C-015

ハードウェア特殊化 AES 暗号回路のＦＰＧＡへの実装と消費電力の測定
An FPGA implementation of hardware specialized AES encryption circuits and power consumption measurements

松岡 俊佑† 市川 周一‡
Shunsuke Matsuoka Shuichi Ichikawa

1. はじめに

現在最も広く利用されている暗号アルゴリズムに AES 暗号がある．AES の暗号処理は，CPU で処理するには負荷が大きく，高速処理させるのに暗号回路を実装して用いられることが多い．組み込み機器に暗号回路を実装するさいの制約として，回路規模や動作速度の他に，重要な項目として消費電力がある．

論理回路の入力の一部を定数として固定し，回路を最適化設計することで，論理ゲートが削減できる．これをハードウェア特殊化技術という．AES 暗号回路においても，入力暗号鍵を定数に固定することで回路を最適化することができる[1],[2]．ただし，異なる入力暗号鍵によって別な回路を新たに生成しなければならないため，FPGA のような再構成可能デバイスに適した実装方式となる．

本研究では，AES 暗号回路にたいして入力暗号鍵を固定したハードウェア特殊化回路を 2 種類設計した．さらに，設計した回路を SASEBOGⅡボードに実装し，回路動作時の消費電力を測定したので報告する．

2. AES 暗号回路

AES では入力平文は 128 ビット，暗号鍵長は 128，192，256 ビットのうちから選択することができ，鍵長によって繰り返しラウンド数が 11，13，15 に決まる．本研究では，鍵長は 128bit とする．1 ラウンド分の処理は，基本的には SubBytes，shiftRows，MixColumns，AddroundKey の 4 種類の演算からなる．これらの演算をラウンドの数だけ順に繰り返すことにより，暗号文が生成させる．ただし，最初のラウンドでは AddroundKey のみが実行され，最終ラウンドでは MixColumns は行わない．また，AddroundKey では，ラウンド鍵との排他的論理和処理が行われるが，各ラウンド鍵は入力暗号鍵をもとに鍵拡張処理により生成される．

本研究では，東北大学の青木研究室の Web ページにて公開されている AES 暗号回路[3]を評価の基本として用いる．ループ型アーキテクチャが採用されており，1 ラウンド分の 4 種類の演算行うための回路と中間値を保存するためのレジスタ，および各ラウンド鍵を生成するための鍵拡張部からなる．

3. AES 暗号回路のハードウェア特殊化回路

3.1 ラウンド鍵固定回路(fixed_round_key)

青木研のループ型 AES 暗号回路(original)をもとに，入力暗号鍵を定数に固定した 2 つのタイプのハードウェア特殊化回路を設計した．まず一つ目の回路として，入力暗号鍵の値が決まると，0～10 ラウンドのラウンド鍵の値も一意的に決まることから，全 11 個のラウンド鍵を定数に固定したラウンド鍵固定回路(fixed_round_key)を設計した．original 回路の鍵拡張部に置き換え，マルチプレクサで各ラウンド鍵を選択する方式とした．

3.2 xor-or_by_ROM 回路

AddroundKey 処理は，ラウンド鍵との排他的論理和処理(Ex-OR)をとる．ラウンド鍵を定数に固定すると，Ex-OR の一方の入力が定数に固定されたことになる．Ex-OR の残りのもう一方の入力と出力との関係は，ラウンド鍵の定数値を用いてあらかじめ計算しておくことができ，これをテーブル化することで Ex-OR を ROM に置き換えることができる．全 128 ビットの Ex-OR を 8 ビットごとに 1 個の ROM に置き換えた xor-by_ROM 回路を設計した．ROM のデータ幅は 8bit，入力アドレスは，1～10 ラウンド選択用に 4bit 追加し 12bit とした．

