ハードウェア特殊化 AES 暗号回路の耐タンパ性に関する研究

研究代表者　　松岡　俊佑　　旭川高専　機械システム工学科　准教授

1 はじめに

入力暗号鍵をあらかじめ決定しておき，論理回路に埋め込むタイプの AES 暗号回路[1],[2]は FPGA への実装において，オーソドックスなループ型アーキテクチャと比較して，少ない論理ブロック量で実装することができ，消費電力も削減効果も得られる．暗号回路に求められる性能の一つにサイドチャネル攻撃に対する耐タンパ性がある．とりわけ電力解析[3]は回路動作時の消費電力をもとに暗号鍵情報を暴き出すことができ，セキュリティ上の大きな脅威となっている．電力解析攻撃の代表的な手法の一つに相関電力解析[4]がある．本研究では，鍵埋め込み型 AES 暗号回路の相関電力解析への耐性評価を行ったので報告する．

2 ループ型 AES 暗号回路

AES暗号は128bitの平文をブロック単位としてSubBytes, shiftRows, MixColumns, AddRoundKey の 4 つの基本処理を順番に 0～10 ラウンド繰り返すことにより暗号文が生成される[5]．各ラウンドにおける AddRoundKey では，128bit のラウンド鍵との排他的論理和演算をとる．0～10 ラウンド鍵は 128bit の入力暗号鍵をもとに鍵拡張処理にて生成される．AES 暗号回路にはさまざまなアーキテクチャ方式が研究されている[6-9]．このうち一般的なアーキテクチャ方式として，1 ラウンドごとに回路処理し，ラウンド回数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[10]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．

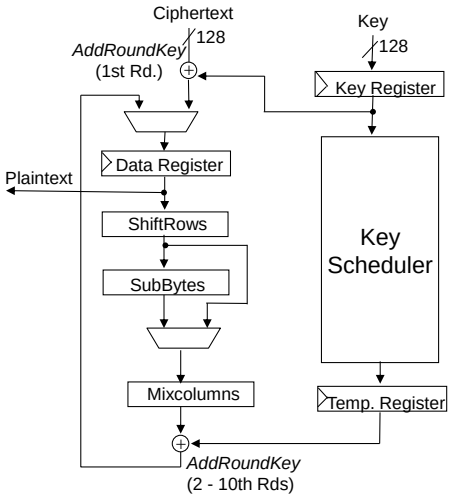

図 1．ループ型 AES 暗号化回路

3 鍵埋め込み型 AES 暗号回路

論理回路の一部の入力が定数値であるならば，最適化設計することでゲート数を削減することができる．これを部分評価または回路特殊化という．本節では，われわれがこれまでに提案した入力暗号鍵を定数に固定した AES 暗号回路について述べる．

3-1 XOR_by_RAM 回路

入力暗号鍵が定数であるならば，鍵拡張部で生成されるラウンド鍵も定数値となる．あらかじめラウンド鍵を生成しておき，回路内部の RAM に保存しておけば，鍵拡張部は省くことができる．図 2 に示した XOR_by_RAM 回路では，AddRoundKey へのラウンド鍵入力を定数とし，さらに全 128bit の排他的論理和処理を 8 ビットごとにテーブル化し，RAM として実装する．RAM のアドレス入力は，ラウンド選択用に 4 ビット追加し，12 ビットとし，容量は 11 ラウンド×28＝352 byte となる．FPGA のブロック RAM に全 16 個の RAM を実装すれば，論理ブロックの使用容量を削減することができる．

