3ZB-8

AES 用演算器を搭載したプロセッサによる Advanced Encryption Standard の高速化

穴井　秀知†　浜辺　直輝†　小島　正典†　柴田　浩†
†大坂工業大学　情報科学部

1. はじめに

インターネットを利用したモバイルな動画端末の実用化が進むに伴い[1],伝送のセキュリティ確保が望まれている.これに対して,高速な暗号化を低電力なプロセッサで実現する必要がある.

動作周波数 30MHz 程度の 32bitRISC プロセッサで 128 ビットの AES(Advanced Encryption standard)を行った場合,約 0.5Mbit/s ほどの速度が得られている.

本稿では,AES の中で複雑な処理を専用演算器としてハードウェア化すると,プロセッサのみに比べ,処理時間を約 20%に短縮し,約 5 倍の高速化が可能と考えた．そこで,VHDL 記述によって,AES 用演算器を搭載した RISC プロセッサを設計し,これを検証をした.

2. AES のアルゴリズム

AES 暗号方式は,ブロック暗号であり,ブロック長を 128,192,256 ビットの各ブロック長を持つことができる.またこのブロック長とは独立に,鍵長を 128,192,256 ビットとすることができる.

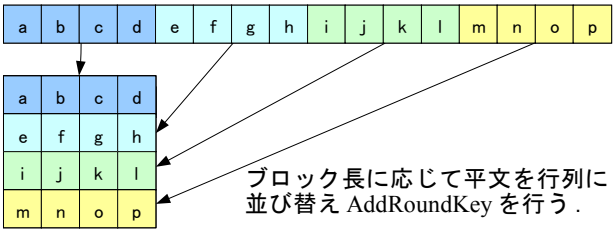

図 1. 初期化

AES では,図 1 に対して,1 ラウンドの処理として SubBytes,ShiftRows,MixColumns,AddRoundKey を行う.

これを選択された鍵長とブロック長によって決まるラウンド数分繰り返すことにより,暗号化を行っている.以下にその 4 つの処理について述べる[2].

2.1. SubBytes

SubBytes は非線形の転置であり,各バイト単位に対して,ビット転置を行う.

本来の処理は 1 バイト長のデータを 2 進数の多項式とし,

$$m(x)=x^8+x^4+x^3+x+1 \quad (\ 11B\ ,16\text{進数})$$

に対して逆元を計算し,アフィン変換を行う.

しかし,入力された 1 バイトのデータに対して出力を一意に決定できることから,先にテーブルを用意しておき,それに従って変換を行う方式が用いられることが多い.これは他の暗号方式での S-box に相当する.

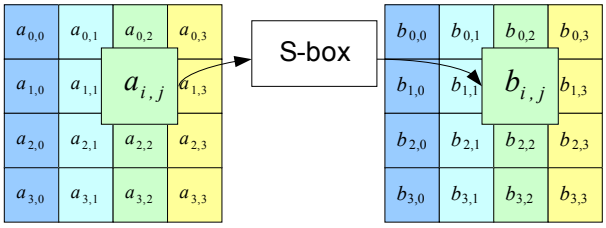

図 2. SubBytes

On the accelerating method for the Advanced Encryption Standard using processor with an assorted computing unit

†Faculty of Information Science, Osaka Institute of Technology

2.2. ShiftRows

行方向に対して,数バイト単位での回転処理を行う.

