L-021

対数モデルを用いた相関電力解析

Correlation Power Analysis Attack used a logarithmic model

櫻井　敦規†　　岩井　啓輔†　　黒川　恭一†
Atsunori Sakurai　　Keisuke Iwai　　Takakazu Kurokawa

1．まえがき

情報技術の発達により，各情報端末及び通信の安全性を確保する必要性が高まっている．その安全性を確保する技術の中核として暗号が利用されている．暗号アルゴリズムは，一般にその内部が公開されており，多数の研究者により検証され，強度が立証されたものが使用されている．しかしながら，近年，暗号を実装したモジュールの消費電力等のサイドチャネル情報を計測することで，暗号解読を行う攻撃手法(サイドチャネル攻撃)の危険性が指摘されている．サイドチャネル攻撃の一種である電力解析に，Brier ら[１]によって提案された相関電力解析（CPA：Correlation Power Analysis）があり，消費電力と中間値のハミング距離に線形の関係があることを仮定している．CPA は未対策のデバイスでは比較的少ないデータ数で鍵の特定が可能な攻撃法である．ここでは，ループアーキテクチャでハードウェア実装された AES に対し，消費電力と中間値のハミング距離には非線形の関係があることを示し，CPA に対数モデルを適用することにより，鍵特定に必要な波形数を削減可能であることを示す．

2．対数モデル CPA

本章では，CPA の概要について述べ，また，消費電力と中間値の予想鍵が非線形の関係であることを示す．

2.1　CPA の概要

CPA は図１に示すように，暗号文と予測した部分鍵から遷移前のデータレジスタの値を予測し，データレジスタの遷移前後のハミング距離を予測する．

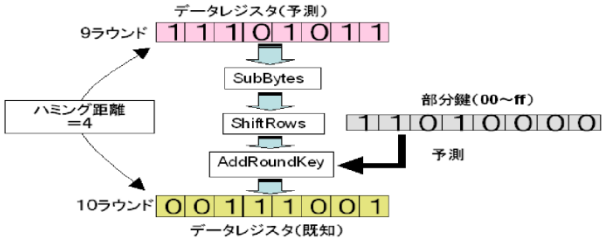

図１　ハミング距離の予測

予測したハミング距離とそれに対応した消費電力データから式（１）に示すピアソンの積率相関係数を求め，最も強い相関を示した部分鍵を正解鍵として推測する．この相関係数の計算には，ハミング距離と消費電力の間に線形の関係があることを仮定しており，ハミング距離と消費電力に線形の相関がない場合は相関値が小さくなる．

$$\hat{\rho}_{W_H}(R) = \frac{N\sum W_i H_{i,R} - \sum W_i \sum H_{i,R}}{\sqrt{N\sum W_i^2 - (\sum W_i)^2}\sqrt{N\sum H_{i,R}^2 - (\sum H_{i,R})^2}} \qquad (1)$$

ここで，N はサンプル数（i=1,...,N），W_i は消費電力，$H_{i,R}$ は部分鍵 R で得られた中間値のハミング距離である．

2.2　AES 最終ラウンドの消費電力モデル

現在一般に使用されている CMOS LSI は CMOS のスイッチングによる動的消費電力と常時消費される静的消費電力の 2 種類がある．静的消費電力は，使用するデバイスにより決まっている一定の消費電力であるため，動的消費電力に着目して考察を行う．

まず初めに，レジスタの消費電力について考察を行う．レジスタの動的消費電力はレジスタの遷移ビット数（ハミング距離）は CMOS のスイッチング回数に比例する.ゆえに，動的消費電力は，ハミング距離に比例する．

