情報処理学会論文誌 Vol. 51 No. 6 1345–1356 (June 2010)

暗号モジュールの電力差分解析耐性評価における電力モデル等の決定方法

高橋芳夫[†1,†2] 松本勉[†2]

電力差分解析に対する暗号モジュールの耐性を評価するには，評価対象に適合した電力モデルと攻撃定義式が必要である．本論文では，電力相関解析を含む電力差分解析のある大きなクラスに対する暗号モジュールの耐性評価においては，相関係数を最大にすることを目的として電力モデル等のパラメータ推定を行えばよいことを示す．そのためのモデル式とパラメータを定める手順をブロック暗号 AES の場合を例にして示し，実際に推定値を導出する．そして電力差分解析に対する対策を特に施していない 4 種類の AES 実装について電力相関解析の実験を行い，既存の電力モデルや攻撃定義式の適用では正確に求めることが難しかった電力差分解析耐性を安定して評価できることを実証する．

How to Determine Appropriate Power Models for Fair Evalation of DPA Resistance of Cryptographic Modules

Yoshio Takahashi[†1,†2] and Tsutomu Matsumoto[†2]

An appropriate selection of power models is necessary to fairly evaluate the resistance of a cryptographic module against a class of Differential Power Analysis (DPA) attacks. If a wrong power model is adopted, the possible failure of an attack instance does not imply that the target is secure against the corresponding attack method. This paper shows that a systematic way of determining appropriate parameters in power models for a large class of DPA attacks, which includes Correlation Power Analysis (CPA). This paper confirms the effectiveness of the proposed method based on CPA experiments on four different implementations of AES, which strengths against CPA were difficult to identify by conventional methods.

1. はじめに

近年，サイドチャネル攻撃に対する安全性を確認するための評価基準の策定が急がれている．サイドチャネル攻撃とは，暗号機能を備えたセキュリティチップ等の暗号モジュールを主な対象とし，暗号処理中のチップの消費電力や放射電磁波あるいは処理時間等の測定値を分析してチップ内の秘密鍵等を特定しようとする攻撃法である．サイドチャネル攻撃の中でも DPA（Differential Power Analysis，電力差分解析[1),⋆1]）と呼ばれる攻撃法はブロック暗号に広く適用可能であるため対処が必要であると注目を集め，より強力な攻撃法の提案と対策法の研究がさかんになされてきた．そして暗号モジュールの安全性を確認するために DPA への耐性を評価する手段の研究も必要になってきている．

DPA 耐性の評価については，消費電力等を実測して求めた攻撃に必要な測定データ数あるいは測定時間や計算時間等の攻撃コストを評価基準に利用するアプローチがある．攻撃コストの算出には長時間を要することが懸念されるが，DPA 耐性が十分であることが保証された対策法は未確立なため，このアプローチが有力視されている．

DPA はチップの入出力（平文や暗号文）と測定値との間にある相関が成立することを仮定し，秘密鍵を最尤推定的な枠組みで特定するアルゴリズムであるとも見なせる．どのような確率論的モデルを仮定して尤度関数に相当する式を定義するかが攻撃コストに関わるポイントである．オリジナルな DPA の提案後，MOS トランジスタの電気的特性や DPA アルゴリズムの機能が詳細に分析され，ハミング重みモデルと呼ばれる “電力モデル” や平均差分（Difference of Means）と呼ばれる “攻撃定義式” が整理された（論文 2) 等）．このモデルや定義式によって DPA の動作原理が解明されると，その次には DPA の改善のために電力モデルと攻撃定義式の改良や精緻化が提案された．CPU や FPGA 等のデバイスの特徴（レジスタやメモリ，バスの動作，ゲートの遷移確率等）や測定手段に依存したパラメータ等に着目した提案がなされている（論文 3)–9) 等）．

実際のチップの動作は，トランジスタ等の素子の特徴に加えて回路構成や実装方式による特徴が合わさるため，チップごとに適用可能なモデルは異なり，既存のモデルの適用だけで

†1 NTT データ
NTT Data Corporation
†2 横浜国立大学
Yokohama National University

⋆1 消費電力の代わりに電磁波を測定しても DPA と同様な攻撃（DPA のアナロジで DEMA と呼ばれる）が可能である．本論文では DPA を中心に検討するが，そのまま DEMA に適用できる部分は多い．

は評価結果が著しく不適切になる可能性もある．少なくとも電力モデルを恣意的に選択すると評価の正当性は失われるため合理的な選択が必要である．それには評価対象に合わせて最も有効な電力モデルや攻撃定義式を見い出して選択することが望ましい．ところが攻撃法の研究では，少ない攻撃コストで最大の成果を得ることに主眼があり，対策法の脆弱性分析のためにモデルの詳細な検討がなされても，チップごとの差異にモデルや定義式を適合させる手段の検討は不十分であった．

本論文では，DPA（改良版も含む）への耐性評価の手順化を目的として，電力モデルや攻撃定義式を適合させる問題は，測定値との相関が最大となる値（この値を本論文では “計算値” と呼ぶ）を求めるシステム同定ないしパラメータ推定問題と置き換えることが可能であることを示す．そのために計算値を求めるためのモデル式とそのパラメータ抽出について検討し，その手順を 1 つ示す．この計算値を導入することにより，既存の電力モデル等の適用では実装方式の差異により左右されて正確に求めることが難しかった DPA 耐性を安定して評価できるようになる．

以下，2 節で本論文で対象とする DPA とその改良や精緻化について説明し，それらの電力モデルと攻撃定義式は計算値に埋め込めることを示す．3 節は 4 節以降で数値例を示すために使用した暗号 LSI と測定環境を説明する．4 節で計算値により DPA が改善される単純な事例を紹介する．5 節では計算値のモデル式とその値を定める手順を示して計算値を求め，この計算値を使った評価結果を 6 節に示して最後にまとめる．

2. DPA の攻撃定義式と電力モデル

2.1 オリジナル DPA とその攻撃定義式

論文 1) で提案された DPA（オリジナル DPA と呼ぶ）は，「暗号処理中の何らかのデータの 1 bit の値に着目して，その 1/0 により消費電力等の測定値を 2 グループに分割して各々の平均を求めれば，何かしら有意な差分があり，ランダムに 2 分したときには各々の平均の差分は 0 になる」という仮説のもとで，暗号文[⋆1]と秘密鍵の一部分（以下，部分鍵とする）の候補から，着目した 1 bit の値を推測して平均差分の絶対値を求め，この値を最大にする候補を正しい部分鍵と推定する攻撃法である．DPA の前提条件は {測定値，暗号文，暗号アルゴリズム} の 3 つを得られることである．

⋆1 暗号化処理と平文の組合せや復号処理との組合せでも本質的な差異はないので，暗号化処理時の測定値と暗号文を使った場合で説明を統一する．最後のラウンド回路の動作がターゲットになる．また，暗号の例として鍵長が 128 ビットの AES-128 の場合で説明するが，AES 以外の暗号にも適用できる．

以下，AES 暗号[10)]（3 節，図 2 も参照）を例に説明する．一連の測定で求めた n 個の測定値の全体を変数 W，暗号文の全体を m で表し，その i 番目の測定値と暗号文を添え字をつけて $\mathrm{W_i}$ と $\mathrm{m_i}$ とする．最終ラウンドのラウンド鍵 128 bit を k，最終ラウンドの入力 128 bit 中の b ビット目に着目してその値を推測する選択関数 SF を，

$$\mathrm{SF}(\mathrm{m_i}, \mathrm{k}, \mathrm{b}) = \mathrm{bit}(\mathrm{SB}^{-1}(\mathrm{SR}^{-1}(\mathrm{xor}(\mathrm{m_i}, \mathrm{k}))), \mathrm{b})$$

とする．ここで SB^{-1} は SubBytes の逆変換，SR^{-1} は ShiftRow の逆変換である．SB と SR はバイト単位の処理なので b を固定すると m の 8 bit と k の 8 bit があれば SF を計算できる．この k の 8 bit が部分鍵である．SB は非線形なので k が異なる SF の出力はほぼ無相関である．SF の値で測定値 W を下記の $\mathrm{W_{SF=0}}$ と $\mathrm{W_{SF=1}}$ の 2 グループに分ける．

$$\mathrm{W_{SF=}}x = \{\mathrm{W_i} \,|\, \mathrm{SF}(\mathrm{m_i}, \mathrm{k}, \mathrm{b}) = x\}$$

