C-012

AES 暗号化回路の実装方法に依存しない CPA 対策回路

CPA Countermeasures Independent of Implementation of AES Encryption Circuits

渡邊 翔† 籠谷 裕人†
Sho Watanabe, Hiroto Kagotani

1. はじめに

近年，IoT 時代の到来により，私たちの生活がより便利になる一方で，インターネットを介して通信を行うデバイスは常に攻撃の危険性に晒されている．このような状況から暗号に求められる信頼性は高くなっており，近年は多くのデバイスに対して暗号回路が安全な通信のためにハードウェア実装されている．一方で暗号に対する攻撃手法の研究が盛んに行われている．その 1 つとして暗号のハードウェア回路から得られる処理時間，消費電力，放射電磁波などといった物理的情報のデータ依存性を用いて情報を解析する非破壊攻撃であるサイドチャネル攻撃が危険視されている．そのため，設計者はサイドチャネル攻撃への対策をしたデバイス設計を行う必要がある．

消費電力を用いたサイドチャネル攻撃の代表的な攻撃法法として，1 つの消費電力波形から解析する単純電力解析 (SPA：Simple Power Analysis)，消費電力波形を繰り返し測定し，統計的に処理を行い解析をする差分電力解析 (DPA : Differential Power Analysis)[1]，消費電力波形及び暗号文と予測鍵をもとに計算されるデータ候補との相関から解析をする相関電力解析 (CPA : Correlation Power Analysis)[2], [3]の 3 つがある．

本研究では，AES (Advanced Encryption Standard) 暗号[4]を対象として，暗号処理の消費電力波形をかく乱する消費電力を発生させるため，乱数生成器と非線形な演算回路を直列に連結した対策回路を実装した．非線形な演算として AES 暗号の処理の 1 つである SubBytes，有限体上の乗算および二乗算を用いた，無対策版と連結数の異なる各演算の対策版とを比較することにより，相関電力解析へ耐性評価を行う．

2. 基礎

2.1 AES 暗号

AES 暗号はブロック長 128bit のブロックをデータの単位として暗号化・復号化を行う共通鍵暗号方式である．今回は鍵長 128bit のものを使用しており，入力データ 128bit を 8bit ずつ分割しラウンド数-1 回 SubBytes，ShiftRows，MixColumns，AddRoundKey の処理を行う．最終ラウンドは MixColumns 以外の処理を行う．

SubBytes で用いる S-box は有限体$GF(2^8)$上の逆元演算とアファイン変換を組み合わせて定義される．そのため，S-box を表引きではなく演算器として実現できる．本研究では，暗号化回路と対策回路には合成体を用いた S-box[5]を使用している．

† 岡山大学 Okayama University

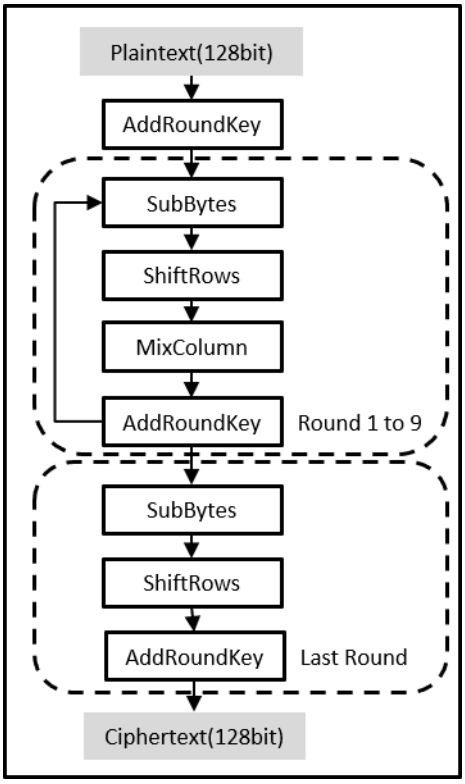

図 1. AES-128 アルゴリズム

2.2 相関電力解析(CPA)

相関電力解析(CPA)とは推測した部分鍵と既知データ(平文または暗号文)から計算される中間データ候補と，暗号回路から発生する消費電力との相関を計算し，部分鍵を特定する攻撃手法である．

AES 暗号での処理の際，10 ラウンド目では MixColumns を行わない．そのため暗号化後の暗号文と予測鍵から 9 ラウンド目の出力の推測が可能である．予測した 9 ラウンド出力と 10 ラウンド出力のハミング距離と推測した消費電力に相関があると仮定し，ピアソンの相関係数を求める．(式 1)

$$\rho_{W,H_i^{k_b}} = \frac{\frac{1}{n}\sum_{n=1}^{N}[W_n - \bar{W}]\,[H_{n,i}^{k_b} - \overline{H_l^{k_b}}]}{\sqrt{\frac{1}{n}\sum_{n=1}^{N}[W_n - \bar{W}]^2}\sqrt{\frac{1}{n}\sum_{n=1}^{N}[H_{n,i}^{k_b} - \overline{H_l^{k_b}}]^2}} \quad (1)$$

