C-020

鍵スケジューラを省略した AES 暗号回路の FPGA による実装評価
An FPGA implementation and performance evaluation of AES circuits without key scheduler

松岡 俊佑† 藤枝 直輝† 市川 周一†
Shunsuke Matsuoka Naoki Fujieda Shuichi Ichikawa

1. はじめに

AES (Advanced Encryption Standard)は，共通鍵暗号として現在最も広く用いられている[1]．AES の回路実装においては，スループットに優れた回路や，小規模な回路，低消費電力回路など，さまざまな回路アーキテクチャが報告されている[2],[3]．特に組込み機器用の AES 暗号回路においては，回路規模や速度性能はもとより消費電力に対して厳しい制約がある．

一般に論理回路の入力の一部が定数値ならば，回路を最適化して論理ゲートを削減することができる．AES 暗号回路においても，入力暗号鍵を定数値にすることで，論理規模が削減され性能が向上する[4],[5]．ただし暗号鍵毎に別な回路を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．

本稿では，鍵固定 AES 暗号回路の新たな回路方式[6]の消費電力について，詳細な評価を行ったので報告する．

2. AES 暗号回路

AES では， SubBytes， ShiftRows， MixColumns， AddRoundKey の 4 種類の演算を順に繰り返していく．AddRoundKey は，ビットごとの XOR 処理，SubBytes は S-BOX と呼ばれる 8 ビットごとの非線形処理からなる．これらの 1 回分の繰り返し処理のことをラウンドという．入力暗号鍵長が 128 ビットのときは，ラウンドは 11 回繰り返される．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 が省略される．また，鍵スケジューラでは，入力暗号鍵をもとに第 1～10 ラウンド鍵が生成され，AddRoundKey の XOR 演算へ入力される．

東北大学の青木研究室の Web ページ[7]にて公開されているループ型 AES 暗号回路 (図 1) を評価の基本として用いる．1 ラウンド分の 4 種類の演算を行うための回路と中間値を保存するためのレジスタ，およびラウンド鍵を生成するための鍵スケジューラからなる．評価回路には，SubBytes の回路構成がことなる，AES_TBL，AES_Comp，AES_PPRM1，AES_PPRM3 がある．

3. 暗号鍵を固定した AES 暗号回路

先行研究の鍵を固定した AES 暗号回路 (XOR_by_ROM)[5]を図 2 に示す．入力暗号鍵を定数値として固定すれば，10 個のラウンド鍵も定数値となり，鍵スケジューラ回路は省くことができる．さらに，AddRoundkey へのラウンド鍵入力を定数値として XOR 演算をテーブル化し，ROM として実装する．ROM のデータ幅は 8 ビット，入力アドレスはラウンド選択用に 4 ビット追加し 12 ビットとする．AES のブロック長は 128 ビットのため，全容量は 16×2816 バイトと FPGA のブロック RAM (BRAM)へ実装するのに適した容量となる．

†豊橋技術科学大学
Toyohashi University of Technology

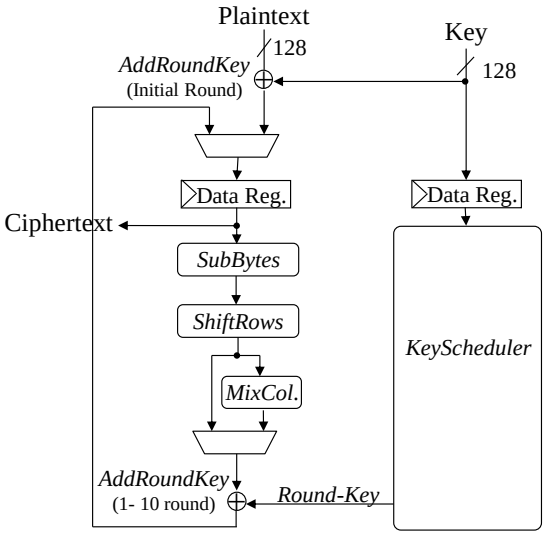

図 1. **AES 暗号化回路[7]**

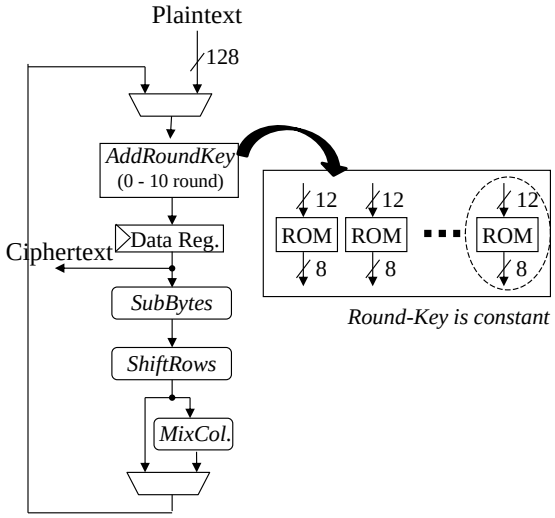

図 2. XOR_by_ROM **回路**[5]