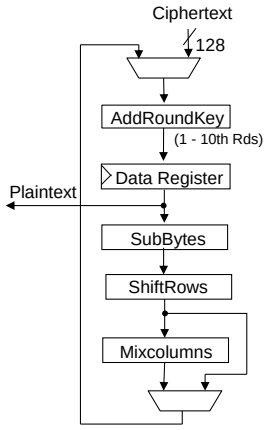

図 2. XOR_by_RAM 回路

3-2 S-BOX Absorption 回路

AES 暗号の基本処理の一つである SubBytes は，S-BOX と呼ばれる 8 ビット入出力の非線形変換処理からな

公益財団法人電気通信普及財団
研究調査助成報告書　第35号　2020年度

る．評価の基本として用いた青木研のループ型 AES 暗号回路では，S-BOXは8ビット幅のテーブル×16個で回路が構成されている．一方，XOR_by_RAM回路のAddRoundKeyテーブルも8ビット幅のテーブル×16個からなる．図 3 の S-BOX Absorption 回路[11]では，S-BOX と AddRoundKeyテーブルを8ビットごとに1つのテーブルに統合し，FPGAの内蔵ブロック RAM へ実装する．ただし，最終 10 ラウンドではSubBytesは実行されないので，AddRoundKey処理のみでテーブル化する．S-BOX は AES 暗号回路のうちで論理規模の大部分を占める回路であるので，その削減効果は大きい．

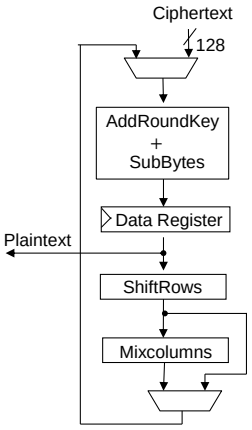

図 3. S-BOXAbsorption 回路

3-3 WhiteBox 暗号回路

前述のXOR_by_RAM回路やS-BOX Absorption回路のXORテーブルは，FPGAの内蔵BRAMへの実装を想定している．BRAMは，論理ブロックに比べて構造がシンプルなので，リバースエンジニアリングの標的になりやすく，BRAMの情報を手がかりにして鍵が解読されてしまう危険性がある．このような環境下において，鍵情報を秘匿化する技術にホワイトボックス暗号システムがある[12]．もともとは，暗号プログラムコード内に記述された暗号鍵などの秘密情報を秘匿化するのに使われていた手法で，AES 暗号回路へも適用することができる[13]．その仕組みを図4に示す．あるテーブル関数A，Bが順に実行される場合を考える．Bは，鍵入力を固定値としテーブル化されている．テーブルBに含まれる鍵情報を秘匿化するのに，ホワイトボックス暗号システムを適用する．テーブルAの出力後に，ランダムに生成した全単射テーブルを挿入し，A と全単射テーブルを一つのテーブルに統合する．B の入力前に，逆全単射テーブルを挿入し，これらをひとつのテーブルに統合する．全単射と逆全単射が続けて実行されると，全単射の入力値と逆全単射の出力値は同じ値となるので，同じ処理が実行されることになる．

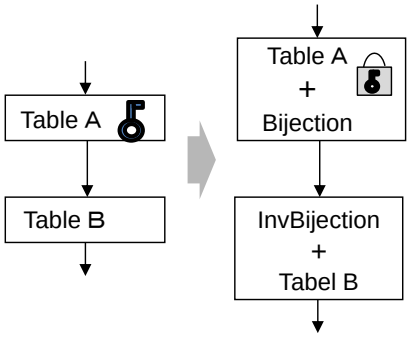

図 4 ホワイトボックス暗号システム

ここでは，ホワイトボックス暗号システムを XOR_by_RAM 回路へ適用し，鍵の秘匿性を改善した回路(図 5)について述べる．第 1～9 ラウンドのAddRouneKeyテーブルと全単射テーブルを統合させる．SubBytes処理の前に逆全単射テーブルを挿入する．iバイト目のAddRoundKeyのROMの内容は，

$$ROMi[\ r * 256 + b] = Bijection[b \oplus RKey[r][i]] \quad (r \neq 10) \quad (1)$$

となる，ここで，r はラウンド数，b は XOR テーブルへの入力値，Bijectionは全単射変換，RKeyはラウンド鍵を表す．最終10ラウンドだけは，AddRoundKey の出力が暗号文となるので全単射を挿入できない．そこで，SubBytes処理後に出力を取り出すこととし，最終10ラウンドに実装するROMの内容は，

$$ROMi[\ r * 256 + b] = InvSubBytes\ (InvBijection\ [b \oplus RKey[r][i]])\ (r = 10) \quad (2)$$