すると平均差分 dW は，

$$\mathrm{dW}(\mathrm{k}, \mathrm{b}) = \mathrm{mean}(\mathrm{W_{SF=1}}) - \mathrm{mean}(\mathrm{W_{SF=0}})$$

と表せる．この dW の式が DPA の攻撃定義式である．1〜128 までの各 b について dW の絶対値が最大になる部分鍵 8 bit を探索することでラウンド鍵 128 bit を特定する．

このオリジナル DPA は，着目するビット数が 1 であり，SF の値により W を 2 分する方式であるが，論文 1) では着目するビットを複数にする，SF に重みを持たせる，W を 3 個以上に分割する，W の複数ポイントを結合する（High-Order DPA）等による改良が示唆されている．

2.2 DPA の攻撃定義式や電力モデルの改良

論文 1) の後，DPA について様々な改良が提案されている．それらは大別して，測定方法や測定値の処理方法を変えて改善を目指すものと，測定値と強い相関を示す値（計算値）を見い出すことに着眼したものの 2 つのクラスに分けられる．

前者には 2nd Order DPA [11)]，Multi-channel attack [12)]，Zero Offset 2DPA [13)] 等がある．

後者には，複数ビットに着目して，そのハミング重みと閾値との大小により W を 2 分割する “閾値型 DPA” [2)]，各ビットで作成した平均差分を加算する “加算型 DPA” [3)] がある．AES の場合，同じ SBOX の入力 8 bit は同じ部分鍵を推定するため，この 8 bit が複数ビットとして利用される．複数ビットはビットごとに直前の状態（Ref）が異なることもあり，その場合には Ref とのハミング距離を求めることが必要になる．この Ref は単一ビット（オリジナル DPA）の場合には無用のはずであるが，実装によっては Ref が必要である（“ビット遷移型 DPA” でないと攻撃が成功しない）ことが論文 6) 等で指摘されている．そのほかに W の平均差分ではなく，W とハミング距離との相関係数を利用する CPA（Correlation

Power Analysis，電力相関解析[4]）がある．

オリジナル DPA と後者の方式とを合わせて “H 型 DPA” と略称する．

2.3　実装情報を利用した電力モデルの精緻化

サイドチャネル攻撃には，DPA で使用する 3 つの情報以外に，事前測定で得たデータあるいはソースコード等の設計データといった実装に関する情報を利用するものがある．この実装情報を利用した攻撃は DPA より強力になる可能性があるので，固定の値や容易に入手できる値ならば，DPA の電力モデルに定数あるいはパラメータとして組み込むことは現実的に想定すべきことであり，このような（隠れた）パラメータが入手できた場合であっても安全であることが望ましい．

実装情報を用いた既存の電力モデルとして Toggle-Count[8]，Stochastic model[7]，Signed distance model[9] の 3 つを示す．

Toggle-Count はソースコードが入手できる条件で回路シミュレータを使って着目したビットの遷移回数をカウントする方式である．バックアノテートしたネットリストでシミュレーションを行い，SBOX の出力 0〜255 ごとに遷移回数の平均を求める．

Stochastic model は，測定値からビットごとの重みを求める方式である．パラメータとして s_0 と $\mathrm{s}_1, \ldots, \mathrm{s}_f$ があり SF の出力に重み付けを行う．計算値 H の i 番目を

$$\mathrm{H_i} = \mathrm{s}_0 + \Sigma_{\mathrm{j}=1,\ldots,f} \mathrm{s_j} * \mathrm{SF}(\mathrm{m_i}, \mathrm{k}, \mathrm{j})$$

として求める．これと同じ提案が論文 15) にもある．

Signed distance model では，CMOS ゲートの ON と OFF では充放電される負荷や電気が流れる経路が違うことから，パラメータ δ を測定値から定めてビット遷移時の重みを ON 時は 1，OFF 時は $1-\delta$，遷移しないときは 0 とする方式である．

Signed distance model はビットの動作，Stochastic model はビット間の差異，Toggle-Count は複数ビットを 1 単位にするという具合に着目しているレイヤが異なる．

2.4　“計算値” の導入による電力モデルと攻撃定義式の一元化

2.2 小節で例示した H 型 DPA の攻撃定義式と電力モデルは，CPA における W と相関を示す値（本論文でいう計算値）によって一元的に表現できることを，論文 14) で提案された複数ビットに着目した攻撃を一般化した PPA（Partitioning Power Analysis）を利用して示す．$\mathrm{W_i}$，$\mathrm{m_i}$ と対応する計算値を $\mathrm{H_i}$ とし，$\mathrm{H_i}$ の全体を変数 H で表す．

PPA ではパラメータとして $\mathrm{h}_0, \ldots, \mathrm{h}_f$ を使う．f は着目するビット数で $f+1$ が W の分割数となる．$\mathrm{h_j}$ は分割した各グループの重みである．PPA の H はハミング距離モデルで定める．着目する f 個のビットを $\mathrm{b}_1, \ldots, \mathrm{b}_f$，各ビットの直前の値を $\mathrm{Ref}_1, \ldots, \mathrm{Ref}_f$ とし，H の i 番目の値 $\mathrm{H_i}$ は，

$$\mathrm{H_i} = \Sigma_{\mathrm{j}=1,\ldots,f} \mathrm{xor}(\mathrm{SF}(\mathrm{m_i}, \mathrm{k}, \mathrm{b_j}), \mathrm{Ref_j})$$

とする（ハミング重みモデルは $\mathrm{Ref_j}$ を 0 固定に，ビット遷移型は $\mathrm{Ref_j}$ を $\mathrm{bit}(\mathrm{m_i}, \mathrm{b_j})$ に置き換えることで対応できる）．H の値で W を分割したグループの 1 つを

$$\mathrm{W_{H}}_{=x} = \{\mathrm{W_i} \,|\, \mathrm{H_i} = x\}$$

として示す．DPA の平均差分に対応する PPA の攻撃定義式は，

$$\mathrm{dW_{PPA}(k)} = \Sigma_{\mathrm{j}=0,\ldots,f} \mathrm{h_j} * \mathrm{mean}(\mathrm{W_{H=j}})$$

である．オリジナル DPA は $f=1$，$\mathrm{h}_0 = -1$，$\mathrm{h}_1 = 1$ として表せる．**表 1** に論文 14) で示されたパラメータを AES 用に変換したものを示す．なお，PPA のパラメータ表示は厳密な等価表現ではなく，各ビットの SF の値（1/0）がバランスしていること，たとえば 4 bit に着目した場合，1111 が出現する確率は 1/16 であること等を仮定している．

PPA はパラメータ $\mathrm{h}_0, \ldots, \mathrm{h}_f$ を選定することにより CPA 等を表せることを示したが，その $\mathrm{h}_0, \ldots, \mathrm{h}_f$ を H に埋め込むことによって，PPA は CPA として表すことができる．以下に簡潔に示す．$\mathrm{N_j}$ を $\mathrm{H_i} = \mathrm{j}$ となる m の個数とする．新しく H′ を，$\mathrm{H'_i} = \mathrm{h_j}/\mathrm{N_j}$，$\mathrm{j} = \mathrm{H_i}$ により形式的に定義する．H′ を用いた CPA の攻撃定義式は（μ は平均，σ は分散），

$$\begin{aligned}\mathrm{dW_{CPA}} &= \Sigma_{\mathrm{i}}(\mathrm{H'_i} - \mu\mathrm{H})(\mathrm{W_i} - \mu\mathrm{W})/(\sigma\mathrm{W}\sigma\mathrm{H})^{1/2} \\ &= (\Sigma_{\mathrm{i}}(\mathrm{H'_i W_i}) - \Sigma_{\mathrm{i}}(\mu\mathrm{W}\mu\mathrm{H}))/(\sigma\mathrm{W}\sigma\mathrm{H})^{1/2}\end{aligned}$$

