Technical Reports on Information and
Computer Science from Kochi
Vol. 3 (2011), No. 4

暗号化アルゴリズムのハードウェア化の研究

Hardware Implementation Methodology of Encryption Algorithms

前木場　達也　　村岡道明
Tatsuya Maekoba　　Michiaki Muraoka
情報科学コース　村岡研究室

1. まえがき・背景

近年、インターネットやネットワークの普及により、文書や画像などのデジタルデータの第三者による改ざんや盗みが多発し、深刻な問題となっている。この問題への対策として暗号化技術の利用が有効であるが、情報量の増加により、それに伴う暗号化処理の時間も増加してきている傾向にある。

この問題の解決のために、本研究では、暗号化アルゴリズムのハードウェア化による高速化を検討する。暗号化アルゴリズムＡＥＳの高速化として、ソフトウェア上でスピードを改善するＣＡＭを付加した超並列ＳＩＭＤプロセッサ[1]などが行われている。しかし、ソフトウェア改善では高速化が不十分なため、ハードウェア化による高速化が望まれている。

2. 研究目的

従来本研究室では、暗号化アルゴリズムのＤＥＳのハードウェア化、ＦＰＧＡ実装、パイプライン化を試行した。[2][3]本研究では、暗号化アルゴリズムＡＥＳのフルハードウェア化を行い、Pentium 4、ARM946E-S でソフトウェア実装を行った結果とハードウェア実装をしたものとを比較することでより詳しい処理比較を行う。また、さらなる高速化を目的としたパイプライン化を導入することで、暗号化アルゴリズムＡＥＳの更なる高速化の可能性を検討する。

3. 研究内容

研究内容として、Ｃ言語の記述である暗号化アルゴリズムＡＥＳを Verilog 記述に書き換え、並列化を加えることで高速化を目指す。その後、パソコン上でシミュレーションしたのち、時間精度付きモデルで計測[4]した ARM946E-S での実行時間と、Pentium 4 で計測した実行時間との比較をし、より詳しい性能比較を行う。また、パイプライン化も検討し、評価をする。

3.1 暗号化アルゴリズム AES

暗号化アルゴリズムＡＥＳは、入力データに対し、「Sub Bytes」「Shift Rows」「Mix Columns」「Add Round 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を得る事が出来るようになっている。AES 暗号化の処理の手順を図１に、４種類の基本処理の説明を図１の下に示す。

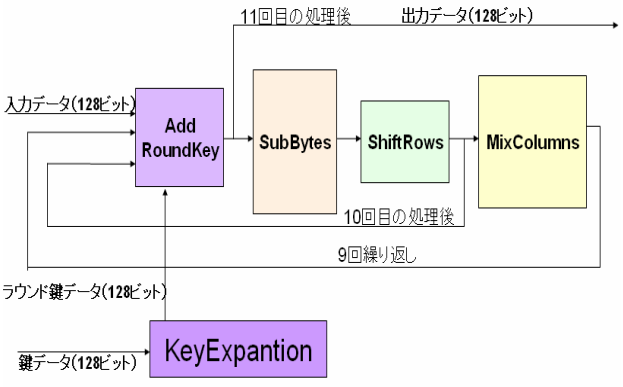

図１　AES 暗号化の処理の手順

3.2 ファンクションシミュレーション

暗号化アルゴリズム AES を verilogHDL に書き換え、ファンクションシミュレーションでの実験を行った。ModelSim-Altela 6.1 Web Edition 上でファンクションシミュレーションを実行し、サイクル数を計測したものを以下の表 5.1 に示す。

表5.1　ファンクションシミュレーションの結果

周波数(MHz)	10MHz	20MHz	25MHz	50MHz	80MHz	100MHz
周期(nsec)	100ns	50ns	40ns	20ns	12.5ns	10ns
1回の処理時間	12650ns	6325ns	5060ns	2530ns	1581.25ns	1265ns
1回のサイクル数	114サイクル	114サイクル	114サイクル	114サイクル	114サイクル	114サイクル

実行条件 : ModelSim-Altela 6.1 Web Edition

3.3 タイミングシミュレーション

ファンクションシミュレーションを行ったハードウェア記述で書かれたファイルを、QuartusII 7.1 Web Edition を使用して、10MHz から 100MHz までクロックを設定して論理合成を行った。

そして、合成してできたネットリストと SDF(Standard Delay File)を用いて ModelSim-Altela 6.1 Web Edition 上で、タイミングシミュレーションを行った。結果を表 5.2 に示す。

表5.2　タイミングシミュレーションの結果

周波数(MHz)	10MHz	20MHz	25MHz	50MHz	80MHz	100MHz
周期(nsec)	100ns	50ns	40ns	20ns	12.5ns	10ns
1回の処理時間	12658.238ns	6334.034ns	5068.666ns	2538.622ns	1589.603ns	1272.143ns
1回のサイクル数	114サイクル	114サイクル	114サイクル	114サイクル	114サイクル	114サイクル

実行条件：ModelSim-Altela 6.1 Web Edition

3.4 性能比較

今回作成した暗号化アルゴリズムのハードウェア記述のプログラムと Pentium 4、ARM946E-S でそれぞれ計測したソフトウェア実装の時間との比較をした。周波数が 3.2 GHz の Pentium4 で計測すると 2.4MB のデータを暗号化処理するのに約 1.419sec かかったのに対して、ハードウェア実装では約 0.190sec であったので、約 7.4 倍短縮された。また、周波数が 25MHz の ARM946E-S で計測すると 16B のデータを暗号化処理するのに約 0.59948msec かかったのに対して、ハードウェア実装では約 1272.143nsec であったので、約 471 倍短縮されたことになる。これより、ハードウェア化による高速化は有用であることがわかる。

4. まとめ

本研究では、暗号化アルゴリズム AES のハードウェア化による高速化を提案した。作成したハードウェアは FPGA 実装をすることにより 100MHz で動作可能であることがわかった。また比較結果として、Pentium(R) 4 の 3.2GHz の場合、暗号化アルゴリズム AES をハードウェア化することにより約 7.4 倍、ARM946E-S の 25MHz の場合は約 471 倍まで暗号化処理時間が高速化されるということがわかった。

5. 参考文献

[1] 田上正治，石崎雅勝，熊木武志，幸野豊，小出哲士，“CAM を付加した超並列 SIMD プロセッサ”，平成 19 年度電気・情報関連学会中国支部連合大会，2007 年 10 月
[2] 松永淳弥，“暗号化アルゴリズムのハードウェア化手法の性能評価”，平成 19 年度高知大学卒業論文，2008 年 3 月
[3] 山口良典，“暗号化アルゴリズム DES の FPGA 化による性能評価”，平成 20 年度高知大学卒業論文，2009 年 3 月
[4] 松永惇弥，“ソフトウェアの実行時間を考慮したハードウェア/ソフトウェア分割手法”，平成２１年度高知大学修士論文，2010 年 3 月