ここでWとHは電力波形とハミング距離，$\bar{W}$と$\bar{H}$は平均電力波形と平均ハミング距離である．この相関係数が大きいものが正解鍵となる．

3. 対策回路の回路構成

本研究の対策回路では，AES 暗号の実装方法に依存せず動作する乱数と非線形な演算回路を用いた．回路構成を以下の図に示す．(図 2)

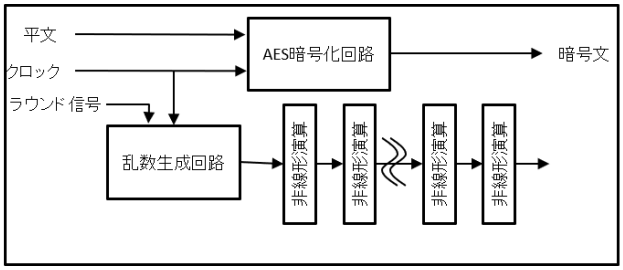

図 2．対策回路

3.1 乱数生成器

乱数生成回路の回路構成は排他的論理和とシフトレジスタとフィードバックで形成される線形帰還シフトレジスタである．回路構成を以下の図に示す．(図 5)

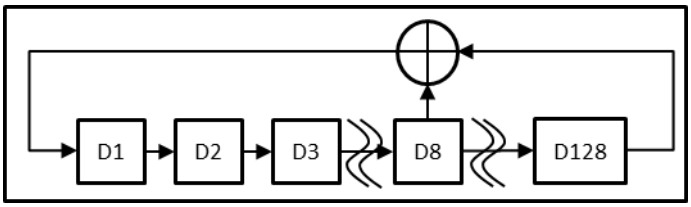

図 5．乱数生成回路の構成

用いた多項式は$x^{128}+x^{8}+1$を使用した．非線形回路の入力には下位 32bit または 8bit を用いた．回路は暗号化時のラウンド制御の信号が“1”の時のみクロックに同期してシフトレジスタが動き，値が更新されるように設計している．

3.2 非線形演算

非線形演算では AES 暗号の SubBytes，乗算，二乗算を使用した．論理合成時に最適化を防ぐために，最終演算後の結果全てのビットを XOR ゲートを用いて 1 bit の出力とし，汎用ピンに出力している．

3.2.1 SubBytes の構成

SubBytes では AES 暗号化回路部分でも使用している合成体で構成された SubBytes を用いている．乱数生成回路で生成された 32bit を入力とし，演算結果を次の SubBytes に入力とする．今回は連結数を 1～8 個とした．

3.2.2 乗算の構成

乗算では 8bit を入力とし，多項式$x^4+x+1=0$による 4×4bit の演算を行う．乗算器は AND ゲートと XOR ゲートを用いて構成する．1 つ目は入力値の 1～4bit と 5～8bit による乗算結果を出力の 1~4bit とし，2 つ目は入力値の 1，3，5，7bit と 2，4，6，8bit による乗算結果を出力の 5～8bit とする．今回は連結数を 20，40，60，80，100，120，140 個とした．

3.2.3 二乗算の構成

二乗算では 8bit を入力とし，多項式$x^8+x^4+x^3+x^2+1=0$による 8bit の乗算を行う．二乗算器は XOR ゲートを用いて構成する．今回は連結数を 50，100，150，200，250，300，350 個とした．

3.3 回路規模の比較

対策回路を Verilog を用いて記述し，暗号化回路とともに Xilinx ISE14.7 を用いて論理合成した．回路規模の比較を (表 1) に示す． SB1~8 は SubBytes を用いた対策を表し，SB の後ろの数字は連結数を表す． mul20~140 は乗算を用いた対策を表し，mul の後ろの数字は連結数を表す． sq50~350 は二乗算を用いた対策を表し，sq の後ろの数字は連結数を表す．

表 1．対策の回路規模比較

	LUT 数	スライス数
default	3269	1090
SB1	3608	1195
SB2	4036	1354
SB3	4346	1494
SB4	4662	1684
SB5	4978	1685
SB6	5198	1774
SB7	5398	1953
SB8	5800	2108
mul20	3712	1295
mul40	4040	1132
mul60	4372	1474
mul80	4703	1544
mul100	5030	1678
mul120	5357	1813
mul140	5691	1952
sq50	3529	1150
sq100	3676	1142
sq150	3832	1382
sq200	3977	1301
sq250	4126	1285
sq300	4280	1511
sq350	4428	1490