とする．

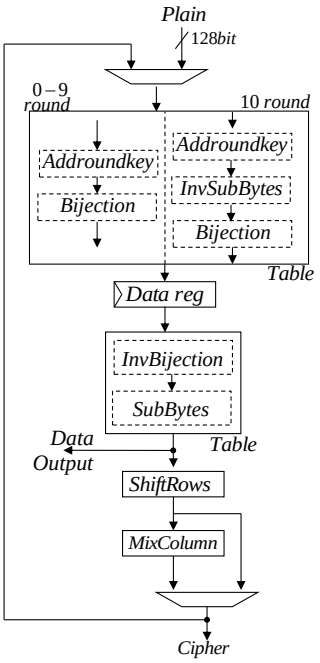

図 5 ホワイトボックス暗号回路

公益財団法人電気通信普及財団
研究調査助成報告書 第35号 2020年度

6. SAC テストによる難読化評価

ここでは，ホワイトボックス暗号回路の AddRoundKey＋全単射テーブルの難読化強度の評価を行う．評価手法には，乱数のランダム性や S-BOX のような非線形変換処理の分散性を調べるのに用いられる SAC テスト[14]を適用する．

ハミング距離が 1 となるテーブルへの入力 x,y の全ての組み合わせ，

$$\forall x,y|H(x,y)=1 \quad (3)$$

において，テーブル出力 F(x)，F(y)のハミング距離を H(F(x) ，F(y))とする．理想的に分散されているテーブルと，評価対象となるテーブルとの H(F(x) ，F(y))の χ^2 検定が SAC テストの評価値となる．

XOR_by_RAM 回路の AddRoundKey テーブル，および WhiteBox 回路の AddRoundKey＋全単射テーブルの SAC テストの評価結果を表 1 に示す．入力暗号鍵 100 個について，それぞれテーブルを生成し，χ^2 検定の平均ととった．ただし， 全単射テーブルにも SAC テストを施行し，χ^2 検定値が 20(危険率 0.01)以内になるように生成した．XOR_by_RAM 回路では，テーブル値が偏って分散されており，χ^2 値は危険率を大きくオーバーしている．一方，WhiteBox では，χ^2 値は危険率を 20 以内に収まり，全単射変換挿入したことによりテーブル値が十分に分散されていることが確認できた．

表 1. SAC テストの評価結果

	XOR_by_RAM	WhoteBox
χ^2 値	361274	16.9

7 FPGA への実装評価

ここでは，評価の基本として用いた青木研究室の AES 暗号回路(original)，XOR_by_RAM 回路，S-BOX Absorption 回路，WhiteBox 回路を FPGA に実装評価した結果について述べる．ターゲットデバイスには，FPGA(Virtex5 XC5VLX30)とした．論理合成・配置配線ツールは ISE14.7 を用いてデフォルト設定で回路を生成する．実装結果を表 2 に示す．

表 2 FPGA への実装結果

Design	Logic Scale (Slices)	BlockRAM	Max. Freq .(MHz)	AT Product (slice*msec)
original[3]	522	6	220	2.4
xor_by_RAM[2]	378	18	97	3.9
S-BOX Absorption	214	18	215	1.0
WhiteBox	369	18	97	3.8

Original 回路では BlockRAM を S-BOX で 4 個，残り 2 個を外部入出力用のデータバッファで使用している．original 以外の回路で使用している 18 個の BlockRAM のうち分けは，外部入出力用のバッファに 2 個，AddRoundKey テーブルに 16 個となっており．S-BOX は論理ブロック(slice)を使用して実装されている．論理規模（Logic Scales）は，Original 回路にたいして XOR_by_RAM 回路は 28%減．S-BOX Absorption 回路は 59%減と削減効果がみられる．一方，WhiteBox 回路についても，論理規模は 29%減と，XOR_by_RAM 回路と同規模で実装できる．

8 相関電力解析

7-1 実験環境

AES 暗号回路に対する電力解析手法には,Kocher らが考案した電力差分解析(Differential Power Analysis, DPA)や，DPA を拡張した相関電力解析(Correlation Power Analysis, CPA)がある．とりわけ CPA は，より少ない電力波形で暗号鍵が特定可能な強力な攻撃手法として知られている．ここでは，オーソドックスなループ型 AES 暗号回路および鍵埋め込み型 AES 暗号回路に対して CPA 攻撃を実施し，その耐性評価を行った．CPA の手順を図に示す．Xilinx 社の FPGA（Virtex5 XC5VLX30)に各種 AES 暗号回路を実装する．平文を変えなが