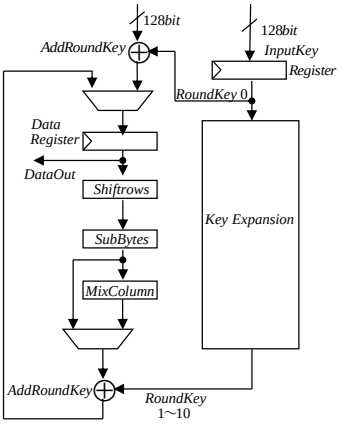

図 1 AES 暗号化回路

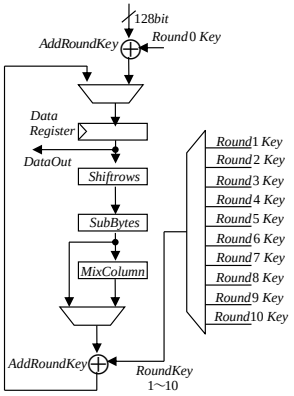

図 2 ラウンド鍵固定回路

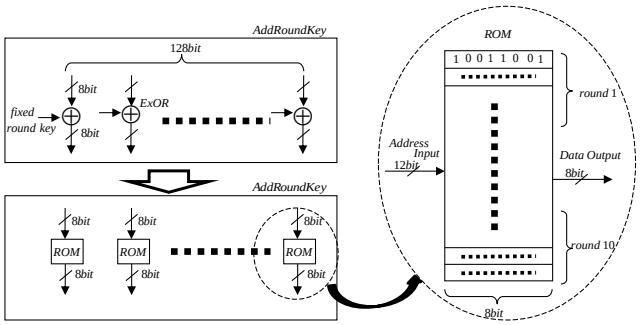

図 3 ExOR-ROM 化回路

†旭川工業高等専門学校
Asahikawa National College of Technology
‡豊橋技術科学大学
Toyohashi University of Technology

4. FPGA への実装

4.1 評価環境

評価基板には，産業技術総合研究所および東北大学によって開発されたサイドチャネル用標準評価基板 SASEBOG Ⅱを用いた．電力解析攻撃の研究・評価用に作成されたボードで，暗号回路 IP や制御回路，通信回路，および電力波形測定アプリケーションが公開されている[4]，ボードには Xilinx 社製 FPGA である Virtex-5 XC5VLX30 と Spartan3A XC3S50AN が搭載されており，Virtex-5 には暗号回路を，Spartan3 には制御・通信回路を実装する．電力測定用のオシロスコープには Agilent 社の DSO1024A を用いた．PC とオシロスコープは USB ケーブルで接続されており，波形取得アプリケーションによりオシロスコープをリモートコントロールし，消費電力データを PC へ取り込むことができる．PC と SASEBOG Ⅱボードは USB ケーブルで接続されており，PC から平文や入力暗号鍵を送信し，暗号回路で生成された暗号文を取り込むことができる．

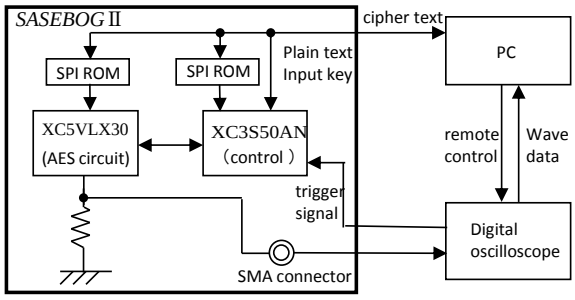

図 4 実験環境のブロック図

4.2 実装結果

ループ型 AES 暗号回路(original)と 2 種類のハードウェア特殊化回路(fixed_round_key, xor_by_ROM)を，Xilinx 社の FPGA 用ツール ISE13.2 を用いて論理合成および配置配線した．ターゲットデバイスは Virtex-5 XC5VLX30 とし，論理合成オプションはデフォルトとした．実装結果を表 1 に示す．FPGA の論理規模(occupied slice)は，original 回路に対し fixed_round_key は 80%, xor_by_ROM は 64%となり，いずれの回路も論理規模が削減された．特に xor_by_ROM は 36%減と削減率は大きい．最大周波数は，xor_by_ROM が 1.2 倍に改善された．これらの実装結果より，提案したハードウェア特殊化回路の論理規模に対しての削減効果が確認できた．とりわけ，xor_by_ROM は論理規模および最大周波数の改善効果が大きい．

