MS60401IP

SHA1 Operation IP Module (Verilog-HDL)

■ 概 要

MS60401IP は、機器の認証等の使用を想定した Secure Hash Algorithm 1 に基づく Hash 演算を行う IP モジュールです。512bit の data から 160bit の Hash 値を求めます。

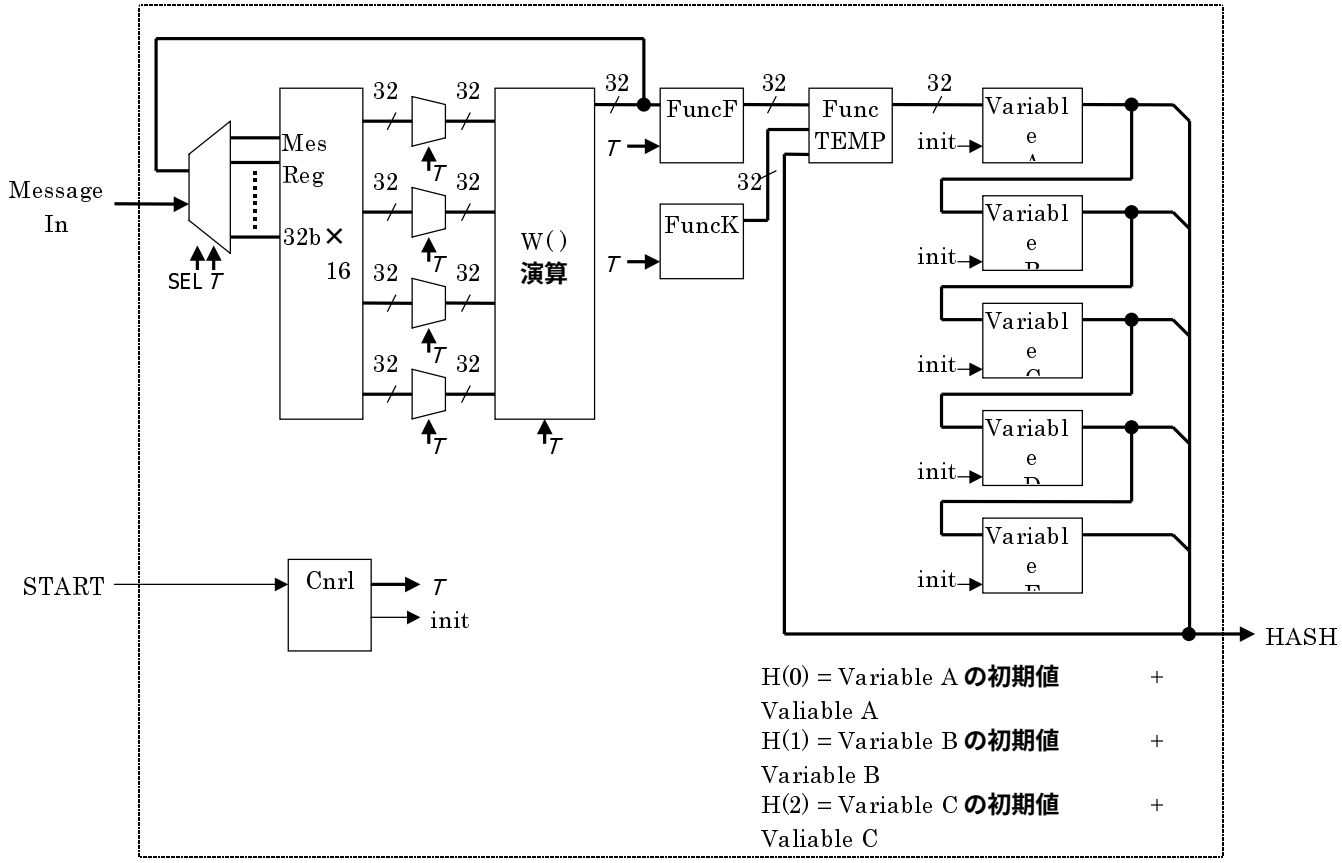
■ 特 長

- ●入力される Message Digest は 512bit 固定
- ●Hash 演算時間は入力クロックの 80clk
- ●BUSY 端子により演算中を表示
- ●START 信号により初期化の後演算開始
- ●FIPS180-1 Secure Hash Standard 準拠