ここで $\mathrm{A} = \Sigma_{\mathrm{i}}(\mu\mathrm{W}\mu\mathrm{H})$，$\mathrm{B} = (\sigma\mathrm{W}\sigma\mathrm{H})^{1/2}$ とすると，

$$\begin{aligned}\mathrm{dW_{CPA}} &= (\Sigma_{\mathrm{i}}(\mathrm{H'_i W_i}) - \mathrm{A})/\mathrm{B} \\ &= (\Sigma_{\mathrm{i}}((\mathrm{h_j}/\mathrm{N_j})\mathrm{W_i}) - \mathrm{A})/\mathrm{B}, \quad \mathrm{j} = \mathrm{H_i} \\ &= (\Sigma_{\mathrm{j}}\mathrm{h_j} * \Sigma_{\mathrm{H=j}}(\mathrm{W_i})/\mathrm{N_j} - \mathrm{A})/\mathrm{B} \\ &= (\Sigma_{\mathrm{j}}\mathrm{h_j} * \mathrm{mean}(\mathrm{W_{H=j}}) - \mathrm{A})/\mathrm{B} \\ &= (\mathrm{dW_{PPA}} - \mathrm{A})/\mathrm{B}\end{aligned}$$

となる．着目した各ビットの SF の値の分布が k によらず同じであれば項 A と項 B は定数となる[⋆1]．つまり，H の定義により CPA と PPA の攻撃結果は同じにできる．

CPA では変数 H は $\mathrm{W_i}$，$\mathrm{m_i}$ と対応する実数であればよいので，2.3 小節の実装情報も埋め込める（PPA は H の値で W を分割するため実数を対応させることはできなかった）．

⋆1 既存の電力モデルでは H は SF の 1 の個数をカウントしたものなので，SF の 1 の数が同じなら μH，σH は同じになる．k は W には影響しないので，μW，σW は変化しない．付録参照．

表 1　H 型 DPA と PPA パラメータ
Table 1　H-type DPA and it's PPA-Parameter.

	攻撃定義式	電力モデル	PPAのパラメータ
オリジナルDPA	$dW(k,b)=\mu(W_{SF=1})-\mu(W_{SF=0})$	HW	h_0〜h_1 : -1, 1
閾値型DPA	$dW_{MS}(k)=\mu(W_{H>4})-\mu(W_{H<4})$	HW	h_0〜h_8 : -1,-1,-1,-1,0,1,1,1,1
加算型DPA	$dW_{MA}(k)=\sum_b dW(k,b)$	HD	h_0〜h_8 : -1,-6,-14,-14,0,14,14,6,1
CPA	$dW_{CPA}(k)=corr(H,W)$	HD	h_0〜h_8 : -1,-6,-14,-14,0,14,14,6,1 /($\sigma W \sigma H$)

μ : 平均，σ : 分散，HW : ハミング重みモデル，HD : ハミング距離モデル

2.5　相関係数の求め方

相関係数の求め方について補足説明する．i 回目の暗号処理時に測定した測定値 W_i が時系列の l サンプルからなるとする．W_i を n 個並べた W は $n \times l$ 行列と見なせる．W の t 列目を Wt とする．また n 個の計算値 H は $n \times 1$ 行列と見なせる．W と H の相関係数 R の t 番目の要素を，

$$R_t = \mathrm{corr}(\mathrm{Wt}, \mathrm{H}), \quad t = 1, \ldots, l$$

とする．corr はピアソンの積率相関係数である．この R は時系列のベクトル（$1 \times l$ 行列）である．R をスカラ値で代表させる場合，次の 3 つが考えられる．

R1 = max(abs(R(a:b)))　　：R の a : b 間の絶対値の最大
R2 = mean(R(a:b))　　：R の a : b 間の平均
R3 = corr(H, mean(W(a:b)))　　：W の a : b 間の平均と H との相関

オリジナル DPA は平均差分のピークに着目し，R1 を採用している．ピークだけに着目するとノイズ等によって誤検出する場合があり，R2 や R3 の方がエラーレートが低いことも多い．処理時間の点では R3 が有利である．R3 は論文 16) 等で使用されている．ただし，R2 や R3 は区間 a : b を適切に定める必要がある．区間 a : b が未知の場合には，W に移動平均やローパスフィルタ等により前処理を施した後に R1 を求める，あるいは R に移動平均等の後処理をした後 R1 を求めることにより，処理時間のメリットは失われるが，エラーレートを改善できる．

3.　数値例の作成に用いた暗号 LSI

4 節以降の説明に具体的数値を付けるため，サイドチャネル攻撃の実験用に開発されて配布されている SASEBO-R 用暗号 LSI を使用した[*1]．

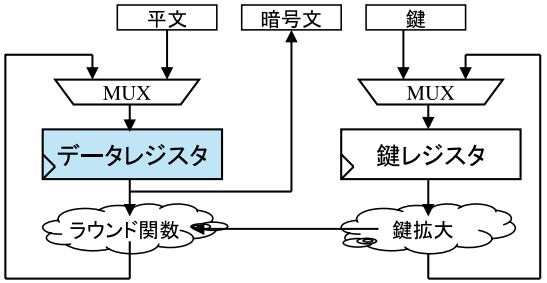

図 1　AES のデータパス概略
Fig. 1　Abstruct of AES data path.

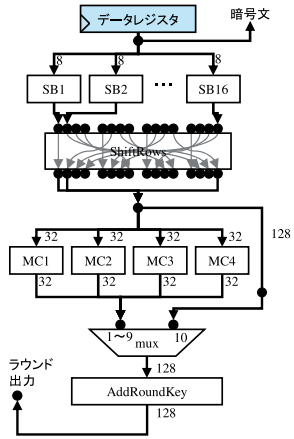

図 2　AES のラウンド回路
Fig. 2　AES round circuit.

この暗号 LSI には異なる方式で実装された複数の AES 回路が含まれている．回路の全体構成はどの実装も同じで，**図 1** に示すループアーキテクチャを採用し，1 ラウンド分の回路を規定回数繰り返し動作させることで平文を暗号文に変換する．DPA 対策等の特殊な機能はない．暗号文をデータレジスタに保持するため，暗号文を入力としてラウンド回路が 1 回余分に動作する点が特徴的である．

AES の 1 ラウンドは，SubBytes（SB），ShiftRows（SR），MixColums（MC），AddRoundKey（ARK）の 4 つのステージからなる（**図 2**）．SB はバイト単位の非線形置換（いわゆる SBOX）16 個，SR はバイト単位の転置，MC は 4 byte 単位の線形変換で，SR と MC でビットの拡散を行う．ARK はラウンド鍵との XOR である．

AES の SBOX は単純には，8 bit 入力 8 bit 出力のテーブルとして表現できるが，SBOX がラウンド回路の大部分を占め，消費電力においても大半が SBOX の動作によるものであるため，SBOX の回路規模や消費電力を小さくする構成法が提案されている．この暗号 LSI

⋆1 この暗号 LSI は TSMC 社の 130 nm CMOS プロセスで製造された集積回路で，特殊なものではない．仕様書が文献 17) で，測定データの一部が文献 18) で公開されている．

では次の 4 つの AES 回路がある（詳細は文献 17) を参照）.

AES_Comp_ENC_top（合成体）

AES_TBL（Case 文）

AES_PPRM1（1 ステージの PPRM 論理）

AES_PPRM3（3 ステージの PPRM 論理）

この 4 つを IP1，IP2，IP3，IP4 と略記する.

暗号 LSI の動作クロックは，1 ラウンド分の動作を観察しやすい値として 6 MHz にした. **図 3** は AES のラウンド回路が動作したときの波形である．測定ポイントは SASEBO-R ボードに用意された GND 側シャント用抵抗（1 Ω）の両端である．時刻 0 がクロックの立上りで 83.33 ns 付近がクロックの立下りである．ラウンド回路の動作による電圧変動の影響は 80 ns 付近で収まっている.

平文はカウンタ（CTR モード）で与え，1〜262,144（= 256 * 1,024）とした.

鍵は鍵 1〜鍵 7 までの 7 個で，鍵 i の値は i とした.

例）鍵 1 = 00000000000000000000000000000001

測定に使用した機器は，安定化電源・オシロ等の電力解析攻撃の実験によく使用される機器で，標準的性能を備えたもの（極端に高価な機材でもなく，また他の実験で使用されている機材と比較して見劣りはしないレベルのもの）を使用した．主な機器を以下に示す.