表 1 FPGA への実装結果

	original	fixed_round_key	xor_by_ROM
occupied Slices	522	421	333
BlockRAM	6	6	6
Max.Frequency(MHz)	220.16	215.61	259.87

4.3 消費電力の測定

AES 暗号回路(original)と 2 種類のハードウェア特殊化回路(fixed_round_key, xor_by_ROM) を SASEBOG Ⅱボードに搭載されている FPGA(XC5VLX30)に実装した．各回路について消費電力を 1000 回測定し，平均した波形を図 4(a)に示す．動作クロック周波数は 1MHz，オシロスコープのデータポイント数は 600 とした．ループ型 AES 暗号回路において，ラウンド毎にレジスタが更新されるたびに消費電力がピーク値となる様子が確認できる．4 ラウンド付近の波形を拡大すると図 4(b)となる．それぞれの回路において，消費電力にわずかな違いが見られる．このうち xor_by_ROM の消費電力波形は全期間に亘って最小となった．また，0～600ns 間の電力波形の平均値は，original では 108.14mW，fixed_round_key は 110.79mW，xor_by_ROM は 104.07mW となり，xor_by_ROM の電力消費は original に対して 3.7%低下した．

5. まとめ

AES 暗号回路に対して入力暗号鍵を定数に固定したハードウェア特殊化回路を 2 種類（fixed_round_key, xor_by_ROM)設計し，FPGA への実装および消費電力を測定した．その結果，xor_by_ROM は回路規模および最大周波数ともに改善され，消費電力についてもわずかに削減されることが確認できた．

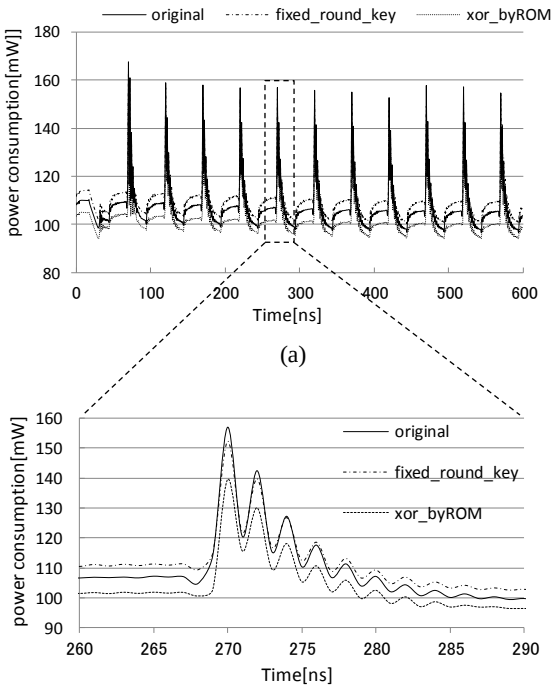

図 5 AES 暗号回路の消費電力波形

参考文献

[1] R.Atono, S.Ichikawa, “Design and Evaluation of Data-dependent Hardware for AES Encryption Algorithm” IEICE Trans. Info. Sys., vol. E89-D, no.7, pp. 2301-2305, 2006.
[2] 松岡俊佑, 日野善規,市川周一,”AES 暗号と Camellia 暗号に対する暗号鍵を固定したハードウェア特殊化回路”, 電子情報通信学会論文誌 D,Vol.J94-D, No.10, pp.1696-1700, (2011).
[3] 東北大学青木研究室，”Camellia IP Core”，http://www.aoki.ecei.tohoku.ac.jp/crypto/web/cores.htm
[4] 産業総合技術研究所情報セキュリティ研究センター，http://www.rcis.aist.go.jp/special/SASEBO/SASEBO-GII-ja.htm
[5] T.Sugawara, N.Homma, T.Aoki, A.Satoh, “Differential power analysis of AES ASIC implementations with various S-box circuits”, ECCTD, August, 2009.