SHS(Secure Hash Standard:FIPS PUB 180-3)
SHA-1/224/256/384/512Core

<1.Introduction>

The SHA core is full compliance with SHS(Secure Hash Standard:FIPS PUB 180-3 **SHA-1/224/256/384/512**).

The core's target is ASIC/FPGA.

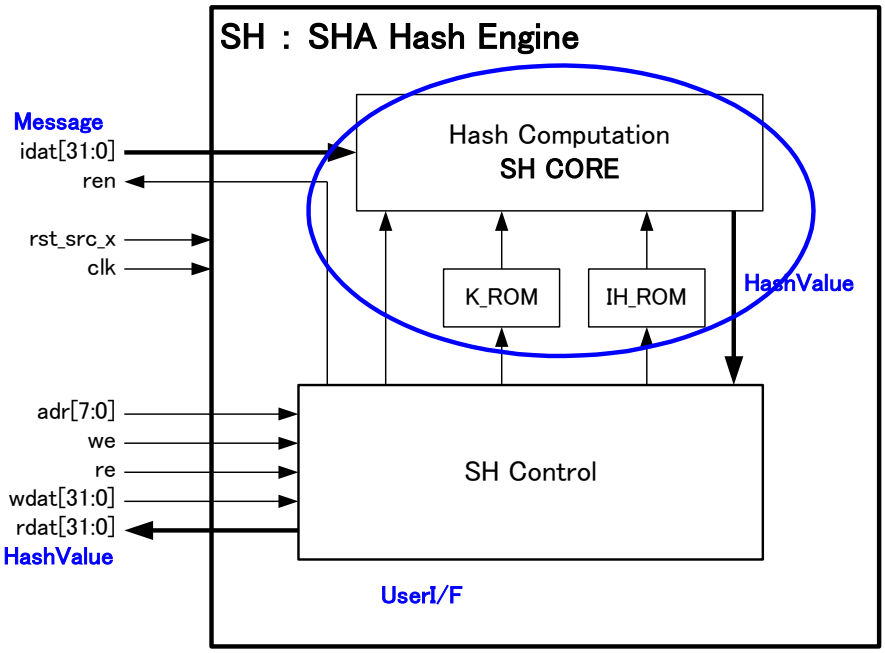
The high performance which achieves the throughput **1.2Gbps** at ASIC / **600Mbps** at FPGA is the feature.

We offer the core module with user interface design.

<2.Features>

The figure below shows a block diagram of the SHA system.

The SHA cores are shown by the blue encircled modules. (The other modules are user interface.)



-Core Features

Standards	FIPS PUB 180-3(SHS)		SHA-1 (Hash Length160bit)	supported
			SHA-224(Hash Length224bit)	supported
			SHA-256(Hash Length256bit)	supported
			SHA-384(Hash Length384bit)	supported
			SHA-512(Hash Length512bit)	supported
			Message Length	max 4Gbyte
			Padding Process	supported
Structure	SHA : 1core			
Round Process	SHA-1		Non-pipelined **1clock cycle**	
	SHA-224/256/384/512		Non-pipelined **2 clock cycle**	
Throughput	ASIC	SHA-1	**1,233Mbps**	
		SHA-224/256	**787Mbps**	
		SHA-384/512	**1,264Mbps**	
	FPGA	SHA-1	**616Mbps**	
		SHA-224/256	**393Mbps**	
		SHA-384/512	**632Mbps**	

-Input/Output I/F

Input Data Bus	Input **32bit** Data Bus	SHA-1	16Cycle/Block
		SHA-224/256	16Cycle/Block
		SHA-384/512	32Cycle/Block
Output(Hash Result)	Register Access		
Registers	Register Access	mode setting	
		Processing byte setting, Padding Total Message Length setting	
		Hash_Calc_Start・Busy・Done_flag	
		Processing byte SnapShot register	

-System

Clock	Single Synchronous Clock	ASIC	**200MHz**
		FPGA	**100MHz**
Reset	Single Asynchronous Reset		
Total pins	**109pin**		
ROM	32index ×32bit × 2, 128index×32bit × 1		
Target Technology	ASIC/FPGA		

株式会社シーデックス Cdex.Co.,Ltd.

〒206-0804 1623-1, Momura, Inagi-shi, Tokyo, Japan

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