AES(Advanced Encryption Standard：FIPS PUB 197)準拠

暗号化・復号化 Core

<1.Core について>

共通鍵ブロック暗号 AES(Advanced Encryption Standard：FIPS PUB 197)における FIPS PUB 197 準拠の暗号化・復号化 Engine の Core にあたります。

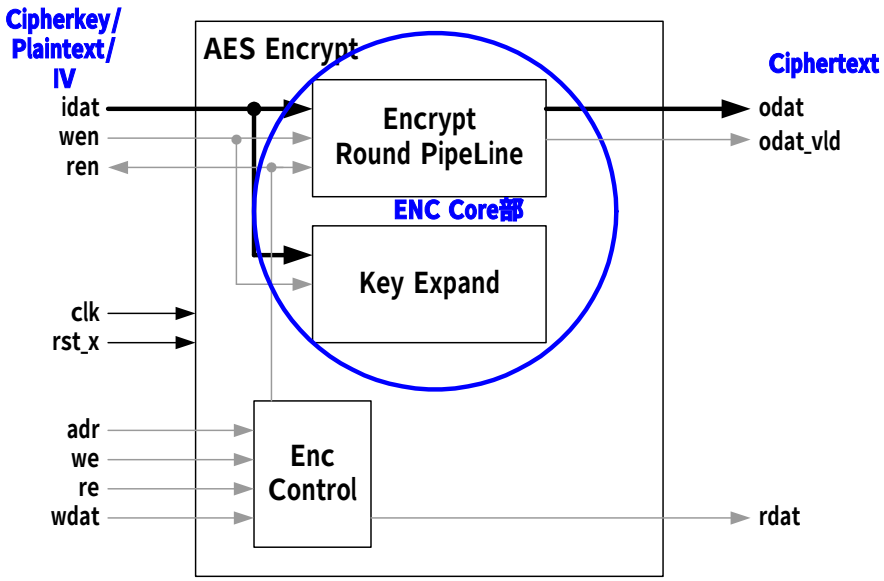
ASIC/FPGA をターゲットとし、ASIC 時 8Gbps 以上/FPGA 時 4Gbps 以上の暗号化・復号化レートを実現する High パフォーマンスを特徴としています。

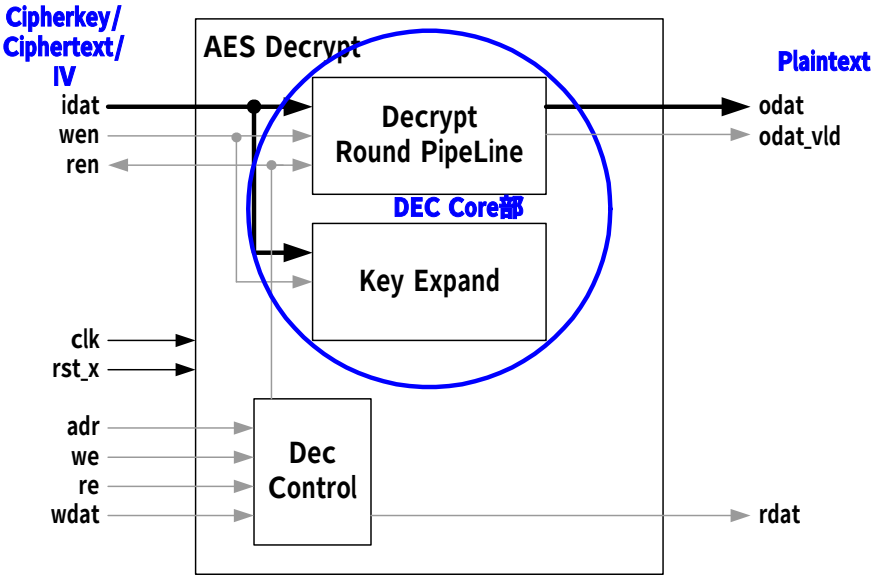
ご提供の際には Core 部とともに、User I/F を付属してご提供致します。

<2.Spec>

以下に、AES 暗号化/復号化システムのブロック図を示します。

青丸で示す部分が ENC/DEC 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 197(AES)規格準拠	AES-128(鍵長 128bit)	対応
		AES-192(鍵長 192bit)	対応
		AES-256(鍵長 256bit)	対応
		ブロック長	128bit 固定
	NIST Special Publication 800-38A	ECB(Electronic CodeBook Mode)	対応
		CBC(Cipher Block Chaining Mode)	対応
構成	Encrypt ブロック(以降 ENC)･Decrypt ブロック(以降 DEC)の 2 ブロック構成		
Round パイプライン	ECB(Electronic CodeBook Mode)	4/5/5 段(128/192/256bit 時)パイプライン	
	CBC(Cipher Block Chaining Mode)	パイプラインなし 4/5/5 クロックサイクル(128/192/256bit 時)	
Key Expand 生成	5/4/4 クロック(128/192/256bit 時)		

処理レート	ASIC 時	ECB(Electronic CodeBook Mode)	8Gbps 以上
		CBC(Cipher Block Chaining Mode)	3.2Gbps/2.5Gbps/2.5Gbps
	FPGA 時	ECB(Electronic CodeBook Mode)	4Gbps 以上
		CBC(Cipher Block Chaining Mode)	1.6Gbps/1.25Gbps/1.25Gbps

-入出力 I/F

入力 Data Bus	入力 128bit Data Bus 以下を Mux し共用 Bus とする	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
出力 Data Bus	出力 128bit Data Bus	ENC	Cipher text	128bit
		DEC	Plaintext	128bit
制御	レジスタアクセス	mode 設定		
		処理 byte 設定		
		Encrypt/Decrypt 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	100MHz
		FPGA 時	50MHz
リセット	1 系統非同期		
信号数	333 本		
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