YDK株式会社ワイ・デー・ケー

FPGA用　AES暗復号　IPコア

データ秘匿の高速化　H/Wエンジン

株式会社ワイ・デー・ケー

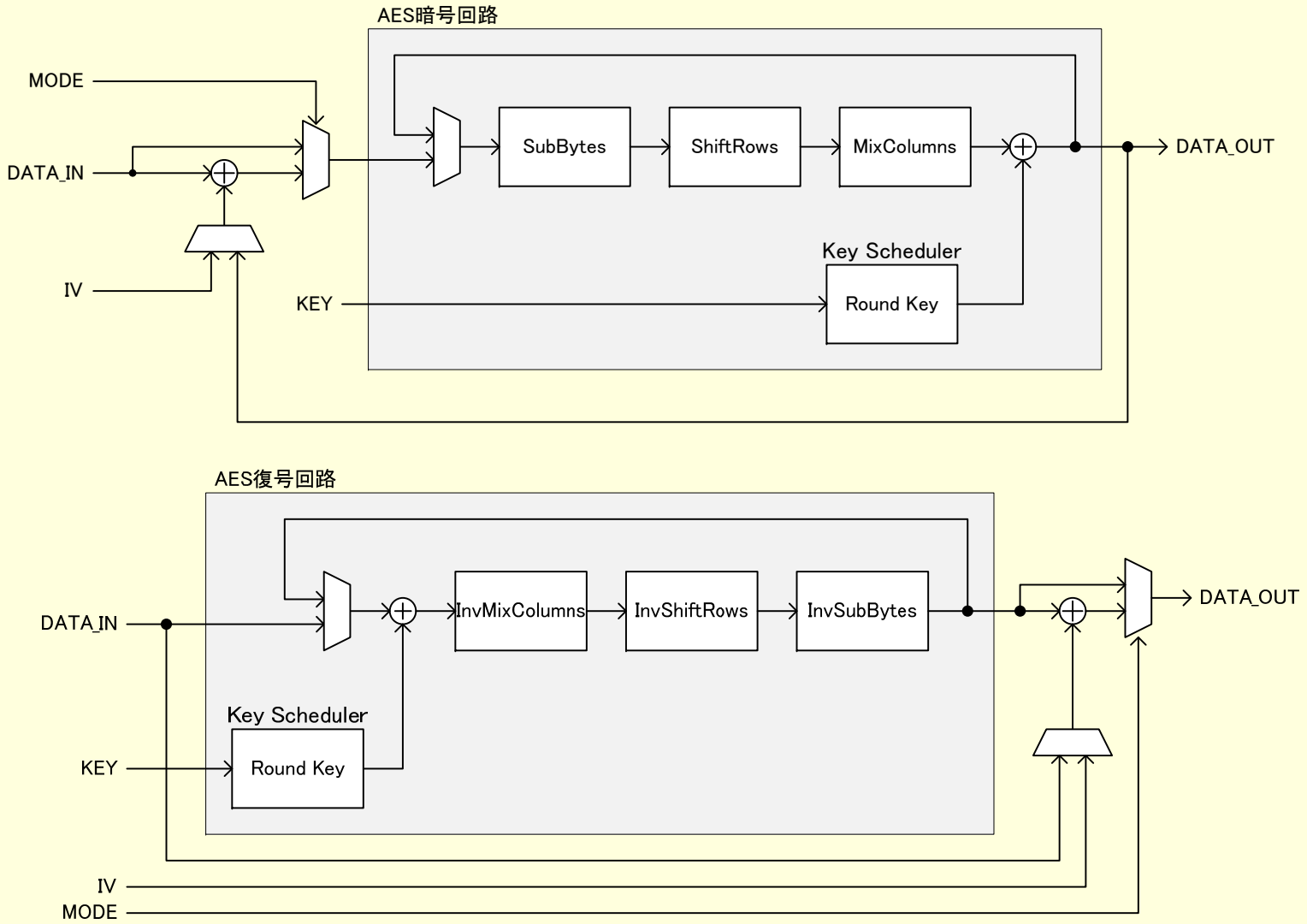
特徴

yCORE-AESはFPGA向けのAES（Advanced Encryption Standard)暗復号用IPコアです。本IPコアは鍵長128bitに対応しております。標準で暗号利用モードCBCも対応しております。

