AES(Advanced Encryption Standard:FIPS PUB 197) Encryption/Decryption Core

<1.Introduction>

The Crypto core is full compliance with AES(Advanced Encryption Standard ： FIPS PUB 197).

The core's target is ASIC/FPGA.

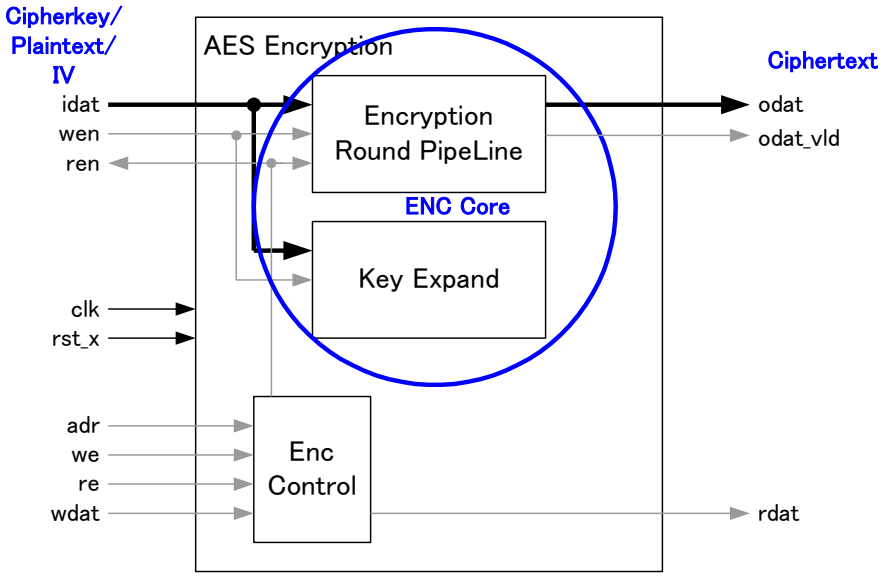
The high performance which achieves the encryption/decryption throughput **more than 8Gbps** at ASIC / **4Gbps** at FPGA is the feature.

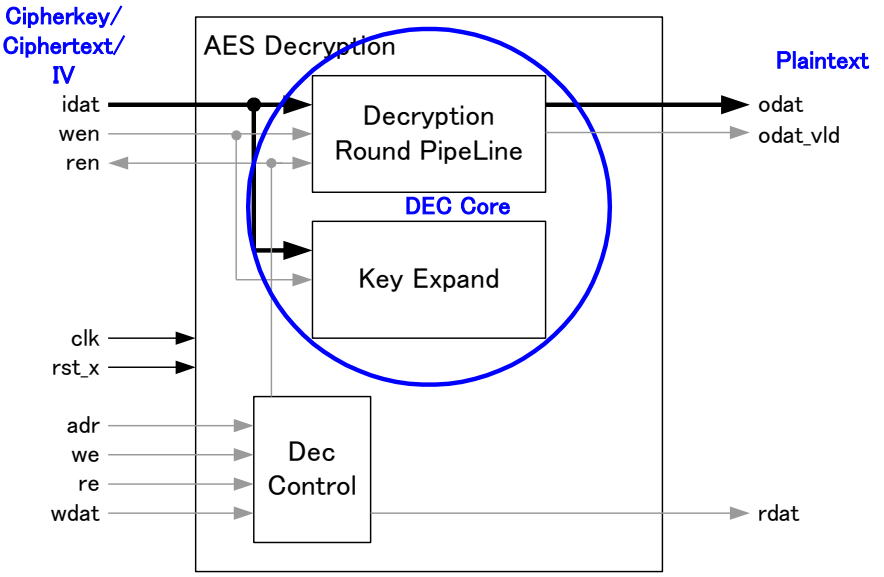
We offer the core module with user interface design.

<2.Features>

The figure below shows a block diagram of the AES encryption/decryption system.

The encryption/decryption cores are shown by the blue encircled modules. (The other modules are user interface.)





-Core Features

Standards	FIPS PUB 197(AES)		AES-128(Key length128bit)	supported
			AES-192(Key length192bit)	supported
			AES-256(Key length 256bit)	supported
			Block Size	128bit (fixed)
	NIST Special Publication 800-38A		ECB(Electronic CodeBook Mode)	supported
			CBC(Cipher Block Chaining Mode)	supported
Structure	Encryption core(ENC) / Decryption core(DEC) : 2cores			
Round Pipeline	ECB(Electronic CodeBook Mode)		**4/5/5 stage(128/192/256bit mode) Pipelined**	
	CBC(Cipher Block Chaining Mode)		**Non-pipelined 4/5/5clock cycles(128/192/256bit mode)**	
Key Expand	**5/4/4 clock(128/192/256bit mode)**			
Throughput	ASIC	ECB(Electronic CodeBook Mode)	**>8Gbps**	
		CBC(Cipher Block Chaining Mode)	**3.2Gbps/2.5Gbps/2.5Gbps**	
	FPGA	ECB(Electronic CodeBook Mode)	**>4Gbps**	
		CBC(Cipher Block Chaining Mode)	**1.6Gbps/1.25Gbps/1.25Gbps**	

-Input/Output I/F

Input Data Bus	Input **128bit** Data Bus	ENC	Plaintext	128bit
			Cipher key	128/192/256bit
			IV(Initialization Vectors)	128bit
		DEC	Cipher text	128bit
			Cipher key	128/192/256bit
			IV(Initialization Vectors)	128bit
Output Data Bus	Output **128bit** Data Bus	ENC	Cipher text	128bit
		DEC	Plaintext	128bit
Registers	Register Access	mode setting		
		Processing byte setting		
		Encryption/Decryption_Start・Busy・Done_flag		
		Processing byte SnapShot register		

-System

Clock	Single Synchronous Clock	ASIC	**100MHz**
		FPGA	**50MHz**
Reset	Single Asynchronous Reset		
Total pins	**333pin**		
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