4. 提案回路（XOR&S-BOX_by_ROM）

青木研の評価回路のひとつである AES_TBL では S-BOX をテーブル実装している．S-BOX はビット幅 8 ビットの ROM×16 個で構成される．一方，XOR_by_ROM 回路の XOR テーブルもデータ幅 8 ビットの ROM×16 個からなるので，S-BOX と XOR テーブルは 8 ビットごとに 1 つの ROM として統合することができる．我々は，Addroundkey と SubBytes を一つのテーブルとして統合した回路 XOR&S-BOX_by_ROM を新たに提案している[6]．提案回路を図 3 に示す．

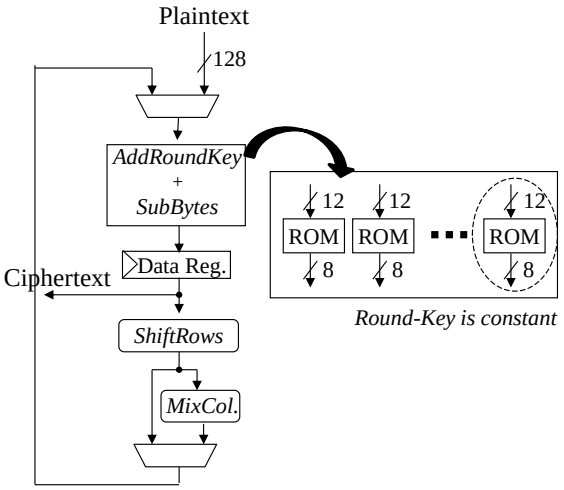

図 3. XOR&S-BOX_by_ROM 回路

5. 消費電力測定

SASEBO-GⅡボード[8]とオシロスコープを用いて消費電力測定環境を構築した．ボードには，Xilinx 社 FPGA の Virtex5 XC5VLX30 が搭載されている．Xilinx 社の FPGA ツール ISE14.7 を用いて，青木研の評価回路と XOR_by_ROM 回路，および提案した XOR&S-BOX_by_ROM を論理合成し，Virtex5 XC5VLX30 へ実装する．温度による影響を考慮して，一つの回路について平文を変えながら消費電力を 1000 回測定したあと，次の回路を実装し測定を繰り返していく．全種類の回路の測定を 10 回行う．消費電力の平均値と論理規模 (slice 数)の関係を図 4 に示す．ピアソン係数は 0.988 と強い相関を示した．論理規模が小さな回路ほど消費電力は少ない．提案した XOR&S-BOX_by_ROM は論理規模と平均消費電力ともに最小となった．

AES_TBL と XOR_by_ROM，XOR&S-BOX_by_ROM は FPGA 内のブロック RAM (BRAM)を使った実装と，分散 RAM (distribute RAM)として論理ブロック上に ROM を実装した回路についても消費電力を測定した (図 5)．BRAM を使って実装すると，slice 数の減少に伴い，消費電力も低下する傾向にあるが，BRAM の使用による消費電力への直接的な影響は，今回の測定結果からは見出せなかった．

AES_TBL と XOR_by_ROM，XOR&S-BOX_by_ROM の 1 ブロックの暗号化における平文 1000 回の平均消費電力を図 6 上部に，その 4, 5 ラウンド部分を切り出し拡大したものを図 6 下部に示す．クロックに同期してレジスタの中間データが更新されるたびに動的電力を消費し，スパイク波形が生じている．XOR&S-BOX_by_ROM は全周期にわたって静的電力は最小となった．

6. おわりに

本研究では，鍵を固定した AES 暗号回路として，AddRoundKey と SubBytes を一つの RAM に統合した XOR&S-BOX_by_ROM の消費電力について詳細な評価を行った．提案回路を SASEBOGⅡボードへ実装したところ，特に静的消費電力の削減率が大きいことが確認できた．FPGA へ AES 暗号回路を実装した場合の消費電力は，静的電力の影響が大きく，また slice 数の減少に相関して静的消費電力も低下する．今後の課題として，他の FPGA へ実装した場合の消費電力についても調査していく．