- 安定化電源　　：KIKUSUI PMC18-5A
- オシロスコープ：LeCroy WaveRunner 6050A
- パソコン　　：汎用品

電源電圧は装置パネルの表示で 3.30 V に設定し，ボードの外部電源とした．オシロのサンプリングレートは 5 GS/s，垂直軸は 10 mV/div に設定した.

以上の条件で，4 個の IP，7 個の鍵につき，各 262,144 個の波形を収集した.

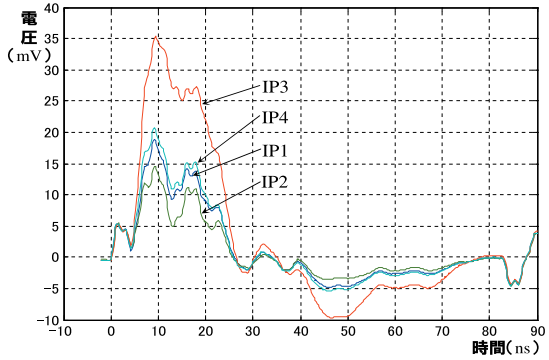

図 3　ラウンド回路動作時の電圧変動
Fig. 3　Wave of AES round.

4. 計算値の見直しによる攻撃成功確率の改善例

4.1 デバイスの特徴を利用した改善例

AES 暗号（IP2 のコード）を搭載した FPGA ボードで行ったいくつかの H 型 DPA 実験の結果を**図 4** に示す．横軸は波形数で，縦軸はラウンド鍵 16 byte 中のエラーとなったバイト数の平均である．以下，(1 – (エラー数の平均)/16) を攻撃成功確率と略記する．CPA と加算型は攻撃成功確率はほぼ同じで，閾値型はいくらか成功確率が劣る.

オリジナル DPA は，波形数が増えるにつれてエラー数は減少しているが，ビットにより差異が大きい．エラー数の少ない bit 4〜8 のみを使用して PPA を行えば成功確率が改善されることが予想できる．そこで Stochastic Model と同様なパラメータ s_j を導入して H の i 番目の値を

$$H_i = \Sigma_{j=1,\ldots,f} s_j * \mathrm{xor}(\mathrm{SF}(m_i, k, b_j), \mathrm{Ref}_j)$$

とし，s_1〜s_3 を 0，s_4〜s_8 を 1 のように bit 4〜8 に対応する s のみを 1 とした攻撃結果が図 4 の「選択型」である．CPA よりも攻撃成功確率が改善されている.

4.2 モデルの合成による改善例

ハミング重みモデルによる計算値 H1 と H1b，ハミング距離モデルによる計算値 H2 の

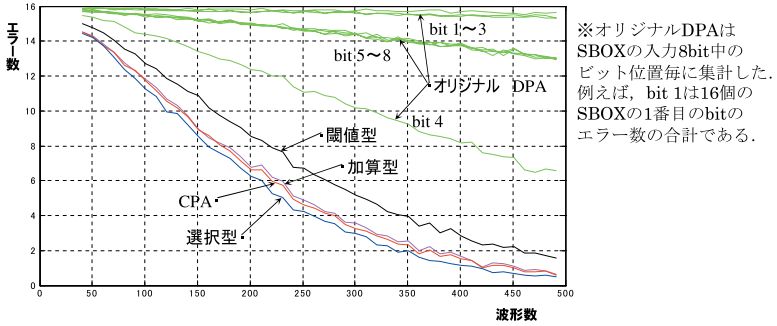

図 4　主な H 型 DPA の攻撃結果
Fig. 4　Result of H-type DPA.

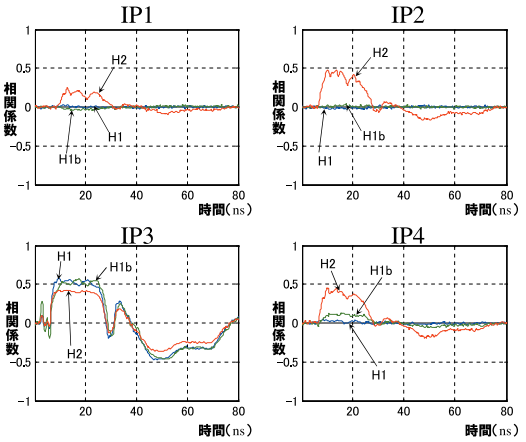

図 5　IP1〜IP4 の相関係数 R
Fig. 5　Corr R of IP1∼IP4.

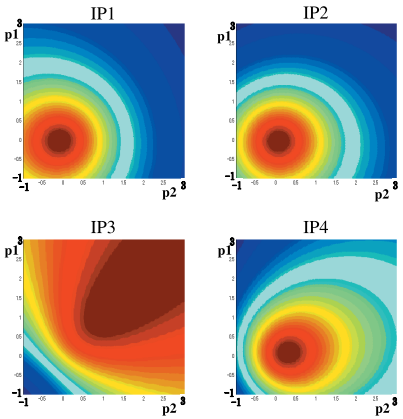

図 6　合成パラメータ探索
Fig. 6　Composite parameter.

3 つを定義する．D10 は n 個の AES の最終ラウンドの入力 128 bit（$n \times 128$ 行列）で，m は n 個の暗号文 128 bit（$n \times 128$ 行列）である．bit(m, j) は m の j 列目を取り出す．

$$H1 = \Sigma_{j=1,\ldots,128}\, bit(D10, j)$$
$$H1b = \Sigma_{j=1,\ldots,128}\, bit(m, j)$$
$$H2 = \Sigma_{j=1,\ldots,128}\, bit(xor(D10, m), j)$$

この 3 つの計算値を使って IP1〜IP4 の測定値について求めた R を**図 5** に示す．図 3 の 0〜30 ns の区間を平均して求めた R3 を**表 2** に示す．同じ ASIC であっても実装方式により相関係数の様子が異なることが分かる．特に IP3 では H1，H1b，H2 の 3 つで強い相関を示す．そこでパラメータ p1，p2 を導入した計算値 H3 を定義する．

$$H3 = H1 * p1 + H1b * p2 + H2$$

この H3 について，p1，p2 を −1〜+3 の範囲で探索して W と H3 の相関を最大とする値を求める．p1，p2 を変化させたときの R3 の様子を**図 6** に示す．R3 の最大値とそのときの p1，p2 を**表 3** に示す．特に IP3 で通常の電力モデルによる R3 よりも大きな値 R3 = 0.87 が得られた．

4.3　ビット単位の重み付けによる改善例

IP1〜IP4 の Stochastic Model によるビット単位の重みを**図 7** に示す．ただし論文 7) とは異なり，遷移 4 パターン（00，01，10，11）に分類した．横軸が bit 1〜8，縦軸が重み

表 2　電力モデルによる相関係数 R3
Table 2　Corr R3 by power model.

	H1	H1b	H2
IP1	0.00107	-0.04644	0.38411
IP2	-0.02255	0.01880	0.68977
IP3	0.54135	0.54501	0.41304
IP4	0.03432	0.14177	0.51273

表 3　合成による相関係数 R3
Table 3　Composite Corr with p1, p2.

	H3
IP1	0.38691（p1=0.00, p2=-0.13）
IP2	0.69053（p1=-0.04, p2= 0.02）
IP3	0.87298（p1= 1.32, p2= 1.33）
IP4	0.53292（p1= 0.06, p2= 0.27）

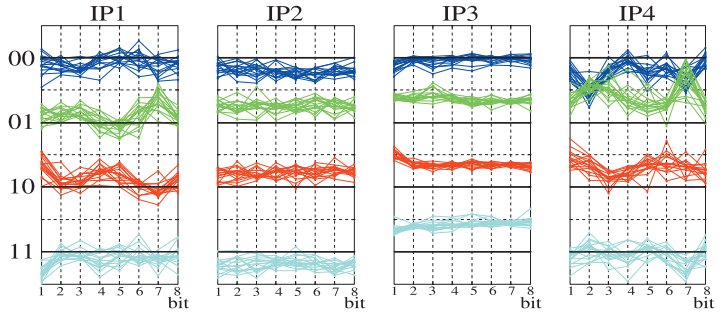

図 7　Stochastic model による bit-wise パラメータ
Fig. 7　bit-wise parameter by Stochastic model.

