社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2004－ＣＳＥＣ－26　(45)
2004／7／21

DPAのリークモデル構築と論理シミュレーションによる評価

佐伯 稔† 鈴木 大輔† 市川 哲也‡

† 三菱電機(株) 情報技術総合研究所 〒247-8501 神奈川県鎌倉市大船 5-1-1
‡ 三菱電機エンジニアリング(株) 鎌倉事業所 〒247-8501 神奈川県鎌倉市大船 5-1-1
E-mail: † {rebecca,dice}@iss.isl.melco.co.jp, ‡ ichikawa@iss.isl.melco.co.jp

あらまし 電力差分解析(Differential Power Analysis, DPA)は，データに依存した微小な電力変化に基づいて暗号デバイス内部の秘密情報を解析する技術である．本論文では，特にCMOSデバイスに着目して，DPAによって秘密情報の解析を可能とするような情報(=リーク)が発生する原因を考察し，リークモデルを構築する．さらに，設計の上流段階で効率良くリークの有無を評価するための論理シミュレーションによるDPA評価手法を提案する．

キーワード DPA, CMOS, 遷移確率, 論理シミュレーション

Construction of DPA Leakage Model and Evaluation by Logic Simulation

Minoru SAEKI† Daisuke SUZUKI† and Tetsuya ICHIKAWA‡

† Mitsubishi Electric Corporation, Information Technology R&D Center,
5-1-1 Ofuna Kamakura, Kanagawa, 247-8501, Japan
‡ Mitsubishi Electric Engineering Company Limited, Kamakura Office,
5-1-1 Ofuna Kamakura, Kanagawa, 247-8501, Japan
E-mail: † {rebecca, dice}@iss.isl.melco.co.jp, ‡ ichikawa@kam.mee.co.jp

Abstract Differential Power Analysis(DPA) is a techinique that analyzes the secret information in the code device based on minute electric power change according to data. In this paper, we consider about the cause where the information that enables analysis of secret information by DPA occurs, especially in CMOS device, and construct DPA leakage model. Moreover, we propose the DPA evaluation technique using logic simulation, which efficiently evaluates the presence of DPA leakage at the upstream stage of design.

Keyword DPA, CMOS, Transition Probability, Logic Simulation

1. はじめに

電力差分解析(以下DPA)はKocherらによって提案された暗号デバイスに対するサイドチャネル解析の一つであり，大量の消費電力情報を統計処理することで、秘密情報に関らない回路部分の影響や測定系のノイズ成分を除去し、重要情報のみを抽出し得る強力な攻撃法である[1],[2]．従来，暗号デバイスの設計者は“秘密情報に依存したごくわずかな電力変化”には特に注意を払っておらず，ここを突いたDPAは脅威とも言える．従って，DPAに対して早急に対策を確立することが望まれている．

DPA耐性を持った暗号デバイスを開発する際，ただ闇雲に試作と評価の試行錯誤を繰り返すのは現実的でないし，まず不可能であろう．また，効果のある対策であっても，速度や回路規模及び消費電力などの面でのオーバヘッドが小さいものの方が良いことは言うまでもない．こうしたことから，経験的／発見的な手法に頼るのではなく，まずDPAによって秘密情報の解析を可能とするような情報(電力差分波形上のスパイクとして現れる有意な電力差分；以下，本論文では単に“リーク”と呼ぶ)の発生源と発生メカニズムを明らかにし，その上で効率的な対策を施すべきであると考える．このためには，設計のより上流段階で効率的にDPA評価を行うことが重要となる．

本論文では，主に現在広く用いられているデバイスの一つであるCMOSについて，リークの基本的な発生メカニズムを検討し，その妥当性をモデル回路を用いた実験結果によって実証する．さらに，精度と効率を両立した，論理シミュレーションによるDPA評価手法を提案し，提案手法が論理設計の段階でリークの有無を判定するために有効であることを示す．

なお，本論文中の実機実験は全て，三菱電機が開発

したサイドチャネルアタック評価用プラットフォーム(SCAPE: Side Channel Attack Platform for Evaluation)[5]を用いて行い，対象回路は本ボードに搭載した Xilinx Inc.の FPGA(Virtex1000)に実装，評価した．