ら回路動作時の電力波形をオシロスコープ(DSO1024A, Agillent Tec. Co.)で 2 万回繰り返し測定する．ループ型 AES 暗号回路では，各ラウンドの中間データはデータレジスタに格納される．CPA では最終第 10 ラウンドのレジスタ出力 Tn[10][i]と第 9 ラウンドのレジスタ出力 Tn[9][i]との間の遷移情報(ハミング距離 hn[i])と，消費電力波形 Wn[j]との相関値 r(i, j)を次式にて算出して鍵情報を特定する．

$$r(i,j)=\frac{\sum_{n=1}^{N}(h_n[i]-\bar{h}_n[i])\cdot(W_n[j]-\bar{W}_n[j])}{\sqrt{\sum_{n=1}^{N}(h_n[i]-\bar{h}_n[i])^2\cdot\sum_{n=1}^{N}(W_n[j]-\bar{W}_n[j])^2}} \quad (4)$$

ここで，$\bar{h}_n[i]$ は i バイト目における全暗号出力のハミング距離の平均値を表す．Wn[j] は時刻 j における全電力波形の平均値を表す．第 10 ラウンド出力(暗号文) Tn[10][i] は攻撃者には入手可能とする．第 10 ラウンド鍵の i バイト目のラウンド鍵 RKey[10][i] を推定入力し，第 9 ラウンドのレジスタ出力値 Tn[9][i] を次式で算出する

Tn[9][i]=InvSubBytes[(InvShiftrows[T[10][i] ⊕ RKey[10][i]) (5)

ただし，S-BOX Absorption 回路では，第 10 ラウンドのテーブル RAM は SubByte を含まないので，第 9 ラウンドのレジスタ出力値は次式で算出する．

Tn[9][i]= InvShiftrows[T[10][i] ⊕ RKey[10][i]] (6)

9 相関電力解析の結果

サイドチャネル攻撃用標準評価ボードへ前節で述べた original，および鍵埋め込み型 AES 暗号回路(XOR_by_RAM, S-BOX Absorption)を実装し，各回路に対して CPA 実験を行った．図 6 は各実装回路において，各波形数における正解鍵の導出に成功したバイト数を示している．AES_TBL と XOR_by_ROM は数百波形で全バイトの第 10 ラウンドの鍵の導出に成功している．しかし，S-BOX Absorption は波形数を増やしても i =0～3 バイト目の鍵が導出されない．この 4 バイト分は AES 暗号処理の InvShiftorows 処理においてシフト変換処理されず，第 9 ラウンドのレジスタ出力値は次式となる．
この値と第 10 ラウンドの i=0～3 バイト目のレジスタ出力 Tn[10][i]とのハミング距離をとると，

hn[i]= HD[T[10][i], T[10][i] ⊕ RKey[10][i]] (i=0～3) (7)

となり，第 10 ラウンドのレジスタ出力 T[10][i]がどのような値においても，ハミング距離は一定値となる．よって相関値の導出が不可となる．WhiteBOX 回路は全単射および逆全単射テーブルにより部分鍵 RKey が難読化されているのでハミング距離との間には相関が得られず，全バイトにおいて鍵が導出されなかった．

