C-014

ハードウェア特殊化 AES 暗号回路のホワイトボックス実装に関する研究
An FPGA White-Box cryptography of the hardware specialized key-specific AES circuit

松岡 俊佑† 市川 周一‡
Shunsuke Matsuoka Shuichi Ichikawa

1. はじめに

ネットワーク上であらゆる情報が行き交いしている近年の情報化社会では，常に盗聴や改ざんといったセキュリティ上の脅威にさらされている．暗号技術は，こうした脅威から情報を保護するために欠かせない基盤技術として，あらゆる情報機器で利用されている．大量のデータを高速に暗号処理するには，LSI 上に暗号回路が実装される．モバイル情報端末器や，IC カード，RFID といった小型の組み込み機器に暗号回路を実装するさいには，高速処理はもちろんのこと，コストや消費電力などの制約がある．さらに，暗号回路の実装上の特性を解析して，回路内部の機密情報を暴き出す実装攻撃が盛んに行われており，これらの脅威への耐タンパ性も重要な性能指標の一つとなっている．

論理回路の入力の一部を定数として固定すれば，論理回路を簡単化することができ，回路規模の削減，回路動作の高速化，低消費電力化が期待できる．こうした技術のことをハードウェア特殊化という．筆者らはこれまでに，AES 暗号回路へのハードウェア特殊化の適用を試みており，回路の小規模化，動作速度の向上，消費電力が若干削減できることを示した[1],[2]．本研究では，これまでに提案したハードウェア特殊化回路に改良を加え，耐タンパ性をもつ実装方式について検討する．ソフトウェアの難読化手法として用いられているホワイトボックス暗号[3]を用いてアーキテクチャ回路を設計し，FPGA への実装評価を行ったので報告する．

2. AES 暗号回路

AES 暗号は 128 ビットをブロック単位として暗号化・複合処理される．基本的な処理は SubBytes，shiftRows，MixColumns，AddroundKey の 4 種類の演算からなり，これらの演算を順番に繰り返すことにより暗号文の生成，および平文が複合される．この繰り返しのことをラウンドといい，暗号鍵長が 128 ビットの場合にはラウンド数は 11 回となる．各ラウンドの AddroundKey では，128 ビットのラウンド鍵を入力として排他的論理和演算される．128bit×10 個のラウンド鍵は拡張処理によって生成される． AES 暗号を LSI に実装するさいの暗号回路アーキテクチャ方式として，1 ラウンド分の回路を全ラウンド回だけ繰り返し動作させるループ型アーキテクチャがある．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ループ型 AES 暗号回路[4]を評価の基本(original)として用いた．

3. ハードウェア特殊化 AES 暗号化回路

AES 暗号の入力暗号鍵を定数に固定すれば，ハードウェア特殊化技術を適用して回路を最適化設計することができる．筆者らはこれまでに，以下に示す方式のハードウェア特殊化 AES 暗号回路を設計し，FPGA による実装評価を行ってきた．

3.1 ラウンド鍵固定回路(fixed_round_key)

入力暗号鍵が定数に固定されると，10 個のラウンド鍵も定数となる．全ラウンド鍵をあらかじめ生成しておくことで鍵生成回路が不要となる．鍵生成回路をラウンド鍵の定数値をマルチプレクサで選択する回路に置き換えた fixed_roun_key 回路を設計した．

3.2 xor_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 の残りのもう一方の入力と，Ex-OR の出力との関係はテーブル化することができる．全 128 ビットの Ex-OR を 8 ビットごとにテーブル化し，ROM に置き換えた xor_by_ROM 回路を設計した．