2. リークの発生メカニズム

リークは，配置配線などに依存してたまたま発生するものであろうか，それとも必然的なものなのだろうか？また，CMOS 回路の消費電力は，信号レベルではなく，信号変化に依存するにも関わらず，DPA において選択関数が 0 か 1 かという信号レベルに基づくグループ分けでリークが発生するのは，どのような理由によるものであろうか？本章では，これらの疑問を解明するために，まず DPA に関して本質的な消費電力の見積り方法を CMOS 回路について検討する．次にその見積り方法に基づいて，CMOS 回路のリーク発生メカニズムを，信号の伝搬遅延の無い理想的なデバイスの場合，遅延のある現実のデバイスの場合，の順に考察し，リークモデルを構築することを試みる．

2.1. CMOS 回路の消費電力見積り

本節では，CMOS 回路における，リークに関して本質的な消費電力を見積る方法について検討する．

CMOS の消費電力は，次の 3 つの要素に分けられる．

1)負荷容量を充放電するための電力(*P1*)

2)遷移時の瞬間的な貫通電流による電力(*P2*)

3)漏れ電流による電力(*P3*)

1)の電力は，$P1=\Sigma_i\ (f_i \times C_i \times V^2)$ *(i は全ての信号)* で表される．ここで，f_i は当該信号(i)の単位時間当たりの遷移回数，C_i は負荷容量すなわち接続先の入力容量と配線容量の和，V は電圧である．2)の電力も論理ゲート毎に f_i にほぼ比例する．3)は従来ほとんど無視できる消費電力と見なされることが多かったが，プロセスの微細化が進むにつれて総消費電力に占める比率は大きくなりつつある．しかし，3)のようなスタティックな消費電力は差分をとる際に打ち消しあうため，DPA について考察する上ではやはり無視してよい．

従って，CMOS 回路のリークに関わる本質的な消費電力を見積るためには，上記 1),2)の消費電力を見積ればよいことになる．論理ゲート毎に見るとこれらはともに f_i に比例するので，$P1+P2=\Sigma_i\ (f_i \times k_i)$ とまとめることができる．ここで，k_i の値は，デバイスや配置配線に依存して大きく変わり得る．リークの本質を考察するためには，信号の負荷容量や遷移時間，トランジスタの ON 抵抗などが全て同じであると理想化して考え，全ての k_i が 1 となるように正規化した，

$$P_{DPA}=\Sigma_i f_i \quad (i \text{ は全ての信号}) \qquad (1)$$

を用いるとデバイスや配置配線に依存しない評価ができ，都合が良い．P_{DPA} は，単位時間当たりの信号の遷移回数の総和となる．実際の回路において，上記 k_i が 1 と見なせない場合，当該信号に起因するリークの大きさが式(1)に基づく予測値からずれるが，リークの本質の考察や，設計の上流段階でリークの有無を判定する目的においては支障無い．

以下の議論では，リークを考察する上で，CMOS 回路の(等価的な)消費電力として P_{DPA} を用いる．

2.2. リークモデル

本節では，まず信号の伝搬遅延の無い理想的なデバイスを想定し，そこで発生する基本的なリークのメカニズムを考察する．また，信号の伝搬遅延は存在するが，その影響が小さいモデル回路を用いた実機の実験結果を用い，考察の妥当性を実証する．その後，信号の伝搬遅延の影響(以下，"過渡遷移によるリークの増幅"と呼ぶ)を考慮し，リークモデルの定式化を試みる．

なお，本節中の記号の定義は以下の通りである．

$P_{a=x}$：信号 a が x である確率

$P_{a=x\to y}$：信号 a が x から y へ遷移する確率

$P_{Tr}(a)$：信号 a の遷移確率(= $P_{a=0\to 1}+P_{a=1\to 0}$)

$P_{Tr}(a)_{s=x}$：信号 s が x である時の信号 a の遷移確率

TC：(単位時間当たりの)総遷移回数の期待値

$TC_{s=x}$：信号 s が x である時の(単位時間当たりの)総遷移回数の期待値

L_0：(単位時間当たりの)総遷移回数の期待値の差(信号の伝搬遅延が無い場合)