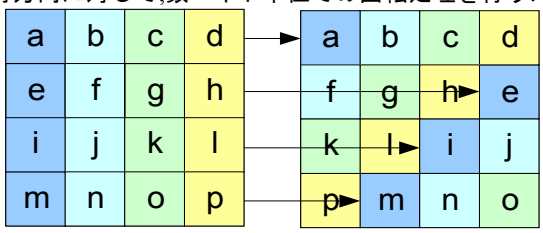

図 3. ShiftRows

2.3. MixColumns

各列に対して以下の式のような処理を行う.

$$C(x)='03'x^3+'01'x^2+'01'x^1+'02'$$

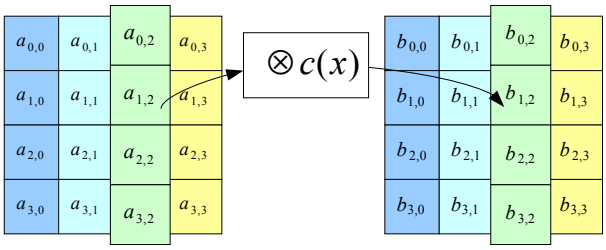

図 4. MixColumns

この式を行列式に変換すると

$$\begin{pmatrix} b_{0,j} \\ b_{1,j} \\ b_{2,j} \\ b_{3,j} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} a_{0,j} \\ a_{1,j} \\ a_{2,j} \\ a_{3,j} \end{pmatrix}$$

のように書くことができる.

2.4. AddRoundKey

鍵拡張により生成された鍵と暗号ブロックの排他的論理和を取る.

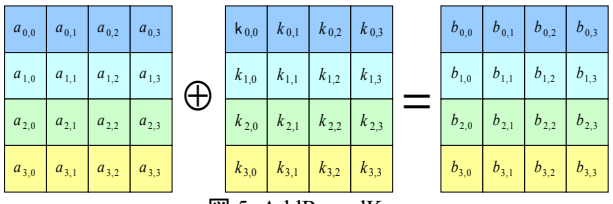

図 5. AddRoundKey

以上のような処理を繰り返すことにより暗号化が行われる.また最終ラウンドでは MixColumn 以外を行う.

3. 32 ビット RISC プロセッサ

本稿では VHDL を用いて以下のような RISC プロセッサを設計した.

- 命令長，データ幅は 32 ビット
- 32 ビットの汎用レジスタを 32 個
- パイプライン構成
- ハーバードアーキテクチャ

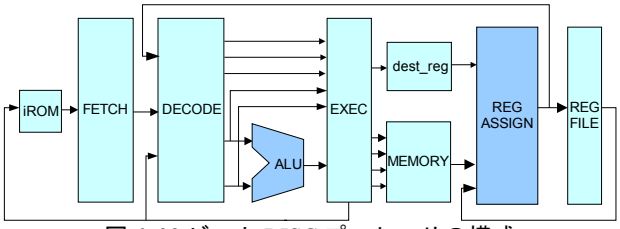

図 6. 32 ビット RISC プロセッサの構成

このプロセッサを VHDL により設計し,Altera 社の Quartus Ⅱ を用いて,FPGA(APEX20K400EBC652-1x)に実装した結果を以下の表に示す.

Total logic elements	***5,856***
ゲート数	***140,800***
動作周波数	***31.35MHz***

4. ソフトウェアのみの AES の実装

上記のプロセッサを用いて,アセンブラにより,ブロック長 128 ビット,鍵長 128 ビットの AES 暗号を実行し,検証した[3].以下にその実行結果を示す.

	回数	***Cycles***
SubBytes	***10***	***1500***
ShiftRows	***10***	***1430***
MixColums	***9***	***3620***
AddRoundkey	***11***	***650***
Total		***7000***

AES の速度は以下の式で求められる[4].

$$MHz * 1000 * 1000 / 1024 / 1024 * 128 / Cycles$$

よって,ソフトウェアのみの実装では,動作周波数 30MHz の場合, $0.52\,Mbit/s$ となった.

5. AES 用演算器の設計

上記の結果より,必要サイクル数の多い MixColumns と SubBytes を演算器として設計することにより,高速化を図る事にした.

5.1. SubBytes,InvSubBytes の設計

SubBytes 処理はソフトウェアのみの場合,メモリ上に S-box 用意して,転置処理を行っていたが,これでは 1 回に 1 要素（8 ビット）ずつしか変換することができない.

