B	O	出力データ (ハッシュ値 B)
DIGEST_C	O	出力データ (ハッシュ値 C)
DIGEST_D	O	出力データ (ハッシュ値 D)
DIGEST_E	O	出力データ (ハッシュ値 E)
DIGEST_F	O	出力データ (ハッシュ値 F)
DIGEST_G	O	出力データ (ハッシュ値 G)
DIGEST_H	O	出力データ (ハッシュ値 H)
BUSY	O	データ入力禁止

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 FPGA では、次のような特性が得られます。

表 3 : IP-SHA2-64 のベンチマーク

ターゲットデバイス	スライス数	BRAM 数	動作速度
XC4V LX25-12	2889	0	151 MHz
XC5V LX30-3	1224	0	196 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。