L_1：(単位時間当たりの)総遷移回数の期待値の差(信号の伝搬遅延の影響がある場合)

2.2.1. 基本的なリーク

暗号デバイスの S-Box を論理ゲートで実装すると，非線形の関数を実現するための論理ゲート(ex.AND)と，線形の関数を実現するための論理ゲート(ex.XOR)で構成できる．例として，図 1 の回路について，信号の伝搬遅延の無い理想的なデバイスを想定し，以下の条件で遷移確率の差を計算することを考える．

条件 1:入力信号 d0,d1,d2,d3 は全て同時に到達する

条件 2:d0 を d1,d2,d3 と独立な DPA の選択関数とする

条件 3:d1,d2,d3 は互いに独立なランダムデータとする

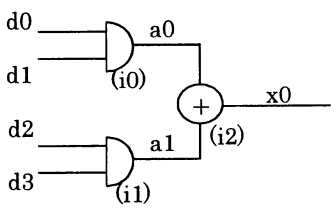


図 1　サンプル回路 1

この時，AND ゲートの出力 a0,a1 と XOR ゲートの出力 x0 の確率分布は，d0 によって以下の場合分け(状態

分け)ができる．

［状態 1：d0 の予測値の正誤がそれぞれ 1/2 の時］

a0：$P_{a0=1} = 1/4$，$P_{a0=0} = 3/4$

a1：$P_{a1=1} = 1/4$，$P_{a1=0} = 3/4$

x0：$P_{x0=1} = P_{a0=1} \times P_{a1=0} + P_{a0=0} \times P_{a1=1} = 3/8$

$P_{x0=0} = P_{a0=1} \times P_{a1=1} + P_{a0=0} \times P_{a1=0} = 5/8$

［状態 2：d0=1 の予測が正しい時］

a0：$P_{a0=1} = 1/2$，$P_{a0=0} = 1/2$

a1：$P_{a1=1} = 1/4$，$P_{a1=0} = 3/4$

x0：$P_{x0=1} = P_{a0=1} \times P_{a1=0} + P_{a0=0} \times P_{a1=1} = 1/2$

$P_{x0=0} = P_{a0=1} \times P_{a1=1} + P_{a0=0} \times P_{a1=0} = 1/2$

［状態 3：d0=0 の予測が正しい時］

a0：$P_{a0=1} = 0$，$P_{a0=0} = 1$

a1：$P_{a1=1} = 1/4$，$P_{a1=0} = 3/4$

x0：$P_{x0=1} = P_{a0=1} \times P_{a1=0} + P_{a0=0} \times P_{a1=1} = 1/4$

$P_{x0=0} = P_{a0=1} \times P_{a1=1} + P_{a0=0} \times P_{a1=0} = 3/4$

［状態 1］から［状態 2］に遷移する際の，a0 の遷移確率は，

$P_{a0=0\to1} + P_{a0=1\to0} = (3/4 \times 1/2) + (1/4 \times 1/2) = 1/2$

となる．［状態 1］から［状態 3］に遷移する際は，

$P_{a0=0\to1} + P_{a0=1\to0} = (3/4 \times 0) + (1/4 \times 1) = 1/4$

である．従って，d0 を DPA の選択関数とした時，その予測が正しければ，AND ゲート(i0)の遷移確率の差は 1/2 - 1/4 = 1/4 になる．同様にして，AND ゲート(i1)では 0，XOR ゲート(x0)では 1/16 となる．

以上のように，d0 を DPA の選択関数とした場合，図 1 の回路全体での総遷移回数の期待値の差は 1/4 + 0 + 1/16= 5/16 となる．この差がリークとして観測されるものと考える．

次に，上記の考え方の妥当性を考察する．図 1 の 2 入力 AND ゲート(i0)の計算と同じようにして，N 入力 AND ゲート(出力=a)における入力の 1 ビット(s)を選択関数とした時の遷移確率の差を計算すると，