次に，SubBytes の消費電力について考察する．SubBytes は入力と出力は必ず異なる値となるように設計されているため，入力値が変化すると必ず出力値が変化する．ゆえに，AES の構造上，レジスタの値が遷移すれば必ず SubBytes の動的消費電力が発生することになる．また，入力される平文がランダムであれば，最終ラウンドの実行前のレジスタの値はランダムになるため，平均するとレジスタ値が遷移する場合の SubBytes の動的消費電力は一定値に次第に収束すると考えられる．一方，レジスタ値が遷移しない場合は最終ラウンドの SubBytes の入力値が遷移しないため，出力値も遷移しないため，動的消費電力は発生しない．

ShiftRows は，ハードウェア実装においてはロジックを必要とせず，ワイヤーで構成されているため，動的消費電力は発生しない．

最後に，AddRoundKey の動的消費電力であるが，鍵の値により出力の遷移確率が異なるが，レジスタや SubBytes の回路規模に比べ小さいため，動的消費電力として与える影響が小さい．よってモデルでは AddRoundKey の動的消費電力をないものとして仮定する．

これらを元に最終ラウンドの消費電力をモデル化したものを図２に示す．

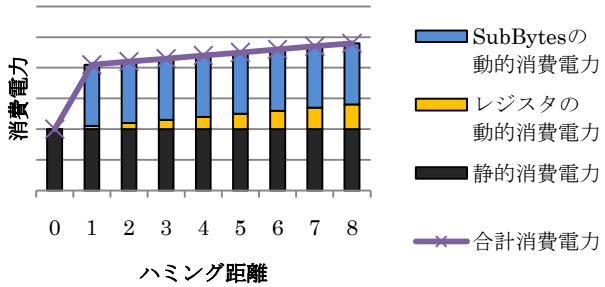

図２　ハミング距離と消費電力の関係

図から明らかの通り，ハミング距離が 0 の場合において，線形モデルから外れており，CPA の精度を下げていると考えられる．そこで，動的消費電力を適切にモデル化すれば，

†　防衛大学校　情報工学科

CPA の精度を改善することが可能であると考えた．しかしながら，使用する暗号デバイスの各構成要素の消費電力を攻撃者が事前に知ることは困難である．そこで，次の条件を満たす関数で近似することにより攻撃精度の改善を図る．その条件は，単純増加関数であり，最初は変化量が大きく，次第に変化量の小さくなる関数である．これを満たす関数として対数関数がある．

2.3 対数モデル CPA

最終ラウンドの消費電力を対数を用いて近似し，これを CPA に適用すると式（2）となり，これを最大とする部分鍵が正解鍵として推定可能である．

$$\hat{\rho}w_H(R) = \frac{N\sum W_i \log(H_{i,R}+\alpha) - \sum W_i \sum \log(H_{i,R}+\alpha)}{\sqrt{N\sum W_i^2 - (\sum W_i)^2}\sqrt{N\sum \log^2(H_{i,R}+\alpha) - (\sum \log(H_{i,R}+\alpha))^2}} \quad (2)$$

ここで α はハミング距離 0 の場合に対数が定義できなくなることを避けるためのバイアス（α>0）であり，攻撃者が任意に設定するものとする．

3. 実験

3.1 実験環境

実験に用いたデバイスは，東北大学と産業技術総合研究所が共同で開発したサイドチャネル攻撃用標準評価ボードである SASEBO-G および SASEBO-R である[２]．それぞれに実装された AES 回路で暗号化を行い，そのときの消費電力をデジタルオシロスコープにて測定した．

3.2 実験結果

まず初めにモデルの正当性を確認するため SASEBO-G を用いて消費電力の測定を行った．得られた消費電力を正解鍵から求めた中間値のハミング距離で分類，平均化した結果を図３に示す．モデルと同様の傾向が表れ，ハミング距離が 0 の時に電圧が大きく下がり，線形なモデルから外れていることが確認できた．