Default 版と回路規模を比較して最大で SubBytes を用いた対策は 1.77 倍，乗算を用いた対策では 1.74 倍，二乗算を用いた対策では 1.35 倍となり，回路規模では二乗算が小さい回路実装となった．また，SB3 と mul60 と sq300 が同程度のサイズである．

4. 評価実験

4.1 実験方法

実験方法としては，PC から FPGA 上に平文，秘密鍵を送信するプログラム SASEBO_G_CHECKER を用いて，平文を 0 から 1 ずるインクリメントして暗号化を行い，その電圧波形を PC 上に 1 万波形分保存する．秘密鍵は「2B 7E

15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C」を用いた．取得した波形に対し，解析用プログラムを実行することにより，ハミング距離モデルによる相関を算出し，波形数ごとの解読可能な鍵のバイト数を特定する．今回の実験で使用した器具を以下の表に示す．(表 2)

表 2．実験使用器具

使用器具	メーカ名，型番，仕様，設定値
評価基板	SAKURA-G
FPGA	XilinxSpartan-6 (XC6SLX75) Xilinx Spartan-6 (XC6SLX9)
Oscilloscope	Keysight，DSOS104A Frequency band: 1GHz 1GS/s，averaging : 1
Passive Probe	Cinch Connectors 同軸ケーブルアセンブリ 425-0028-012 Agilent Technologies N2853A

4.2 実験結果

default 版と 3 章で示した対策回路 22 種類に対して相関電力解析を行った．それぞれで求められた最大相関係数を (表 5) に示す．

表 5．それぞれの対策の最大相関係数

	最大相関係数
default	0.5122
SB1	0.2807
SB2	0.1860
SB3	0.1553
SB4	0.1089
SB5	0.0955
SB6	0.0841
SB7	0.0580
SB8	0.0472
mul20	0.4229
mul40	0.3483
mul60	0.2590
mul80	0.1762
mul100	0.1370
mul120	0.1121
mul140	0.1014
sq50	0.3091
sq100	0.1968
sq150	0.1663
sq200	0.1176
sq250	0.0820
sq300	0.0583
sq350	0.0426

相関係数から計算される CPA を用いて予測した鍵の正当バイト数をそれぞれの対策ごとに (図 6) (図 7) (図 8) に示す．横軸は解析に用いた波形数，縦軸は解析可能バイト数である．