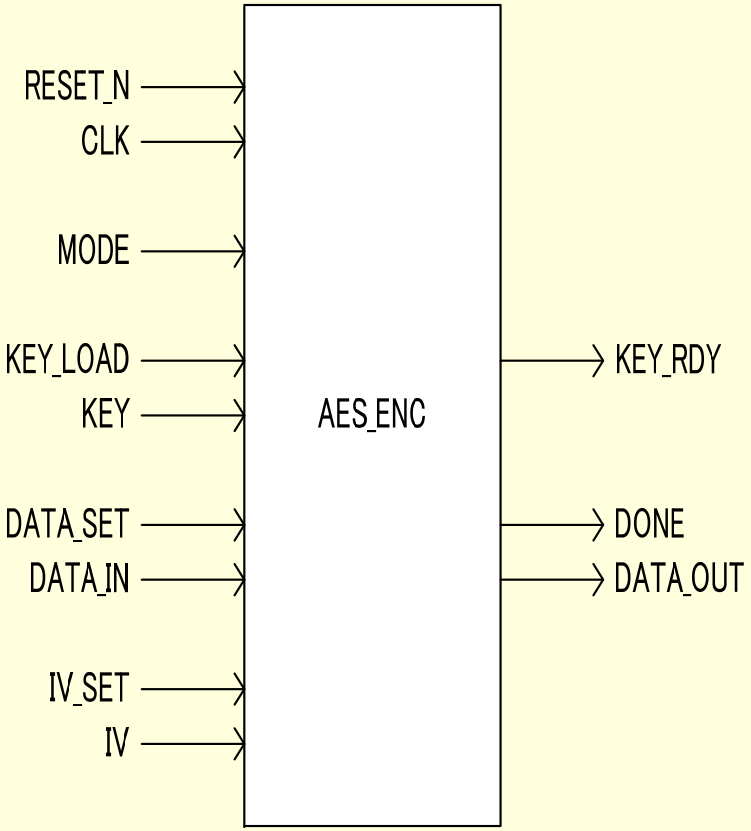
ターゲットカスタマイズ対応可能

yCORE-AESは弊社でフルスクラッチで設計したFPGA用AES暗復号 IPコアです。
Altera®社製Stratix2®,Arria2® の実装実績があります。
また、搭載機器の仕様に合わせてカスタマイズにも柔軟に対応可能です。
既存ターゲットのホストインタフェース、鍵長、暗号利用モード、超高速化（パイプライン処理）など、お気軽にお問い合わせ下さい。

ブロック構成


AES暗号回路
MODE
DATA_IN
IV
KEY
SubBytes
ShiftRows
MixColumns
Key Scheduler
Round Key
DATA_OUT
AES復号回路
DATA_IN
KEY
IV
MODE
InvMixColumns
InvShiftRows
InvSubBytes
Key Scheduler
Round Key
DATA_OUT

インタフェース



信号名	I/O	機能
RESET_N	I	非同期リセット
CLK	I	クロック
MODE	I	暗号モード選択
KEY_LOAD	I	キーロード
KEY[127:0]	I	キー入力
KEY_RDY	O	キーレディー
DATA_SET	I	データセット
DATA_IN[127:0]	I	データ入力
DATA_OUT[127:0]	O	データ出力
DONE	O	完了通知
IV_SET	I	IVセット
IV[127:0]	I	IV入力

yCORE-AESの主な仕様

◇ECBモード　NIST FIPS PUB 197 ECBモード準拠
　平分：128bit/暗号文：128bit
　鍵長：128bit（192bit/256bit対応可能）
◇CBCモード　NIST FIPS PUB 197 CBCモード準拠
　平分：128bit/暗号文：128bit
　鍵長：128bit（192bit/256bit対応可能）
　IV　：128bit
◇ソースコード提供
◇ ロイヤリティフリー

容量/性能例

条件：Altera®社製Stratix2、AES　ECBモード暗号回路
◇回路容量例
・ALUTs：694、Registers：527、ALMs：557、M4Ks：8
◇性能例
・約700Mbit/s（レイテンシ：12クロック、周波数：66MHz）

問い合わせ先：YDK 株式会社 ワイ・デー・ケー　http://www.ydkinc.co.jp/
営業本部　〒206-0811　東京都稲城市押立1705番地
TEL 042-378-8511　高橋、渡辺、井上