■ 入出力信号

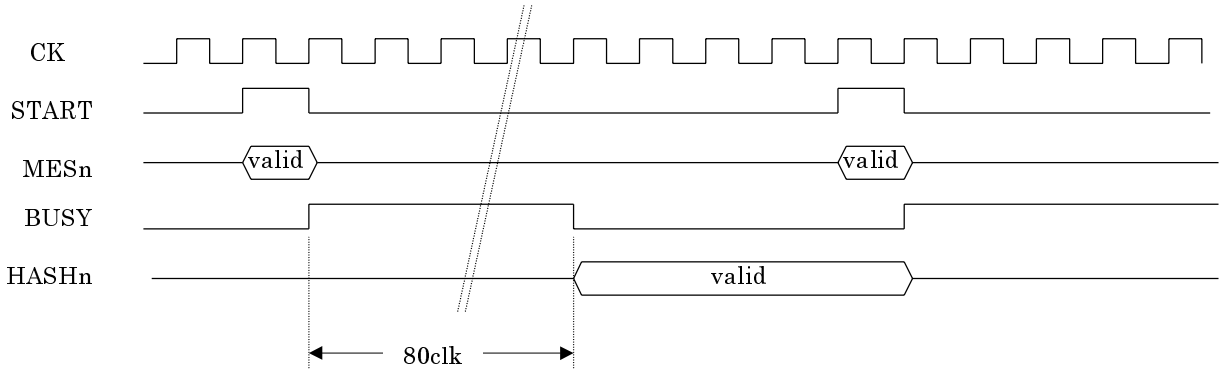
信号名	I/O	極性	信号説明
MES0[31:0]	I		Message Digest 入力．0～31Bit
MES1[31:0]	I		〃 32～63Bit
MES2[31:0]	I		〃 64～95Bit
MES3[31:0]	I		〃 96～127Bit
MES4[31:0]	I		〃 128～159Bit
MES5[31:0]	I		〃 160～191Bit
MES6[31:0]	I		〃 192～223Bit
MES7[31:0]	I		〃 224～255Bit
MES8[31:0]	I		〃 256～287Bit
MES9[31:0]	I		〃 288～319Bit
MESA[31:0]	I		〃 320～351Bit.
MESB[31:0]	I		〃 352～383Bit
MESC[31:0]	I		〃 384～415Bit
MESD[31:0]	I		〃 416～447Bit
MESE[31:0]	I		〃 448～479Bit
MESF[31:0]	I		〃 480～511Bit
START	I	H	Hash 演算開始トリガ．クロック 1ck 分の H パルス． この信号で Message Digest をこのモジュール内にとりこみ演算を開始します． BUSY 中の START 検出は演算再起動となります．
(MULTI)	I	H	Multi-Block Message 処理を指示する信号です． 0 で One-Block Message. 1 で Multi-Block Message です． なおこの機能はオプションです，
H0[31:0]	O		Hash 値出力．H0．Hash 値は BUSY=0 のときのみ有効です．
H1[31:0]	O		〃 H1
H2[31:0]	O		〃 H2
H3[31:0]	O		〃 H3
H4[31:0]	O		〃 H4
BUSY	O	H	Busy 出力．Hash 演算中'1'．START トリガ入力後，'1'の期間 Hash 値は Invalid． BUSY 期間は START トリガから 80CK(固定)です．
CK	I		Clock．ポジエッジ動作．
RSTN	I	L	Asynchronous Reset．Low Active．

■ ブロック図

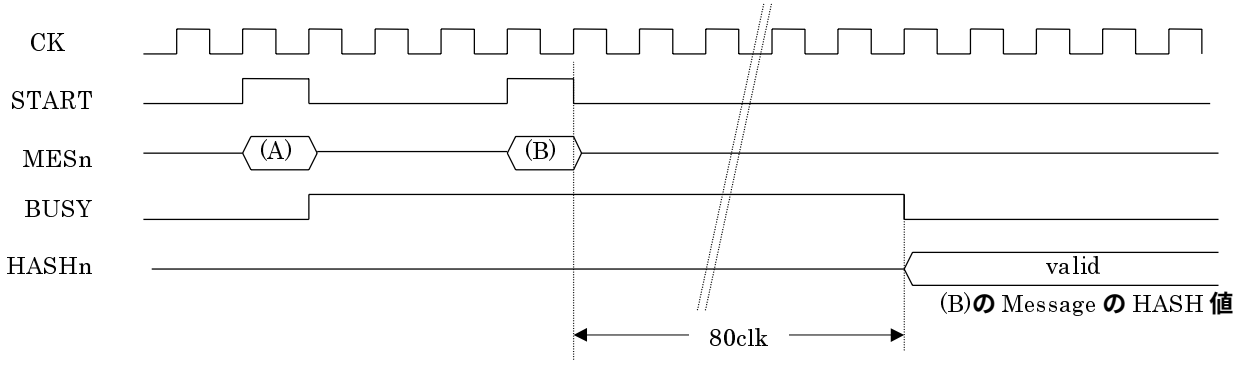


■ タイムチャート

1—1) 外部タイミング（通常）



1—2) 外部タイミング(BUSY 期間中の再スタート)



1.本書に記載された内容につきましては、改善のため予告なしに変更することがあります。
2.本書に記載された情報や図面等の使用に起因した等三者の所有する工業所有権およびその他の権利侵害に対し当社はその責任を負うものではありません。
3.本書に記載された内容を当社に無断で転載または複製することは、ご遠慮下さい。
4.本書に記載された製品は「外国為替及び外国貿易管理法」に基づく戦略物質等に該当します。従って本製品を輸出する場合は、同法に基づく許可が必要となります。

〒407-0014 山梨県韮崎市富士見 3-16-37
TEL 0551-23-0575
FAX 0551-23-0576
http://www.megasys.co.jp/