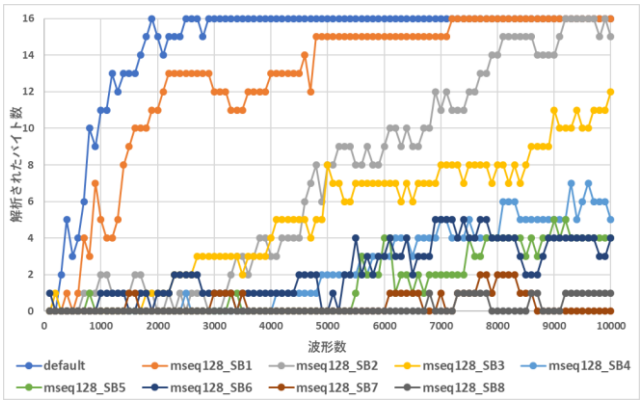

図 6．SubBytes を用いた対策の波形数ごとの解析可能バイト数

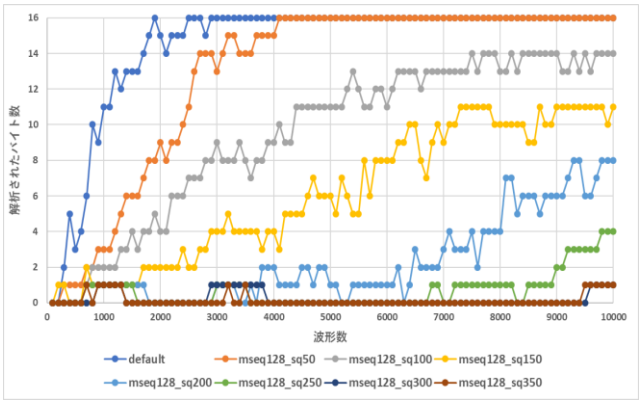

図 7．乗算を用いた対策の波形数ごとの解析可能バイト数

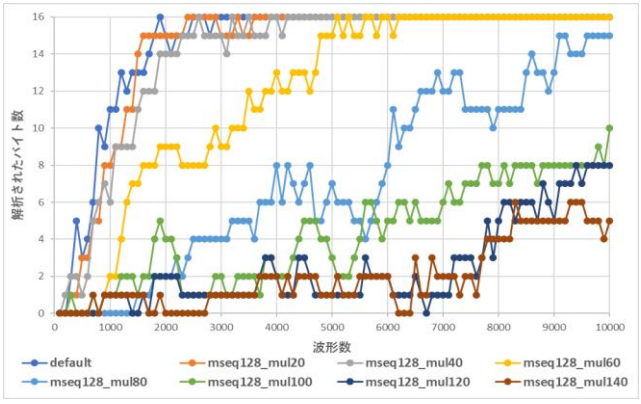

図 8．二乗算を用いた対策の波形数ごとの解析可能バイト数

対策回路は非線形演算回路の連結数が増加するにつれ最大相関係数が小さくなり，1 万波形時の解析されたバイト数も少なくなっている．default 版は 1900 波形で全バイトを解析されているのに対して，SubBytes，乗算，二乗算を用いた対策では連結数が最大の時，1 万波形ではそれぞれ 1Byte，5Bytes，1Byte としか解析されていない．波形数に対する CPA 耐性は二乗算を用いた対策が最も高く，乗算を

用いた対策が最も低いという結果である．また，同回路規模である SB3 と mul60 と sq300 で比較した場合，最大相関係数は二乗算が 3 種類の中で小さい 0.0583 であり，CPA を行った際に解析されたバイト数も 1 Byte であり，最も解析されていない．これらの事から，回路規模も含めると二乗算を用いた対策が回路規模に対して最も効果があると言える．

4.3 考察

評価結果より二乗算を用いた対策が最も回路量あたりの CPA 耐性が高いという結果が得られた．SubBytes，乗算，二乗算のそれぞれの回路は組み合わせ回路により設計されており，それぞれの LUT の出力が次の LUT の入力として到着するまでに遅延量に違いがあるため，演算結果が確定するまでに LUT の結果が何回か変動するために消費電力がランダムに発生し，AES 暗号の消費電力をかく乱させる効果が生まれているのではないかと考える．そのため，非線形演算回路が増加するにつれ，LUT に到着する信号というのも遅延差が大きくなり消費電力も大きくなり CPA への対策効果が大きくなっている．それぞれの非線形演算回路の中で二乗算回路が遅延差が大きくなりやすい回路かつ 1 段あたりの回路規模が小さいため，本研究の中で最も小規模回路かつ高い CPA 耐性があると考えられる．

5. まとめ

本研究では，AES 暗号を対象として AES 暗号の SubBytes，乗算，二乗算を用いた対策回路を提案・設計した．そして，default 版，対策回路 22 種類を FPGA 上に実装し，回路規模を比較し，CPA 評価を行った．

対策回路を用いた場合，default 版と比べて回路規模は SubBytes の場合 1.77 倍，乗算を用いた場合 1.74 倍，二乗算を用いた場合 1.35 倍となった．CPA で得られた解析バイト数は 非線形演算回路の連結数を増加させるにつれ，最大相関係数は小さくなり，1 万波形使用時の解析されたバイト数は少なくなった．SubBytes を用いた場合は 1Byte，乗算を用いた場合は 5Bytes，二乗算を用いた場合は 1Byte という結果が得られた．また，同回路規模で比較した場合，二乗算を用いた対策が最も回路量あたりの CPA 耐性が高いということが分かった．今後の課題と，10 万波形用いて CPA 攻撃を行った際の CPA 耐性の評価と加算や減算など単純な回路を用いた場合の CPA 耐性評価を行い，対策としてより効果的な演算回路を見つけることである．

参考文献

[1] P.C Kocher, J.M Jaffe, B.C Jun, “Differential Power Analysis”, Proceedings of CRYPTO'99, pp.388-397 (1999)
[2] E.Brier C.Clavier, and F.Olivier, “Correlation Power Analysis with a Leakage Model”, CHES2004, LNCS 3156, pp.16-29 (2004)
[3] E.Brier, C.Clavier, F.Olivier, “Optimal Statistical Power Analysis”, Gemplus Card International, France Security Technology Department (2003)
[4] NIST, “Advanced Encryption Standard(AES)”, FIPS PUB 197, Computer Security Division Computer Security Resources Center, [online] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS. 197.pdf
[5] Sumio Morikoka, Akashi Satoh, “An Optimized S-Box Circuit Archtecture for Low Power AES Design” , CHE2002, LNCS, pp.172-186, Springer-Verlag(2003)