3.3 xor_by_BlockRAM 回路

xor_by_ROM 回路の AddroundKey テーブルに FPGA のメモリ領域(BlockRAM)を使用して回路を実装する．

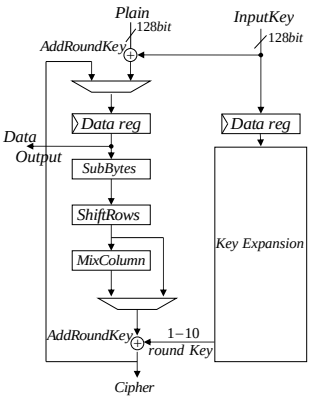

図 1 AES 暗号化回路

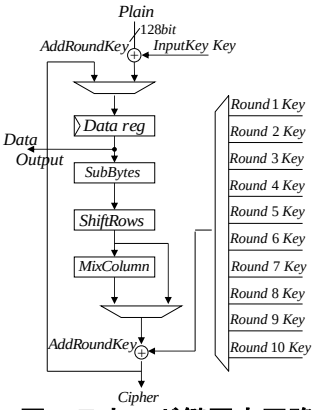

図 2 ラウンド鍵固定回路

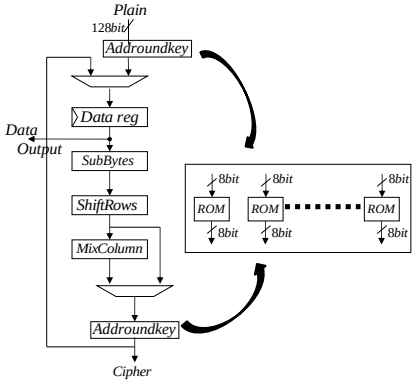

図 3 xor_by_ROM 回路

†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. AES 暗号回路へのホワイトボックス暗号の適用

4.1 ホワイトボックス暗号

FPGA へ書き込まれた論理回路データは，FPGA 内部の SRAM メモリセルに保持されており，回路構成パターンの盗聴に対して無防備となっている．提案したハードウェア特殊化 AES 暗号回路は，論理回路内部に鍵情報が含まれており，こうした実装攻撃に対しての対策を立てる必要があった．そこで暗号ソフトウェアにおいて，内部の鍵情報を隠蔽するための手法として用いられているホワイトボックス暗号を適用して新たにハードウェア特殊化 AES 暗号回路(WhiteBox_by_BlockRAM)を設計した．この手法では，各演算処理を数式処理ではなく，入出力情報をもとに作成したテーブル参照に置き換えて実現する[5]．図 4 に AES 暗号の AddroundKey と SubBytes をそれぞれテーブルに置き換えた例を示す．ここでは，AES の全 128bit のデータを 8bit に分けてテーブルを作成する．AddroundKey 処理は xor_by_ROM 回路と同様にラウンド鍵入力は固定値とし，Ex-OR をテーブル参照に置き換えて実行する．さらに，その出力に全単射変換を挿入してテーブルを作成することによりラウンド鍵情報は隠蔽化される．次段の処理の SubBytes は，入力に逆単射変換を挿入してテーブルを作成する．

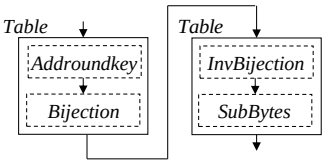

図 4 AddroundKey と SubBytes のテーブル置換

4.2 ホワイトボックス型 AES 暗号化回路

図 5 に，ハードウェア特殊化 AES 暗号回路にホワイトボックス暗号を適用した回路(WhiteBox_by_BlockRAM)を示す．original 回路では，第 0 ラウンドと第 1～10 ラウンドの Addroudkey は別な回路ブロックに分けていたが，これらを 1 つのテーブルにまとめ，FPGA の BolockRAM を使用して実装する．Addroudkey テーブルの最終第 10 ラウンド目のテーブル値は，Addroundkey＋逆 SubButes+全単射とし，データレジスタを挟んで次段のテーブル(逆全単射+SubBytes)で AddroundeKey 処理の出力値を複合させ，その値を暗号文出力とする．

5. FPGA による実装評価

設計したハードウェア特殊化回路，およびホワイトボックス型 AES 暗号回路(WhoteBox_by_BlockRAM)をサイドチャネル用標準評価基板 SASEBOG Ⅱ へ実装した．ボードには Xilinx 社製 FPGA である Virtex-5 XC5VLX30 が搭載されている．Xilinx 社の FPGA 開発ツール ISE13.2 を用いて論理合成，および配置配線した結果を表 1 に示す．論理規模(occupied slice)は，original 回路に対していずれの回路も削減された．特に WhiteBox_by_BlockRAM は，分離していた AddroundKey を一つのテーブルにまとめたこと，BlockRAM を使用したことにより，original 回路に対して 42%減と一番削減効果が大きかった．ただし，BlockRAM を使用したことにより，最大周波数(Max.freq)は，original 回路に対して 0.48 倍と大幅に低下した．これらの実装結果より，提案した WhiteBox_by_BlockRAM 回路は，速度性能は低下するものの，回路規模についてはハードウェア特殊化による削減効果が大きいことが確認できた．

6. まとめ

入力暗号鍵を固定したハードウェア特殊化 AES 暗号回路に改良を加え，ホワイトボックス暗号実装を適用して回路を設計した．この回路方式では，回路構成データ内の暗号鍵情報を秘匿化することができ，さらに FPGA へ実装するさいには論理規模も大幅に削減できることが確認できた．今後は消費電力の測定と，電力差分攻撃に対する耐性評価を行っていく．

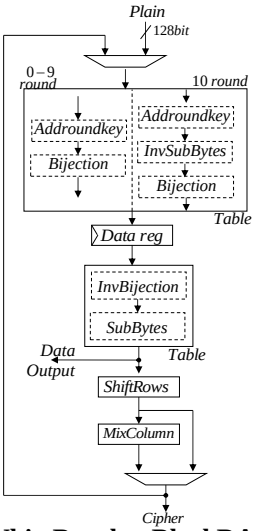

図 5 WhiteBox_by_BlockRAM 回路

表 1 FPGA への実装結果

	occupied Slices	BlockRAM	Max.Freq(MHz)
original	521	6	220
fixed_round_key	439	6	216
xor_by_ROM	344	6	259
xor_by_BlockRAM	410	24	114
WhiteBox_by_BlockRAM	302	22	107

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] Shunsuke Matsuoka, Shuichi Ichikawa: "Reduction of Power Consumption in Key-specific AES circuits," Proceedings of the Third International Conference on Networking and Computing (ICNC 2012), pp. 323-325 (2012).
[3] S. Chow, P. A. Eisen, H. Johnson, and P. C. van Oorschot, “White-Box Cryptography and an AES Implementation”, SAC202, LNCS, vol. 2595, pp.250-270.
[4] 東北大学青木研究室，AES IP Core，http://www.aoki.ecei.tohoku.ac.jp/crypto/web/cores.htm
[5] 辻村 達徳，高橋 芳夫，松本 勉, “テーブルネットワークを用いた FPGA 実装 AES とその電力差分解析耐性”, 電子情報通信学会技術研究報告．ISEC, 情報セキュリティ研究会，106(352), pp.33-40, (2006)