TECHNO CREATE

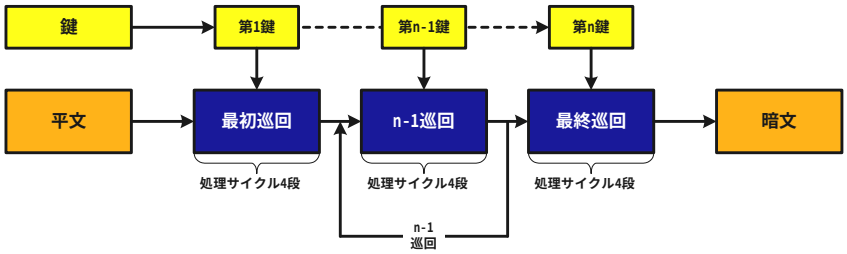
AES 暗号／復号エンジン

本製品は、標準的な共通鍵暗号『AES（Advanced Encryption Standard)』暗号／復号エンジンです。
３種類の暗号鍵長 (AES-128/AES-192/AES-256) をサポートしています。

- **NIST FIPS-197 準拠**
- **暗号化／復号化を１パッケージで実現**
- **ECB/CBC/CTR の動作モードをサポート (※1)**
- **128bit/192bit/256bit の鍵拡張機能を標準搭載 (※2)**
- **最大処理速度 約 110Mbps を実現し、ネットワークセキュリティ機器への応用が可能 (※3)**

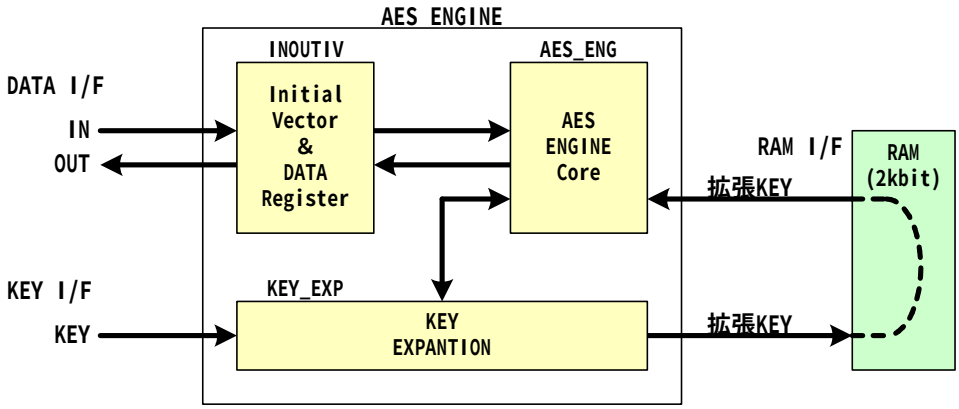
(※1) カスタマイズにより OFB、CFB モードにも対応可能です。
(※2) 拡張鍵を外部から書込むようにカスタマイズすることで規模の縮小が可能です。
(※3) ALTERA Cyclone3 デバイスにおいて、AES-128、動作クロック 40MHz とした場合の AES 処理速度です。転送速度(スループット)については、AES 処理速度に加え、本 AES ENGINE IP に対するデータ書込み/読出し時間を考慮する必要があります。

【AES 暗号化のアルゴリズム】



AES (Rijndael) は DES より高い安全性で、Triple-DES より高速な特長を持つ、128bit を処理単位とした、共通鍵ブロック暗号です。 アルゴリズムは米国連邦情報処理標準規格 (NIST FIPS－197) に準拠しています。

【ブロック図】



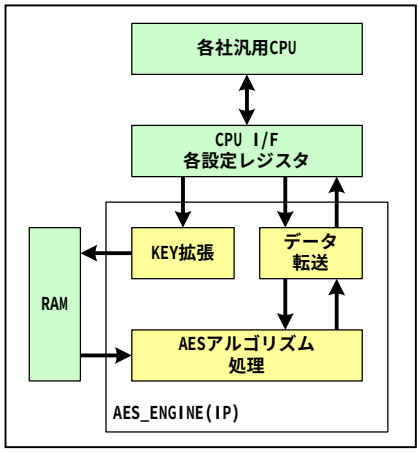
CPU 接続用 I/F をお客様のご要望に合わせてカスタム設計してご提供することにより、
外部制御を容易にすることが出来ます。

【インタフェース】

I/F	信号名	I/O	機能
System I/F	AESCLK	I	AES master clock
	RESETN	I	Negative reset
DATA I/F	ENCMODE	I	ENC/DEC change signal
	KEYSEL[1:0]	I	Key length select signal (0:128, 1:192, 2;256)
	GOSET	I	GO SET(request)
	ACT	O	AES ENGINE active
	INDATA[127:0]	I	Input data
	MODE[1:0]	I	ECB/CBC/CTR mode signal (0:ECB,1:CBC,2:CTR)
	IVREGW[127:0]	I	initial vector register write
	INIFLGS	I	initial vector flags
	OUTDATA[127:0]	O	Output data
	IVREGR[127:0]	O	vector register read
KEY I/F	KEYSET	I	Key set
	KEY[255:0]	I	Key input data
	EXP_ACT	O	Key expansion active
RAM I/F	KEYWT	O	Key data write for external memory
	KEYWA[5:0]	O	Key data write address for external memory
	KEYWD[31:0]	O	Key write data for external memory
	RAD[5:0]	O	Sub key read address for external memory
	SUBKEY[31:0]	I	Sub key(data out of external memory)

【制御手順（例）】

① キー長の設定および、キーデータ(128bit/192bit/256bit)を書込む
② キー拡張処理開始を指示
③ 割り込み等でキー拡張処理終了を確認する。
④ 動作モード(暗号化/復号)を設定する。
⑤ 動作モードに応じて、イニシャルベクタデータを設定する。
⑥ 入力データ(16byte)を入力データレジスタに書き込む。
⑦ 暗号化/復号動作開始を指示する。
⑧ 割り込み等で AES 暗号化/復号動作終了を確認する。
⑨ 出力データ(16byte)を読み出す。
※16byte を越えるデータを暗号化/復号するときは、上記の⑥～⑨を繰り返し、16byte 毎に暗号化/復号を実行する。新たにキーを設定し、暗号化/復号をするときは、上記①～⑤を再度実行した後、⑥～⑨を実行する。



【規模と速度(参考)】

デバイス　　：ALTERA 製 CycloneIII
使用 LE 数　　：約 3,000LEs（AES_ENG 部:約 1700LEs / INOUTIV 部:約 700LEs / KEY_EXP 部:約 600LEs）
必要 Memory 空間　：2kbit
最大動作速度　　：40MHz

※ALTERA 製 CycloneIIIにおける AES_ENGINE IP 単体の参考規模と動作速度になります。
※使用ツール:QuartusII version9.0 Build 132 02/25/2009 SJ Full Version

ソフトウェアにてキー拡張処理を行うことで規模縮小が可能です。
（※その場合、IP の規模は約 2,400LEs になります。）

【記述言語】　Verilog-HDL または VHDL

通信機器･画像処理関連ハードウェア、ファームウェアの
受託開発も承ります。
株式会社テクノクリエート
〔本社〕〒980-0801 仙台市青葉区木町通1－8－28 武山興産ビル
〔東京技術センター〕〒206-0014 東京都多摩市乞田1284永山Uビル

■お問い合わせはこちら
0120－733－606（お問い合わせセンター）
E-mail：info@techno-create.com
http://www.techno-create.com