$GF(2^8)$ の逆元演算テーブルを用いることにした.

以下にその構成を示す.

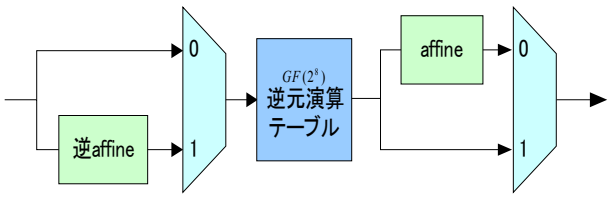

図 7. SubBytes の構成

5.2. MixColumns,InvMixColumns の設計

MixColumns 処理もソフトウェアのみの場合,非常に多くのサイクル数が必要になってしまった.これは行列演算により,演算数が多くなってしまうためだと考えられる.

そこで 1 列ごとの計算を 1 サイクルで行えるようにハードウェアを構成した.また InvMixColumns の回路を共有することにより,MixColumns も行えるようにした.

その構成を図 8 に示す.

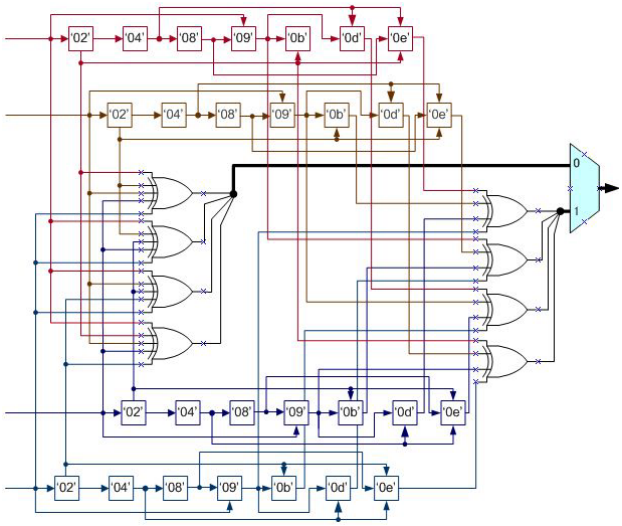

図 8. MixColumns の構成

6. AES 用演算器を搭載したプロセッサ

4 に示した演算器を ALU に併設する形でプロセッサに追加し,再び Quartus Ⅱ を用いて FPGA(APEX20K400 EBC652-1x)に実装を行った.以下にその結果を示す.

Total logic elements	***6,225***
ゲート数	***149,600***
動作周波数	***32.11MHz***

AES 用演算器を用いて,アセンブラの最適化を行い,AES 暗号を実行した結果を以下に示す.

Key/Block length	***Cycles***	***Speed(Mbit/s)***
(128,128)	***1460***	***2.51***
(192,128)	***1840***	***1.99***
(256,128)	***2140***	***1.71***

7. まとめ

AES 用演算器を搭載したプロセッサでは 2.51Mbit/s の結果が得られ,ソフトウェアのみに比べて,約 5 倍高速化することができた.

また,増加したゲート数は約 10,000 となった.

これにより,例えば動作周波数 100MHz のプロセッサで,ストリーミングなどリアルタイムな処理を要求されるデータ転送において,AES 暗号処理にかかる CPU 負荷を 5 分の 1 に減らすことができ,このプロセッサの動画端末に組込むことで端末間の暗号処理が可能になる目処を得た.

参 考 文 献

[1] 羽鳥 好則, 片山 頼明 :
ディジタル映像ネットワーク, コロナ社

[2] Joan Daemen, Vincent Rijmen : AES Proposal: Rijndael
http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf

[3] Federal Information Processing Standards Publication 197:
ADVANCED ENCRYPTION STANDARD(AES)
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[4] AES /Rijndael: speed
http://www.tcs.hut.fi/~helger/aes/rijndael.html