［状態 1：s の予測値の正誤がそれぞれ 1/2 の時］

$P_{a=1} = 1/2^N$，$P_{a=0} = 1 - 1/2^N$

［状態 2：s=1 の予測が正しい時］

$P_{a=1} = 1/2^{N-1}$，$P_{a=0} = 1 - 1/2^{N-1}$

［状態 3：s=0 の予測が正しい時］

$P_{a=1} = 0$，$P_{a=0} = 1$

よって，s=1 の予測が正しい時の a の遷移確率は，

$$P_{Tr}(a)_{s=1} = (1 - 1/2^N)(1/2^{N-1}) + (1/2^N)(1 - 1/2^{N-1})$$

s=0 の予測が正しい時の a の遷移確率は，

$$P_{Tr}(a)_{s=0} = (1 - 1/2^N) \times 0 + (1/2^N) \times 1$$

であり，遷移確率の差は次式で表される．

$$P_{Tr}(a)_{s=1} - P_{Tr}(a)_{s=0} = (2^{N-1} - 1)/2^{2N-2} \qquad (2)$$

式(2)は AND の入力数(次数)N と遷移確率の関係を表すものであるが，N=2,3,4 を代入すると，

N=2：1/4　　N=3：3/16　　N=4：7/64

が得られる．以上の考え方が正しいとすると，N=2,3,4 の各 AND から大きさの比が 16:12:7 であるようなリークが観測されるはずである．このことを実機による実験で確認した結果を図 2 に示す．電力波形の測定に使用したオシロスコープは，Tektronix TDS7104 である(以下同様)．図 2 は次数 N が異なる 3 種類の AND について，入力信号の 1 ビットを DPA の選択関数とした時の電力差分波形(入力データを処理する際の電力波形を大量のランダムデータについて測定し，選択関数の値が 1 か 0 かで測定データを 2 つのグループに分けて，両グループの平均電力の差分をとったもの[1],[2])を一つの図にまとめたものである(サンプル数はいずれも 10000 データ)．横軸は時間，縦軸は 4 入力 AND のリークの最大値が約 7 になるように正規化した電力差分である．

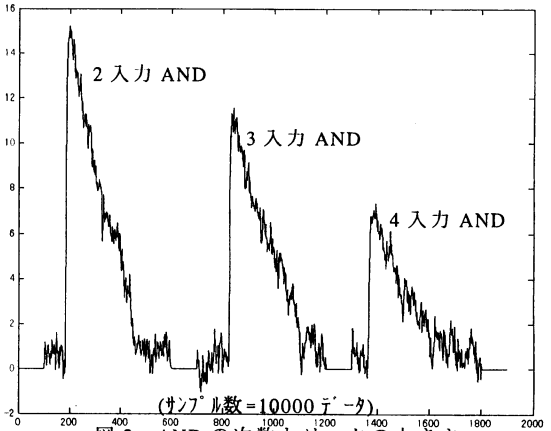


図 2　AND の次数とリークの大きさ

実験で用いたデバイスではもちろん信号の伝搬遅延が存在しているが，過渡遷移の影響(後述)の少ない単純な回路であるため，観測されたリークの大きさは，ほぼ先に述べた比を示しており，遷移確率の差がリークとして現れるという考察の妥当性が実証された．

さらに，リークの大きさが，対象回路全体での遷移回数の期待値の差となることを示すための実機による実験結果を図 3 に示す．本実験では，2 入力 AND ゲートの先に巨大なバッファツリーを接続した回路構成において，バッファの個数だけを 3 通りに変え，それぞれについて電力差分を求めている(サンプル数はいずれも 1000 データ)．図 3 の横軸は時間，縦軸はバッファ個数が M(=256)の時のリークの最大値が 1 になるように正規化した電力差分である．図から，リークの大きさがバッファ個数に比例していること，すなわち対