の値．SBOX の 16 個に対応して 16 本のグラフがある．この 16 本には共通の傾向があり，ビットごと・遷移パターンごとに異なる様子を示している．これは SBOX の実装方法の特徴を反映したものと考えられる．このビット単位の重みを用いた計算値を H4 とする．H4 で求めた相関係数 R3 は，IP1：0.43，IP2：0.70，IP3：0.90，IP4：0.60 となり，合成して求めた H3 よりもいくらか大きな値が得られた（H1〜H4 による攻撃成功確率は図 10 を参照）．

以上のように実装に合わせてパラメータを設定することで攻撃成功確率が改善できる場合があるため，相関が最大となる値の探索は適切な評価に不可欠といえる．

5.　計算値のモデル式とパラメータ推定

評価手順を確立するためには，変数 H を決定する指針が必要である．そこで 2 節で述べた既存の電力モデルや攻撃定義式，実装情報のパラメータを含めて，考えられるすべてを表現できるように変数 H を，3 つの要素：変数 D とビット参照関数 RF と重み付け関数 WF に分解した．次式を H のモデル式とする．

$H_i = \Sigma_{j=1,\ldots,g} WF(RF(D_i, j), j)$

D_i は暗号処理中の中間値を集めた変数で，その値は m_i（と鍵）で決まる．RF によって D_i から f_j bit を取り出して連結し，RF の出力に WF により重みを与える．g は D_i から取り出すビットの塊りの個数を示す．たとえば AES 暗号で SBOX の入力を単位としてビットを取り出すならば，$g = 16$，$f_1 = f_2 = \cdots = f_{16} = 8$ となる．1 bit 単位で取り出すならば $g = 128$ で $f_1 = f_2 = \cdots = f_{128} = 1$ である．レジスタの遷移を求める場合には取り出すビット数は 2 倍になる．f_j がすべて同じならば（$d = 2\hat{}f$ として），WF は単純に $d \times g$ 行列で表現できる．WF を行列に変換したものを重み行列 WM とする．

以下，D，RF，WF について順番に説明する．

5.1　変数 D（関数 RF の入力）

ビット参照関数 RF の入力となる変数 D の定義の仕方に関して，

1) ゲートに着目する・レジスタに着目する
2) 入力に着目する・出力に着目する
3) 値に着目する・遷移に着目する

という 3 つの観点が考えられる．

暗号アルゴリズムの実装は，CPU でも ASIC でも，メモリあるいはレジスタに中間状態が記憶され，レジスタ値を入力として算術論理回路等のゲートが動作する点は同じである．同期式回路ではクロックに同期してレジスタの値が更新されることによりレジスタに接続されている回路が動作し，レジスタが更新されない限り回路は動作しない．回路の動作をレジスタの遷移パターンで分類すれば，回路の動作と遷移パターンには強い相関があることが期待できる．Toggle-Count のようにゲート出力の遷移に着目するとゲートのスイッチの有無をカウントすることになり効率が良さそうに見える．またレジスタでは乱数マスクを行うと攻撃失敗するが，論理ゲートの出力に着目するとグリッチがあるため，攻撃に成功するという報告もある[8]．しかしゲートは多数に多段にあり，どのゲートの出力に着目すべきか判断に困る．ゲートの出力は，ゲートの入力の全ビットを調べれば決定できるので，レジスタで分類すればグリッチも含めてゲート動作を分類できるはずである．

レジスタの遷移はレジスタの更新前の値と更新後の値の組合せで分類でき，1 ビットに着目した場合には，00，01，10，11 の 4 パターンとなる．この 4 つに適切な重みを付ければ，ハミング重みモデル，ハミング距離モデル，Signed distance model，Stochastic Model のすべてを表現できる．

参照する中間処理値によって攻撃コストが影響を受ける点に注意が必要である．仮に秘密鍵と D_i が同じなら W_i も同じ値になる実装方式の場合，RF で D_i の全ビットを取り出し，$g = 1$，$WF(RF(D_i, 1), 1) = W_i$ と定めれば相関係数 $R = 1$ を達成できる．しかし，攻撃を行う際には RF で参照する変数 D のビットは選択関数 SF で求める必要がある．AES の場合，最終ラウンドの入力は m_i の 8 bit と k の 8 bit があれば求められる．ところが第 9 ラウンドの入力になると，SR と MC のビット拡散が入るため，m_i と k の 32 bit が必要になる．第 8 ラウンドの入力は m_i と k の 128 bit が必要となる．W と相関する H が存在したとしても，第 8 ラウンドの入力のようなビットを参照しないと H を構成できない場合には H 型 DPA による攻撃のメリットはない[⋆1]．このように参照するビットにより攻撃コスト（鍵候補を探索するための計算時間）が異なる．

AES 暗号をループアーキテクチャで実装した場合には，D は，i) 入力，ii) 鍵 K と入力によって決まる各ラウンドのデータレジスタ値，iii) 暗号文の 3 つを連結したものが候補になる．本論文では 3 節の暗号 LSI を対象として，最後のラウンド関数の動作に着目したので，4.2 小節で使用した D10 と m の 2 つを連結して D とした．

5.2　関数 RF（ビットのグループ化）

ハミング重み/ハミング距離のどちらも，ビット単位で値を定めた後，それを合計（1 の個数をカウント）するという処理を行うが，ビット単位の処理だけでは十分とはいえないため，複数ビットを 1 単位としても処理できるように RF を導入する．

ビットごとに独立して処理するならば，遷移を求めても，重みを各ビットにつき 4 個の値を用意するだけでよい．しかし，このようにビット単位に分解してしまうと見えない成分がある．**表 4** は 2 入力 AND ゲートの動作を表したものである．「無」はゲートが動作しないことを示す（説明を単純にするためにグリッチは発生しないものとする）．

この AND ゲートの動作は「無」が 10 個，「OFF」が 3 個，「ON」が 3 個の 3 種類あり，入力 2 bit を同時に見る場合にはこれらは正しく分類でき，相関係数は 1 になる．1 bit 単位で見る場合には遷移 4 パターンで分類すると（無 $= 0$，ON $= 1$，OFF $= \alpha$ として），4×2 行列 WM は，その列の要素は 2 列とも同じで，0，2，2α，$1 + \alpha$ となる．この WM を使って AND ゲートの計算値を求めると**表 5** のようになる．遷移前が $(1, 1)$ で遷移後も $(1, 1)$ の場合，AND ゲートは動作しないが，ビット単位で重み付けを行うと $2 + 2\alpha$ になる．この差はモデルが不適合であることによって発生したエラーである．元の値との相関係

⋆1 差分解読法や線形解読法等の従来の暗号解読法と組み合わせる等，サイドチャネル情報のメリットを生かせる可能性は残る．

表 4　2 入力 AND ゲートの動作
Table 4　Bevavior of AND gate.

遷移後＼遷移前	0,0	0,1	1,0	1,1
0,0	無	無	無	OFF
0,1	無	無	無	OFF
1,0	無	無	無	OFF
1,1	ON	ON	ON	無

表 5　AND ゲート動作の復元
Table 5　Recovery of AND gate.

遷移後＼遷移前	0,0	0,1	1,0	1,1
0,0	0	2α	2α	4α
0,1	2	$1+\alpha$	$2+2\alpha$	$1+3\alpha$
1,0	2	$2+2\alpha$	$1+\alpha$	$1+3\alpha$
1,1	4	$3+\alpha$	$3+\alpha$	$2+2\alpha$

数は α の値によって異なるが，仮に $\alpha = 1$ とした場合，0.63 程度である．

逆に，全ビットを 1 単位にすることは，f ビットの遷移を考えると 2 の $2f$ 乗個の状態ができ，AES であればレジスタは少なくとも 128 bit あるので現実的ではない．

以上から，RF は，D を相互干渉するビットごとに分割し，それらを 1 単位にまとめるように定める．その際，ビット間の干渉の強弱により優先順位をつけて，必要十分な範囲に D を分割する．その手順を AES を例にして示す．