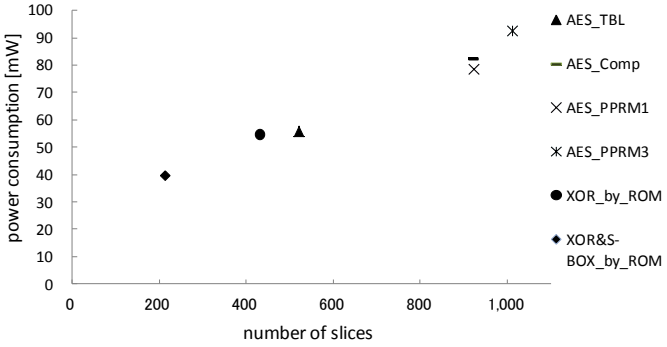

図 4. 論理規模 (slice 数)と消費電力の関係

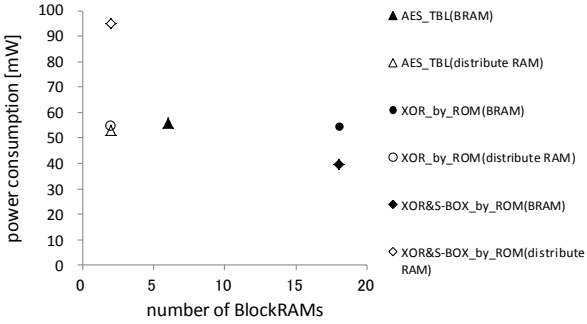

図 5. BlockRAM と消費電力の関係

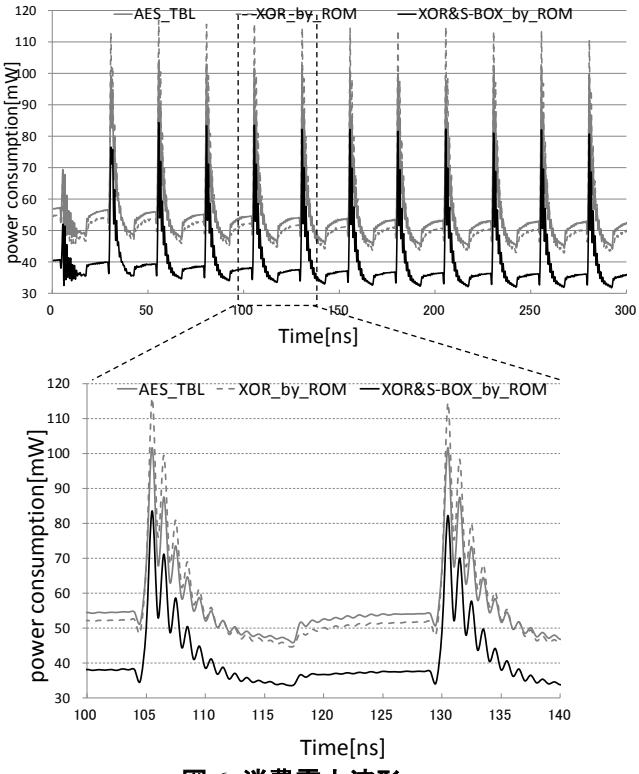

図 6. 消費電力波形

参考文献

[1] National Institute of Standards and Technology (NIST), “ADVANCED ENCRYPTION STANDARD (AES)”, FIPS Publication 197, 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[2] A.Satoh, S.Morioka, K.Takano and S.Munetoh, “A Compact Rijndael Hardware Architecture with S-Box Optimization”, LNCS, vol.2248, pp. 239-254, 2001.

[3] S.Morioka,A.Satoh, “An Optimized S-Box Circuit Architecture for Low. Power AES Design”, CHES2002, LNCS2523, pp.171-186, 2003.

[4] 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.

[5] S.Matsuoka, S.Ichikawa: "Reduction of Power Consumption in Key-specific AES circuits" Proc.ICNC2012, pp.323-325, 2012.

[6] S.Matsuoka, N.Fujieda, S.Ichikawa, "S-Box Absorption Design for Key-specific AES circuits," IEEE TENCON-2014, (Submitted), 2014.

[7] Aoki Laboratory, “Cryptographic Hardware Project, Graduate School of Information Sciences, Tohoku University”, http://www.aoki.ecei.tohoku.ac.jp/crypto/web/cores.html

[8] SASEBO Project, “Side-channel Attack Standard Evaluation Board (SASEBO) -- SASEBO-GII”, http://satoh.cs.uec.ac.jp/SASEBO/en/board/sasebo-g2.html.