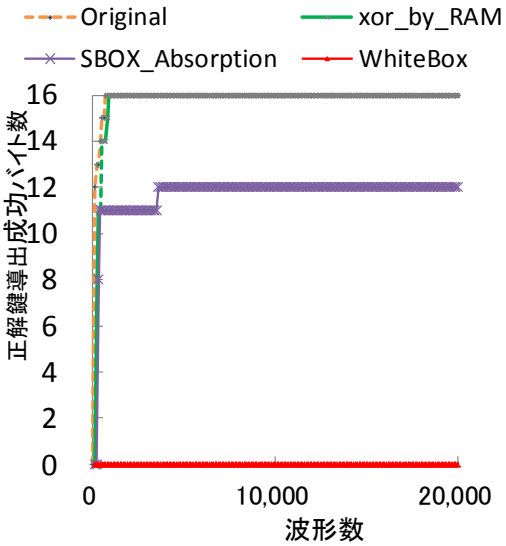

図 6. CPA の結果

10 おわりに

筆者らはこれまでに入力鍵を回路に埋め込みタイプの 2 種類の AES 暗号回路(XOR_by_ROM, S-BOX Absorption)を提案した．FPGA への実装評価では，オーソドックスな AES 暗号回路と比較して，論理回路量(slices)を削減することができる．また，消費電力についても若干の削減効果がみられる．本研究で新たに鍵埋め込み型 AES 暗号回路の相関電力解析(CPA)に対する耐性評価実験を行った．その結果，S-BOX Absorption は 4 バイト分の最終ラウンド鍵が導出されなかった．しかしながら，4 バイトの総当りにより，AES のすべての鍵（16 バイト）は現実的な時間で導出できるため，CPA に対しての耐タンパ性は不十分である．一方，HhiteBox 暗号回路は，鍵情報を難読化したことにより，全１６バイトの鍵が導出されず，CPA に対しての耐タンパ性をもつことが確認できた．

【参考文献】

[1] R. Atono and S. Ichikawa, “Design and Evaluation of Data-dependent Hardware for AES Encryption Algorithm,” IEICE Transactions on Information and Systems, vol. E89-D, no. 7, pp. 2301–2305, 2006.

[2] S. Matsuoka and S. Ichikawa, “Reduction of power consumption in key-specific AES circuits,” in Proc. 3rd International Conference on Networking and Computing, 2012, pp. 323–325.

[3] P.Kocher, J.Jaffe, and B.Jun, “Differential Power Analysis,” Crypto 1999, LNCS, Vol.1666, pp.388-395, 1999.

[4] E.Brier, C.Clavier, F.Oliver, ”Correlation power analysis with leakage model,” CHES2004, LNCS, Vol.3156, pp16-29, 2009.

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

[6] F.-X. Standaert, G. Rouvroy, J.-J. Quisquater, and J.-D. Legat, “Efficient Implementation of Rijndael Encryption in Reconfigurable Hardware:Improvements and Design Tradeoffs,” in Proc. 4th International Workshop on Cryptographic Hardware and Embedded Systems, pp.334–350. 2003.

[8] S. Morioka and A. Satoh, “An Optimized S-Box Circuit Architecture for Low Power AES Design,” in Proc. 4th International Workshop on Cryptographic Hardware and Embedded Systems, 2003, pp. 172–186.

[9] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, “A Compact Rijndael Hardware Architecture with S-Box Optimization,” in Proc.7thInternational Conference on the Theory and Application of Cryptology and Information Security, pp. 239–254, 2001.

[10] J. M. Granado-Criado, M. A. Vega-Rodr´aguez, J. M. S´anchez-P’erez,and J. A. G´omez-Pulido, “A new methodology to implement the AES algorithm using partial and dynamic reconfiguration,” Integration, the VLSI Journal, vol. 43, no. 1, pp. 72–80, 2010.

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

[12] Shunsuke Matsuoka, Naoki Fujieda, Shuichi Ichikawa: "S-Box Absorption Design for Key-Specific AES circuits," Proc. International Conference of Global Network for Innovative Technology (IGNITE2014), pp. 316--319 (2014).

[13] Chow, S., Eisen, P., Johnson, H., & Van Oorschot, ” White-box cryptography and an AES implementation. In Selected Areas in Cryptography”, pp. 250-270, 2003.

[14] 松岡俊佑，市川周一： “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,” 第 12 回情報科学技術フォーラム (FIT 2013), C-014, (2013).

[15] J.C.H. Castro, J.M. Sierra, A. Seznec, A. Izquierdo, A. Ribagorda, “ The strict avalanche criterion randomness test”, Mathematics and Computers in Simulation, 68 (1) (2005), pp. 1–7

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
鍵埋め込み型 AES 暗号回路の相関電力解析に対する耐性化	2020 年電子情報通信学会総合大会	2020 年 3 月 17 日
鍵埋め込み型ホワイトボックス AES 暗号回路の電力解析環境の構築	令和元年度電気・情報関係学会北海道支部連合大会	2019 年 11 月 10 日