AES の最終ラウンドの入力 128 bit を D10，暗号文 128 bit を m とし，各々から i bit 目を取り出して bb_i，同様に j bit 目を取り出して bb_j とする．

$$bb_i = \mathrm{bit}(D10, i) * 2 + \mathrm{bit}(m, i)$$
$$bb_j = \mathrm{bit}(D10, j) * 2 + \mathrm{bit}(m, j)$$

bb_i と bb_j の組合せで測定値を分類して各々の平均を求めると，bb_i と bb_j が相互に干渉していなければ，$(bb_i, bb_j) = (00, 00)$，$(00, 01)$，$(00, 10)$，$(00, 11)$ の 4 個の値と $(bb_i, bb_j) = (**, 00)$，$(**, 01)$，$(**, 10)$，$(**, 11)$ の差は一定になる（**には 01，10，11 が入る）．bb_i と bb_j を入れ替えた場合も同様である．そこでこれらの分散の合計を求め，bb_i と bb_j の間の干渉度合いの評価値とする．

このようにして AES の測定値で求めたビット間の干渉を分析した結果が**図 8** である．縦軸が i，横軸が j で，色で強弱（赤 = 大，青 = 小）を示す．どの IP でも SBOX の入力，たとえば，bb_1〜bb_8 の 8 個間で相互に分散が大きく，干渉があることが分かる．つまり，SBOX の入力となる 8 bit を 1 グループとして扱えばよい．8 bit 程度ならば 1 グループにしても十分取り扱える．

5.3　関数 WF（重み付け）

重み付け関数 WF あるいは重み行列 WM は実装情報を使って求める．

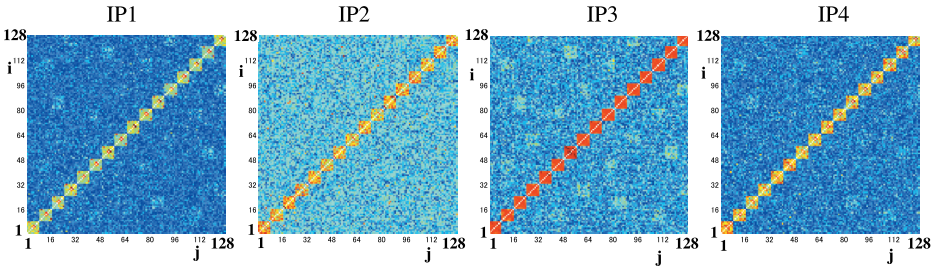

図 8　ビット独立性の分析結果
Fig. 8　Result of bit-dependance analysis.

実装情報として測定値を用いて WM を決める手順について以下に示す．まず，説明用に H のモデル式を変形する．i 行 $RF(D_i, j) + 1$ 列目の要素を 1，他は 0 とする $n \times d$ 行列を Xj とする（n は測定値の個数）．WM の j 列目を WMj とする．すると H のモデル式は（行列の積を ‘ · ’ で明示する，なお下記の式では n 個の値を同時に処理しているので添え字 i がない），

$$H = \Sigma_{j=1,\ldots,g} Xj \cdot WMj$$

となる．つまり，Xj と W が所与の値で，WMj を探索して H と W との相関係数を最大にすればよい（$H' = -H$ とすれば相関係数の符号を反転できるので $+1$ をゴールにできる）．

この種の最適化問題には多くの先行研究があり，近似解を得るための一般的な解法が様々に提案されている．

その例として最も単純な手順である山登り法を簡単に示す[*1]．まず，適当な小さな値 Δ を決める．WMj の初期値を乱数とする（初期値は乱数ではなく，H1〜H4 の値を設定することもできる）．WMj の近傍を WMj の 1 つの要素に Δ を加算したものと Δ を減算したものとして，H を求めて W との相関係数を求め，元の値よりも大きな場合には WMj の要素を更新する．これを各要素について繰り返し適用し，更新されなくなったところで停止する．相関係数の定義から最大値は 1 なので，この手順は必ず停止する．局所最適を回避するために初期値を選び直して複数回試す．

なお，AES の場合，1，5，9，13 番目の SBOX は，最終ラウンド仕様上，各々の入力 8 bit と部分鍵 8 bit が決まると遷移後の値も決まり，遷移パターンの全組合せは発生しない．

⋆1 暗号文の特定部分だけが変化するように平文を選択することにより，WM の値を 1 つずつを測定することも有力と考えられる．

表 6　計算値 H とパラメータ
Table 6　H and it's parameter.

計算値 H	計算値 H のパラメータ		
H1：ハミング重みモデル	g=128, f=1	WM=[0, 1]	RF=bit(D10,j)
H2：ハミング距離モデル	g=128, f=2	WM=[0, 1, 1, 0]	RF=bit(D10,j)+2*bit(m,j)
H3：表3のパラメータ合成	g=128, f=2	WM=[0,1+p2,1+p1,p1+p2]	RF=bit(D10,j)+2*bit(m,j)
H4：bit単位の重み行列	g=128, f=2	WM={4×128行列}	RF=bit(D10,j)+2*bit(m,j)
H5：8 bit単位の重み行列	g=16, f=16	WM={65536×16行列}	RF=$\sum_{i=0..7}$bit(D10,j*8-i)*2^i +256*$\sum_{i=0..7}$bit(m,j*8-i)*2^i

H1のWMは，モデル式からは2行128列であるが，各列の値が等しいので圧縮して要素数2個の配列にできる．H2とH3も同様．

WM1，WM5，WM9，WM13 を定めるには鍵の値を変えて 256 個以上の鍵で測定値を集めることが必要になる．ただし，AES の 16 個ある SBOX の仕様はすべて同じなので，その回路もほぼ同じと仮定できる（図 7 参照）．そこで WM1 = WM2 = ··· = WM16 と見なすならば，H のモデル式は，X = Σ_jXj として，

$$H = X \cdot WMj$$

となる．W と H の相関係数は W = H で最大値 1 となることから，W と H の残差二乗和が最小となるように WMj を定めるならば，擬似逆行列 pinv() を使って，

$$WMj = \mathrm{pinv}(X) \cdot W$$

として線形最小二乗法で WMj を求めることもできる．

6 節の実験用に各々の IP につき鍵 1 の測定値を使って，WM1 = WM2 = ··· = WM16 と仮定して山登り法により WMj を求めた．この行列を使った計算値を H5 とし，相関係数を求めると，IP1：0.85863，IP2：0.83236，IP3：0.98756，IP4：0.86852 が得られた．

5.4　変数 H のまとめ

ここまでに登場した AES 暗号の場合の 5 つの H を**表 6** にまとめる．変数 D は数式を煩雑にしないために D ではなく，D10 と m を直に参照している．

H 型 DPA に対する安全性条件を整理すると，第 1 にあらゆる H を持ってしても正しい部分鍵による相関係数が間違った部分鍵による相関係数と識別できないこと，第 2 に測定値と相関する H が存在するとしてもその値を使って行う鍵探索に計算量的なメリットがないことである[⋆1]．

H1〜H5 の攻撃成功確率については 6 節で示すので，以下，鍵探索計算量について説明する．RF で参照するビットは D10 と m の計 256 bit があるが，CPA で 1 つの部分鍵の探索に必要なのは D10 の 8 bit と m の 8 bit である．そのうち，D10 の 8 bit を SF で求めればよい．m は既知の値なので SF 不要である．これに必要な部分鍵のサイズは 8 bit である．これを 16 回行う．したがって鍵探索計算量はどの計算値を用いても 256 × 16 = 4096 である．

6.　計算値を用いた攻撃成功確率の確認結果

6.1　従来の CPA 結果

従来の電力モデルによる H 型 DPA として，H2 による CPA 結果のグラフを**図 9** に示す．横軸は波形数 N，縦軸はラウンド鍵 16 byte 中のエラー数である．N 個の波形は測定波形全体からランダムに選択した．相関係数は図 5 の 10〜20 ns の間を平均して求めた R2 を使用した．

波形数が同じであっても測定誤差や暗号文の偏り等によりエラー数はばらつくため，グラフには個々の結果をプロットするとともにその平均値も示してある．IP1 の場合，波形数が 3,000 個だとエラー数は 1〜8 の範囲でばらつく．その平均（約 5）を黒線で示してある．表 2 の H2 の相関係数の値と比較すると，相関係数が大きいほどエラー数が少ないという関係になっている．

グラフから，平均エラー数が 1 を下回る波形数を読み取ると，IP1：約 5,500 個，IP2：約 700 個，IP3：約 2,000 個，IP4：約 1,700 個である．このように，この暗号 LSI の AES 実装はいずれもサイドチャネル攻撃対策を何ら施していないにもかかわらず，波形数で見ると IP1 と IP2 で 7〜8 倍もの差がある．

