SHS(Secure Hash Standard：FIPS PUB 180-3)準拠

SHA-1/224/256/384/512Core

<1.Core について>

セキュアハッシュ標準規格　SHS(Secure Hash Standard:FIPS PUB 180-3)における FIPS PUB 180-3 準拠の SHA-1/224/256/384/512 の Core にあたり **1 つの Core** で **SHA-1/224/256/384/512 のすべてに対応**している点を特徴としています。

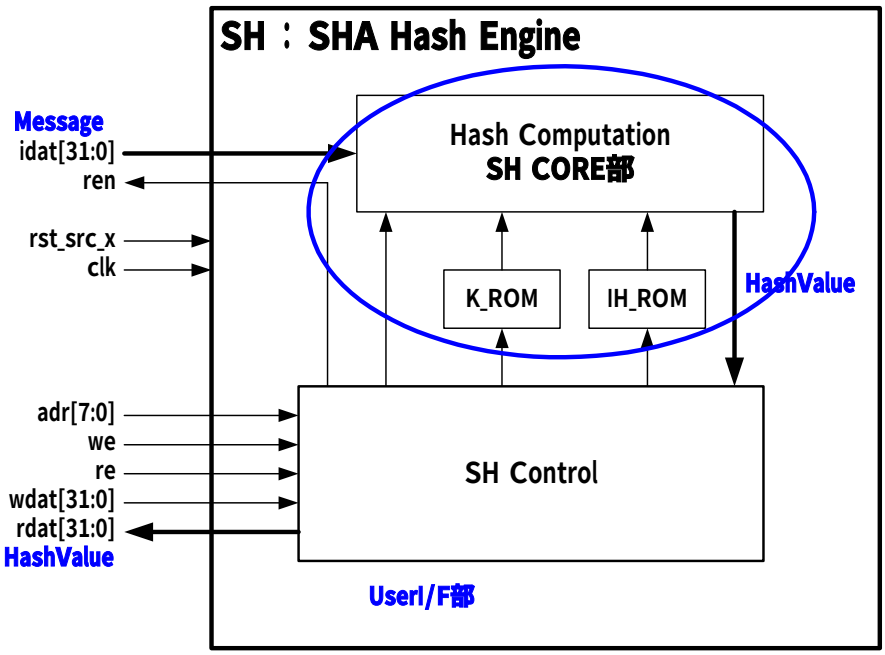
ASIC/FPGA をターゲットとし、処理レートは ASIC 時 **1.2Gbps**/FPGA 時 **600Mbps** を実現しています。

ご提供の際には Core 部とともに、User I/F を付属してご提供致します。

<2.Spec>

以下に、SHA システムのブロック図を示します。

青丸で示す部分が SHA Core 部にあたります。（それ以外の部分は User I/F）



-Core 仕様

規格	FIPS PUB 180-3(SHS)規格準拠		SHA-1　(Hash 値長 160bit)	対応
			SHA-224(Hash 値長 224bit)	対応
			SHA-256(Hash 値長 256bit)	対応
			SHA-384(Hash 値長 384bit)	対応
			SHA-512(Hash 値長 512bit)	対応
			Message 長	最大 4Gbyte
			Padding 処理	対応
構成	SHA ブロックの 1 ブロック構成			
Round 処理	SHA-1		パイプラインなし **1 クロックサイクル**	
	SHA-224/256/384/512		パイプラインなし **2 クロックサイクル**	
処理レート	ASIC 時	SHA-1	**1,233Mbps**	
		SHA-224/256	**787Mbps**	
		SHA-384/512	**1,264Mbps**	
	FPGA 時	SHA-1	**616Mbps**	
		SHA-224/256	**393Mbps**	
		SHA-384/512	**632Mbps**	

-入出力 I/F

入力 Data Bus	入力 **32bit** Data Bus	SHA-1	16Cycle/Block
		SHA-224/256	16Cycle/Block
		SHA-384/512	32Cycle/Block
出力(Hash 計算結果)	レジスタアクセス		
制御	レジスタアクセス	mode 設定	
		処理 byte 設定, Padding 用 Total Message Length 設定	
		Hash 計算開始・Busy・完了フラグ	
		処理 byte 数 SnapShot レジスタ	

-システム関連

クロック	1 系統単相同期	ASIC 時	**200MHz**
		FPGA 時	**100MHz**
リセット	1 系統非同期		
信号数	**109 本**		
内部 ROM	32index ×32bit　2 個,　128index×32bit　1 個		
ターゲットテクノロジ	ASIC/FPGA		

株式会社シーデックス

〒206-0804　東京都稲城市百村 1623-1　パストラルハイム稲城ビル

Tel:042-378-5999　Fax:042-378-5998　http://www.cdex.co.jp