Technical Reports on Information and
Computer Science from Kochi
Vol. 2 (2010), No. 2

暗号化アルゴリズムＡＥＳのハードウェア化による性能評価

Performance Evaluation of Encryption Algorithm AES Hardware

坂本 丈昌　　松永 惇弥　　村岡 道明

Takeaki Sakamoto　Junya Matsunaga　Michiaki Muraoka

高知大学　理学部　情報科学コース　村岡研究室

1. まえがき・背景

高度情報化に伴い、暗号化処理技術は重要性が高まっている。また、データ量の増加とともに、それに伴う暗号化処理の時間が増えている。従来の研究では、ソフトウェア上でスピードを改善する方法が行われてきた。しかしながら、ソフトウェア改善だけでは高速化が不十分であるため、ハードウェア化することが期待されている。

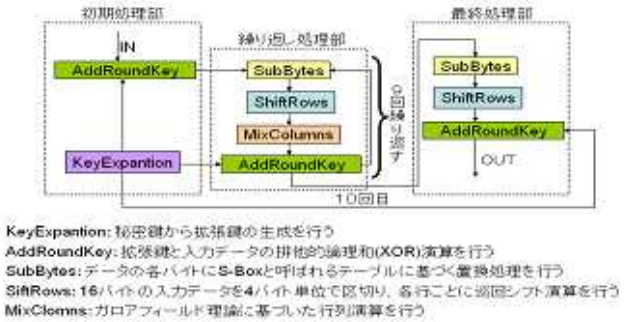
2. 目的

本研究では、暗号化アルゴリズムの一部をハードウェア化することにより暗号化処理の高速化を検討した。今回のハードウェア化では、暗号化アルゴリズム AES を用いて行い、ソフトウェアのアルゴリズムをもとにボトルネック部分のハードウェア化を行った。

3. 研究内容

3.1 暗号化アルゴリズム AES

以下、図 1 により暗号化アルゴリズム AES のフローを示す。



KeyExpantion: 秘密鍵から拡張鍵の生成を行う
AddRoundKey: 拡張鍵と入力データの排他的論理和(XOR)演算を行う
SubBytes: データの各バイトにS-Boxと呼ばれるテーブルに基づく置換処理を行う
ShiftRows: 16バイトの入力データを4バイト単位で区切り、各行ごとに巡回シフト演算を行う
MixClomns: ガロアフィールド理論に基づいた行列演算を行う

図 1.　暗号化アルゴリズム AES のフロー

暗号化アルゴリズム AES では，128bit(16byte) の入力データ(IN）に対し，「SubBytes」「ShiftRows」「MixColumns」「AddRound-Key」の 4 種類の基本処理を繰り返し行うことで，暗号化された出力データ(OUT）が得られる。

3.2 ハードウェア化部分の検討

ハードウェア化するボトルネック部分の発見のために、従来より所有していた暗号化アルゴリズム AES のソフトウェアの時間計測を行い、ハードウェアにすべき部分の決定を行った。以下表 1 により 2.4MB を暗号化した場合の実行時間を示す。

表１.　2.4MB を暗号化した場合の実行時間の割合

実験条件
OS:Windows XP SP3
CPU: Pentium4 3.20GHz
RAM: 0.99GB

繰り返し処理部が大部分を占めているため、ハードウェア化することにより、AES 暗号全体の高速化を計る必があることがわかった。

4. Verilog HDL 記述

次にボトルネック部分の高速化のため、FPGA を前提としたハードウェア化を行った。アルゴリズムの元の C 言語記述と作成した HDL 記述の比較を表 2 に示す。

表 2.　記述比較表

	C言語 [行]	Verilog HDL [行]
SubBytes	16	45
S-box	52	278
ShiftRows	49	82
MixColumns	72	672
GF01・GF02・GF03	19	32
AddRoundKey	18	20
合計	329	1207

記述の合計行数として、アルゴリズムの C 記述では 329 行、HDL 記述では 1207 行と HDL 記述の方が多かった。SubBytes や S-Box、MixColumns などは並列処理をさせているために大幅に行数が増えている。また、HDL 記述はクロックなどによる時間の制御が加えられているため行数が増えている。

5. タイミングシミュレーションの結果と考察

タイミングシミュレーションは、Quartus II 7.1 Web Edition で論理合成を行い、ディレイファイルとネットリストを作成し、それを用いて、論理シミュレータ ModelSim-Altera 6.1g Web Edition 上で行った。以下の表 3 は、タイミングシミュレーション結果を示している。

表 3.　タイミングシミュレーションの結果

ソフトウェアでの実行時間　1．171(sec)

周波数(MHz)	10MHz	20MHz	40MHz	80MHz	100MHz
周期(nsec)	100	50	25	12.5	10
繰り返し処理15万回のサイクル数	10800000	10800000	10800000	10800000	10800000
繰り返し処理15万回の実行時間(sec)	1.08	0.54	0.27	0.135	0.108
ソフトウェアとの比較結果	約1.08倍	約2.1倍	約4.2倍	約8.4倍	約10.8倍

この結果より、Pentium でのソフトウェアに比較すると最大周波数 100MHz では 10.8 倍の処理時間が速いことが分った。また、携帯電話で使用される ARM プロセッサの場合では、最大周波数が 200MHz（ARM920T 200MIPS）であるので、Pentium に比較すると、速度がおおよそ 16 倍遅くなる。したがって、ハードウェア化すると ARM 上のソフトウェアより、約 160 倍処理時間が早くなることがわかった。

6. まとめ・今後の課題など

AES 暗号における繰り返し処理部分のハードウェア化を行った。今回のハードウェア化の手法では、最高 100MHz までは動作可能であることがわかった。ハードウェア化を行った処理部分は、ソフトウェア処理に比べ、実行速度が Pentium では約 10.8 倍になることがわかった。さらに、ARM プロセッサの場合では、約 160 倍早くなることがわかった。今回は、暗号アルゴリズムの一部ハードウェア化を行ったが、今後は、パイプライン化などにより、さらに高速化を検討したい。また、FPGA 実装によるハードウェアの評価についても検討したい。