Technical Reports on Information and
Computer Science from Kochi
Vol. 7 (2015), No. 11

暗号化アルゴリズム AES のハードウェア化の研究

Hardware Implementation Methodology of Encryption Algorithms AES

浪越 隆生　　村岡 道明
Takao Nao　　Michiaki Muraoka
高知大学 理学部 応用理学科 情報科学コース

1. まえがき

スマートフォンやタブレット PC などの携帯端末を用いた大容量のデータをやり取りする機会が増えている．データ転送のセキュリティ向上のためには暗号化技術が必要であるが大容量のデータを暗号化するのには時間がかかる． 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暗号化処理を目指しプロトタイプの開発を行った．

2. 暗号化システム（ユニット）の構成

AES ハードウェアアルゴリズムを実装した暗号化ユニットは図 1 に示す 5 つのブロックで構成される．全体の構成は PC（ホスト）と RS232C 通信インターフェース部と FPGA 部で構成されており，FPGA 内はホスト側とデータ通信を行なう通信モジュール部と受け取ったデータを一時保存する BRAM 部と暗号化処理を行なう AES 暗号化ユニット部の 3 つで構成される．

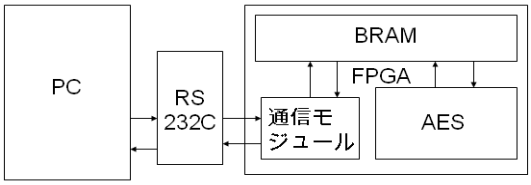

図 1．暗号化システムユニットの構成図

3. 暗号化アルゴリズム AES

AES のアルゴリズムは共通鍵暗号化方式であり 128 ビットのデータブロックを 4 つの変換方式（AddRoundKey, SubBytes, ShiftRows, MixColumns）と拡張鍵生成方式（KeyExpansion）を用いて暗号化を行なう．図 2 には，提案する AES ハードウェアのブロック図を示す．

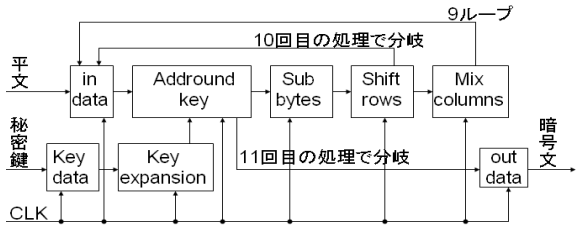

図 2．ハードウェアのブロック図

アルゴリズムをハードウェア化することで各変換方式を並列処理し高速化を図っている．

4. 評価

AES のソフトウェアアルゴリズムとハードウェアアルゴリズムの性能比較を行った．ソフトウェアアルゴリズムの評価比較には 10MB のデータをモバイル機器などに使用されている ARM946E-S_200MHz(以降 ARM9)上での実行時間と PC などに使用されている Core™i7 860_2.8GHz(以降 Core™i7)上での実行時間，ハードウェアアルゴリズムは暗号化ユニット (40MHz)上での実行時間の計測を行なった．比較結果を表 1 に示す．

表 1．ソフトウェアとハードウェアの性能評価

	ソフトウェア		ハードウェア
	Core™i7	ARM9	暗号化ユニット
動作周波数	2.8GHz	200MHz	40MHz
平文:10MB	3.52sec	33.78sec	1.99 sec

Core™i7 上と ARM9 上でのソフトウェア実行時間はそれぞれ 3.52sec，33.78sec となり暗号化ユニットでは 1.99sec となった．

5. 考察

本ハードウェアの通信インターフェースである RS232c(115.2Kbps)の転送速度は暗号化処理より遅く，10MB のデータ転送には 728sec かかる．ハードウェアの性能を引き出すには USB2.0(480Mbps)以上の通信速度を持つ通信インターフェースの実装が望まれ，その場合，10MB のデータ転送時間は 0.166sec となる．

6. 結論

携帯機器用の ARM9 上でのソフトウェア実行と提案するハードウェアでの実行時間を比較すると，約 17 倍ハードウェアのほうが高速であることがわかった．また，ハードウェアの性能を引き出すためには USB2.0(480Mbps)以上の通信速度を持つ通信インターフェースの実装が望まれる．

7. あとがき

本研究の暗号化ユニットの FPGA での性能評価とハードアルゴリズムのパイプライン化による高速化が課題である，さらに復号化機能の実装も期待される．

参考文献

[1] 前木場達也，村岡道明，“暗号化アルゴリズムのハードウェア化の研究”，高知の情報科学第 3 巻 No.4， 2011 年 3 月