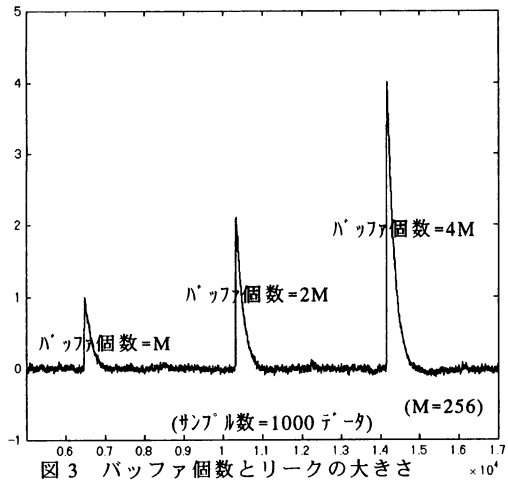


図3　バッファ個数とリークの大きさ

象回路全体での総遷移回数の期待値の差に比例していることがわかる．この回路も先の実験の回路と同様に，過渡遷移の影響(後述)の少ない単純な回路であり，信号の伝搬遅延の無い理想的なデバイスに近い実験結果になっていると考えてよい．

以上の考察と実験により，DPA の選択関数の信号レベルに応じた信号の遷移確率の偏りがリークとして現れることがわかる．すなわち，リークは配置配線などに依存して偶然に発生するものではなく，信号の伝搬遅延の無い理想的なデバイスにおいても発生するものと考えられる．

本節で述べた総遷移回数の期待値の差 (L_0)を簡単な式で表すと次のようになる．a_i は回路内の信号(i は全信号と 1:1 に対応)，s は DPA の選択関数である．

$$L_0 = \Sigma_i (P_{Tr}(a_i)_{s=1} - P_{Tr}(a_i)_{s=0}) \quad (3)$$

L_0は遅延の無い理想的なデバイスを想定しても発生する最も基本的なリーク(以下，“スタティックなリーク”と呼ぶ)と言える．一方，実際のデバイスのリークは，さまざまな形で信号の伝搬遅延の影響を受けたものになる．つまり，配置配線などが大きく関係してくる．次節以降では，この影響を検討する．

2.2.2. 過渡遷移によるリークの増幅

前節では，信号の伝搬遅延に伴う過渡遷移については特に考えなかった．ここではこの過渡遷移の影響について考察し，前節の考察を拡張/一般化する．図 4 の回路において，d0,d1,d2,d3 は回路への入力信号，a,b,c は回路中の論理ゲートの出力信号とすると，例えば AND ゲート(i0)の出力信号 a が遷移した時に信号 d2 が 0 であれば，OR ゲート(i1)の出力信号 b も遷移する．ここで，信号 b の遷移と信号 d3 の遷移が同じタイミングで発生しない限り，信号 b の遷移は XOR ゲート(i2)

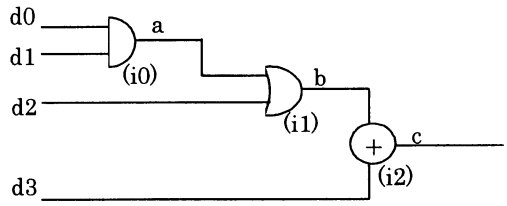


図4　サンプル回路 2

の出力信号 c も遷移させる．同様に，信号 a が確定した後に信号 d2 が確定し，信号 b が遷移すると信号 c も遷移する．XOR ゲート(i2)についても同じように，入力信号の遷移タイミングに依存して，過渡遷移が発生する．このように，信号の時間差を考慮すると，信号の伝搬遅延が無い場合と比べて余計に信号の遷移が発生する．すなわち，1 回の遷移が何倍かに増幅する．前節の図 3 からわかるように，総遷移回数が増えると，それに伴ってリークも大きくなる．

上記の考察でわかるように，スタティックなリークを発生する論理ゲートが，組み合わせ回路の信号伝搬パスの上流にあるほど，リークは大きく増幅される可能性がある．しかし，その増幅率は信号伝搬パスに合流する他の信号の値や遷移タイミングに依存して，同じ論理回路であっても，さまざまに変わり得る．例えば，図 4 の例では信号 a の遷移は信号 d2 が 0 の時は信号 b に伝搬するが，信号 d2 が 1 の時には伝搬しない．これは配置配線に依存した微妙な時間差にも大きく影響される．

このように，過渡遷移による増幅まで考慮して回路全体の総遷移回数の期待値を求め，リークを定式化することは非常に困難であるが，単純化して概念的に定式化することを以下で試みることにする．