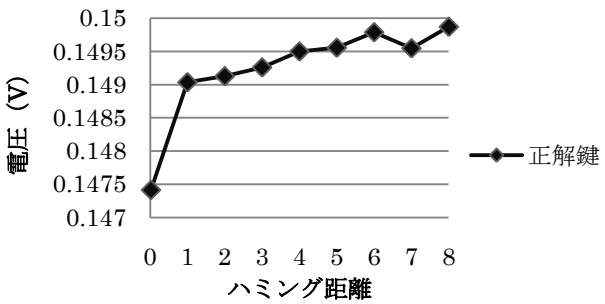

図３　ハミング距離と消費電力の関係（SASEBO-G）

続いて，通常の CPA と対数モデルを用いた CPA の比較を SASEBO-G および SASEBO-R で行った．対数モデルにおいてはバイアス値を 0.0001 から 1000 まで 10 倍ごと変化させてそれぞれの場合について比較を行った．

図４に SASEBO-G の結果を示す．対数モデル CPA は通常の CPA で必要な波形数の半分ですべての鍵を特定している．その時のバイアス値は α=0.01 であった．また，バイアス値が 100 を超えると通常の CPA と変わりがない結果となった．鍵を変更し，同様の実験を行っても対数モデルと通常の CPA を比較すると同数かそれより少ない波形数で特定可能であった．最適なバイアス値は 0.001～1 となった．

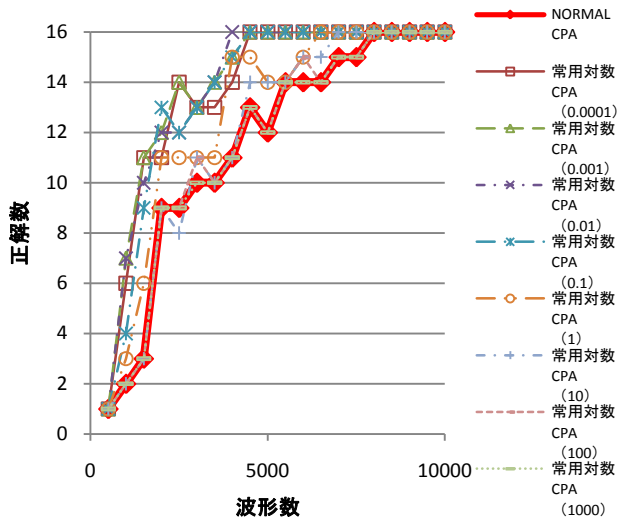

図４　CPA と対数モデル CPA の比較（SASEBO-G）

表１に SASEBO-R の結果を示す．未対策の AES 実装法では通常の CPA に比べ対数モデル CPA が，同数かそれより少ない波形数で全鍵特定に至っている．その際のバイアス値は 0.01～1 であった．サイトチャネル対策が施された実装についてはどちらの手法でも鍵は特定できなかった．

表１　全鍵特定に必要な波形数（SASEBO-R）

実装法	CPA	対数モデル CPA（バイアス値）
Comp	7500	7500（0.1）
Comp_ENC_top	10500	8500（0.01）
TBL	2500	2500（1）
PPRM1	6000	4500（1）
PPRM3	3000	2000（0.01）
S	7500	7500（1）
SSS1	×	×

4. まとめ

対数モデルを用いた CPA を提案したが，SASEBO-G および SASEBO-R での実験により，通常の CPA と比較して鍵特定に必要な波形数を同数または削減することができ，モデルの有効性を示した．最適なバイアス値はすべての場合を通して 0.01～1 程度であったが，極端に大きいまたは小さい値を使わない限り，通常の CPA と同程度または，改善が見込まれるため，実際に攻撃を行う際には，最適なバイアス値を事前に予測することは困難であるが，シビアに調整する必要性は低いものと考える．

参考文献

[1]E.Brier, C.Clavier, and F.Olivier, “Correlation Power Analysis with a Leakage Model,” CHES 2004, LNCS 3156, pp.16-29, 2004.

[2] Research Center for Information Security, AIST, “Side-channel Attack Standard Evaluation Board (SASEBO),”http://www.rcis.aist.go.jp/special/ SASEBO/index-en.html.