6.2　変数 H を使った CPA 結果

5 節の手順により求めた重み行列の効果を確認する．**図 10** のグラフは N 波形をランダムに選択した CPA 結果で，横軸は波形数 N，縦軸はエラー数の平均である．相関係数は R3 により求めた．波形データを平均化した区間は図 3 の 0〜30 ns の間である．

1 枚のグラフには，鍵 1〜鍵 7 の 7 本のグラフをプロットした．H5 で重み行列の作成に用いた鍵 1 のグラフを除いて，鍵の値に関係なくほぼ同じグラフになっている（そのため凡例表示は略した）．H による差異と IP による差異を比較するために各列に IP1〜IP4，各行に H1〜H5 を並べてある．

⋆1 第 1 の条件を満足させるには，WF，RF，D の全組合せからなる集合 G に対して，部分鍵が特定できる要素の不存在証明を与えることが考えられる．たとえば，任意の鍵での測定値について部分鍵を特定できる G の部分集合の条件を導出し，それが空集合になることを確認することで形式的証明を与えることである．しかし，集合 G のサイズは巨大なので効率的な探索アルゴリズムが必要である．

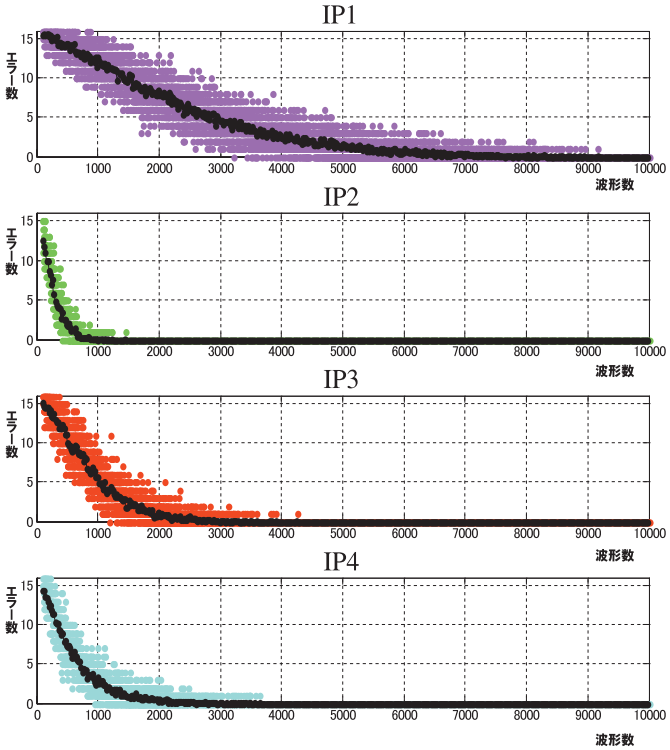

図 9　従来の電力モデルによる H2 で求めた CPA 結果
Fig. 9　CPA results by H2.

既存の電力モデルによる計算値 H1 と H2 の結果は，実装方式による違いが大きく現れている．H1 では IP3 のみが攻撃可能で他は攻撃不可と攻撃の可否自体が違う．H2 ではすべての IP が攻撃可能であるが，その攻撃コスト（波形数）は IP によって数倍の違いがある．H3 や H4 のように測定値を使ってパラメータを調整すると特に IP3 で大きな改善があるが，実装方式による違いは依然として大きい．これらに比べて，ビット間の干渉までを考慮して求めた H5 では，実装方式による攻撃コストの違いが顕著に小さくなっている．特に IP1 は，H2 から H4 までほとんど違いが見えないが，H5 では改善されている．

テーブル参照という最も単純な実装方式である IP2 と他 IP とを比較すると，IP2 の攻撃

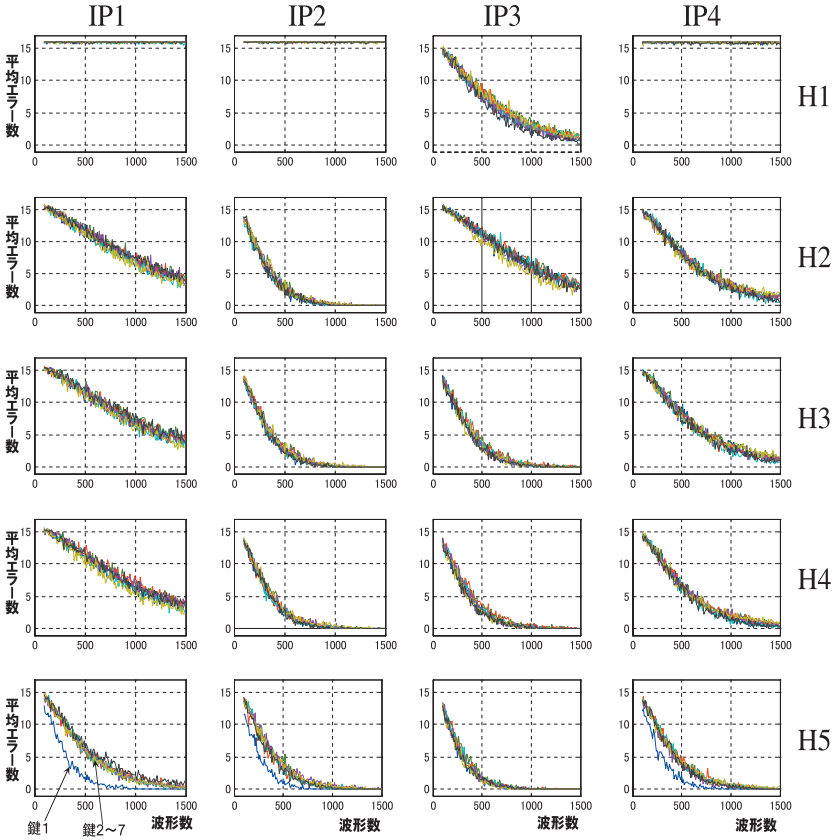

図 10　計算値 H ごとの CPA 結果
Fig. 10　results of CPA by each H.

コストは H2〜H5 のどれでもほとんど同じで，H2 から H5 になるにつれて IP2 以外の攻撃コストが IP2 の攻撃コストに近づいていることが読み取れる．特に H5 では重み行列を作成した鍵 1 において IP1〜IP4 のエラー数がほぼ一致している．IP2 にエラー数が近づく順番は，H3 で IP3 が IP2 と同レベルになり，H4 で IP4 がいくらか改善され，H5 で IP4 と IP1 が近づく．この順番は実装方式と符合している．IP3 は AND-XOR の 1 ステージという極端だが単調な実装方式である．IP3 に最適な電力モデルはハミング重みともハミング距

離とも異なるため，H1 や H2 では攻撃コストが大きいが，ビット間の干渉は AND ゲート 1 段分のみである．一方，IP1 や IP4 は IP3 と比べてロジック段数が深い複雑な実装であり，ビット間の干渉もその分だけ大きいと推測される．

6.3 考　　察

図 9 と図 10 の結果から，H1 や H2 で IP により差異が大きいのは実装方式により DPA 耐性が異なり，それが反映されているというよりも，既存の電力モデルによる CPA では安全性の比較が難しい（評価結果が真の値を示さない）ことを意味し，安全性評価には H5 のような計算値を求めることが必要であると考えられる．試験手順や合否の判定基準を定めると，単に電力モデルを複雑にしただけの実装が出現することが予想される．その場合，既存の電力モデルによる評価では（実際には安全ではないのに）「合格」させてしまう可能性がある．測定値から重み行列を決めて評価すればそのような対策の擬似的な影響を除去して正しく評価できる可能性がある．

なお，図 9 の H2 による CPA 結果と図 10 の H2 の CPA 結果の違いは，相関係数の定義の違いである．図 9 は相関係数 R の 10〜20 ns を平均した R2，図 10 では波形データの 0〜30 ns を平均して求めた値と計算値 H との相関係数 R3 を用いている．このように相関係数を求める際の測定値の処理の仕方によっても DPA 結果に影響がある．そのため H 型 DPA だけではなく，測定値の処理方法に着目した DPA のクラス（W 型 DPA）についても検討が必要である．

7. おわりに

暗号モジュールの電力差分解析に対する耐性について，適切な評価結果を得るには電力モデルや攻撃定義式を評価対象へ適合させることが必要である．この問題は測定値との相関係数を尺度とするパラメータ推定に帰着できることを示した．そして，測定値との相関を最大にする計算値のモデル式を示し，電力差分解析の対策を特に施していない 4 種類のブロック暗号 AES を実装した LSI を測定して，具体的にパラメータを定めた．このパラメータで求めた計算値を使って攻撃成功確率を求めると，従来の電力モデルや攻撃定義式では実装方式の差異により成功確率は大きく影響を受けるが，本論文で整理した手順により求めた計算値では実装方式によらず安定した結果が得られた．すなわち，従来の電力モデルベースの評価で得られる攻撃コストにはモデルを最適化すると消えてしまう擬似的なものが含まれていて，適切な評価結果を得るには評価対象に合わせた電力モデル等が必要であることを実証できた．

本論文では ASIC 実装の暗号 LSI による実験結果を示したが，FPGA や CPU と ASIC では各々消費電力特性の違いから適用可能な電力モデル（ないしモデルのパラメータ）は異なることが分かっている[6]．図 4 に示すように FPGA 搭載 AES では着目したビットにより DPA の攻撃成功確率が異なるのも FPGA 固有の特徴（4 ビット LUT による実装）である．同様に CPU 実装でも論文 15) のように実装情報が存在する．この場合でも本論文に示す手順を用いれば，ハミング重みモデルとハミング距離モデルも包含する重み行列の働きにより実装情報を取り込むことができ，実装に適合した結果が得られると考えられる．

この手順で評価できる耐性は，安全性の必要条件の 1 つであり十分条件とまではいえないが，このように実装形態が異なる暗号モジュールであっても同じ手順が適用できることは暗号モジュールの試験手順として望ましいことである．

今後も DPA は改良されて強力になっていく可能性があるので，電力モデルに実装情報を取り込んで DPA 耐性評価を行うことが評価結果の信頼性担保に有益であると考える．実装に最も適合する電力モデルを探索しても有効な値が得られない場合には（今後の電力モデルの精緻化によって得られる改善も含めて）DPA に対して “ある種” の耐性を有することの証拠になるからである．

謝辞　SASEBO は経済産業省の委託事業の中で，産業技術総合研究所と東北大学が開発したサイドチャネル攻撃標準評価ボードである．本ボードの開発に関わるすべての関係者に感謝する．

参　考　文　献

1) Kocher, P., Jaffe, J. and Jun, B.: Differential Power Analysis, *CRYPTO'99*, LNCS 1666, pp.388–397 (1999/08).
2) Messerges, T.S., Dabbish, E.A. and Sloan, R.H.: Investigations of Power Analysis Attacks on Smartcards, *USENIX 1999* (1999).
3) Bevan, R. and Knudsen, E.: Ways to Enhance Differential Power Analysis, *ICISC 2002*, LNCS 2587, pp.327–342 (2003).
4) Brier, E., Clavier, C. and Olivier, F.: Correlation Power Analysis with a Leakage Model, *CHES 2004*, LNCS 3156, pp.135–152 (2004).
5) Lemke, K., Schramm, K. and Paar, C.: DPA on n-Bit Sized Boolean and Arithmetic Operations and Its Application to IDEA, RC6 and the HMAC-Construction, *CHES 2004*, LNCS 3156, pp.205–219 (2004).
6) 高橋芳夫，佐藤　証，梅田伸明：ブロック暗号の FPGA 実装に対するサイドチャネル攻撃，信学技報，Vol.105, No.484, ISEC2005-111, pp.5–10 (2005/12).
7) Schindler, W., Lemke, K. and Paar, C.: A Stochastic Model for Differential Side Channel Cryptanalysis, *CHES 2005*, LNCS 3659, pp.30–46 (2005/08).

8) Mangard, S., Pramstaller, N. and Oswald, E.: Successfully Attacking Masked AES Hardware Implementation, *CHES 2005*, LNCS 3659, pp.157–171 (2005/08).
9) Peeters, E., Standaert, F.-X. and Quisquater, J.-J.: Power and electromagnetic analysis: Improved model, consequences and comparisons, Integration, *VLSI Journal*, Vol.40, Issue 1, pp.52–60 (2007).
10) National Institute of Standards and Technology: Specification for the Advanced Encryption Standard (AES), FIPS Pub197 (2001).
11) Messerges, T.S.: Using second-order power analysis to attack DPA resistant software, *CHES 2000*, LNCS 1965, pp.238–251 (2000/08).
12) Agrawal, D., Rao, J.R. and Rohatgi, P.: Multi-channel Attacks, *CHES 2003*, LNCS 2779, pp.2–16 (2003).
13) Waddle, J. and Wagner, D.: Towards Efficient Second-Order Power Aanalysis, *CHES 2004*, LNCS 3156, pp.1–15 (2004).
14) Le, T.-H., Clediere, J., Canovas, C., Robisson, B., Serviere, C. and Lacoume, J.-L.: A proposition for Correlation Power Analysis enhancement, *CHES 2006*, LNCS 4249, pp.174–186 (2006/10).
15) 高橋芳夫，福永利徳，大塚浩昭，神田雅透：CPU ボード上のブロック暗号に対するサイドチャネル攻撃，信学技報，Vol.104, No.731, ISEC2004-114, pp.49–54 (2005/03).
16) Akkar, M.-L., Bevan, R., Dischamp, P. and Moyart, D.: Power Analysis, What Is Now Possible..., *ASIACRYPT 2000*, LNCS 1976, pp.489–502 (2000).
17)（独）産業技術総合研究所情報セキュリティ研究センター：サイドチャネル攻撃評価用 ISO/IEC 標準暗号 LSI 仕様書，第 1 版 (2008/04).
18) 暗号モジュールのサイドチャネル攻撃実験データ交換用標準フォーマット（WXF）. http://ipsr.ynu.ac.jp/wxf/index.html (参照日 2009/04/01)

付　　録

σW と σH の影響について

論文 14) では σW と σH の影響について，「σH は k を変えてもあまり変化しない．σW は波形の注目したい部分では値が大きくなり関係ない部分では値が小さくなる．つまり σW で割るとノイズが増加すると指摘し，σW を補正すると特に波形数が少ない場合の成功確率が向上する」として，その実験結果を示している．

たしかに m の分布が完全に均一な場合には，k によらずに σH は定数になる．ランダムに選択した場合でも個数が増加すれば m の偏りは均一化される．ただし，m の個数が少ない場合にはある程度の偏りが存在する．1,000 個程度の場合で計算機実験で確認すると，σH は k により ±10%程度上下した．

この σH の変動は真の鍵の確率分布と独立したものなので，σH で除算することにより dW にランダムなノイズが入ることになる．また m の個数が少ないときには，m 自体のバラツキや測定値の誤差等により攻撃成功確率の分散は大きくなる．そのため，本論文の実験では，測定データ全体の中からランダムに N 個を選択して相関係数を求めることを複数行う．これにより σH と μH の影響を平均化する．

σW と μW については特定区間の平均電圧として扱えば，定数となるので波形を特定区間の平均値で扱うことにする．

(平成 21 年 5 月 21 日受付)
(平成 22 年 3 月 5 日採録)

高橋　芳夫

1990 年株式会社 NTT データ入社．2006 年横浜国立大学大学院環境情報学府博士課程後期入学，現在に至る．暗号実装，サイドチャネル攻撃の研究に従事．CRYPTREC 暗号実装委員会委員．電子情報通信学会会員．

松本　　勉（正会員）

1986 年 3 月東京大学大学院工学系研究科電子工学専攻博士課程修了，工学博士．同年 4 月横浜国立大学講師．2001 年 4 月同大学院環境情報研究院教授，現在に至る．日本学術会議連携会員，国際暗号学会 IACR 理事．暗号アルゴリズム・プロトコル，耐タンパー技術，生体認証，人工物メトリクス等の「情報・物理セキュリティ」の研究教育に 1981 年より従事．1982 年にオープンな学術的暗号研究を目指した「明るい暗号研究会」を 4 名で創設．IACR 主催国際会議 ASIACRYPT 2000，CHES 2006 実行委員長を務めた．1994 年第 32 回電子情報通信学会業績賞，2006 年第 5 回ドコモ・モバイル・サイエンス賞等を受賞．