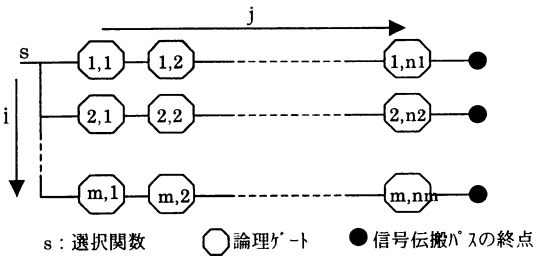


図5　定式化のためのモデル回路

図 5 は，選択関数 s を信号伝搬パスの起点とするような組み合わせ回路を一般化して表したものである．図 5 において，i と j はそれぞれ信号伝搬パスとゲート段数を表す添字である．DPA の選択関数である信号 s のファンアウトを m，各信号伝搬パスのゲート段数を ni とする．論理ゲート(i,j)の先は枝分かれすることも

あるが，図では省略している．単位時間中に信号の遷移が発生する可能性がある，全ての事象の集合を E，ある事象 $e(\in E)$における論理ゲート(i,j)の遷移確率を $P_{Tr}(i,j)_e$，その遷移が次段に伝搬する確率を $\beta_{i,j,e}$とする(i=j の時 $\beta_{i,j,e}$=1)と，(単位時間当たりの)総遷移回数の期待値は，

$$TC = \Sigma_{e\in E}\Sigma_{i=1}^{m}\Sigma_{j=1}^{ni}P_{Tr}(i,j)_e\Sigma_{k=j}^{ni}\Pi_{l=j}^{k}\beta_{i,l,e} \quad (4)$$

で表すことができ，DPA の選択関数 s で分類した時の総遷移回数の期待値の差(L_1)は，

$$L_1 = TC_{s=1} - TC_{s=0} \quad (5)$$

となる．これが信号の伝搬遅延を考慮したリークに相当する．式(4),(5)において，スタティックなリークを発生する論理ゲート毎に，自身の後段の $\beta_{i,j,e}$ を 0 としたものが前述の式(3)に相当する．

本章では，リーク発生のメカニズムとして，
1) DPA の選択関数の信号レベルに応じた遷移確率の偏りによって発生するスタティックなリーク
2)信号伝搬の影響によるリークの増幅
が存在することを示した．これらを定式化したものが式(4),(5)である．以上が，本章の冒頭で述べた二つの疑問に対する回答となる．

3. 論理シミュレーションによる DPA 評価手法

前章で示したように，(単位時間当たりの)遷移確率，総遷移回数という考え方に基づいて，対象回路の DPA 評価を行うことが可能である．本章では，標準的な論理シミュレータを使って論理設計の段階で効率的に DPA 評価を行う手法を提案する．

3.1. シミュレーションによる評価の必要性

例えば，DPA 耐性を備えた暗号デバイスを開発する際，事前にいくらリークが発生しないように考慮したとしても，思わぬ箇所でリークが発生する可能性は否定できない．このことは，大規模回路の開発において，膨大なテストパターンを用いて論理検証を行っても，予期せぬ論理不具合が残る可能性が否定できないことと同様である．暗号デバイス製造後に DPA 耐性が不十分であることが判明すると，開発期間やコストが大幅に増加することになる．このような問題を回避するためには，できるだけ設計の上流段階でシミュレーションによって対象回路の DPA 耐性を評価し，対策を施していくことが求められる．

3.2. 検討項目

シミュレーションによる DPA 評価を実現するための検討項目として，次のようなものが挙げられる．
・シミュレータの種類
・回路モデル(RTL/ネットリスト，遅延モード)
・消費電力情報抽出方法
これらについて検討した結果を以下に述べる．

(1)シミュレータの種類

消費電力の見積り精度を重要視するならば，SPICE 系の回路シミュレータが有望であるが，設計の上流段階で効率的な評価を行うことは困難である．一方，前章で定式化した考え方は，論理シミュレーションと親和性が高い．また，論理シミュレーションは論理設計の段階で実施可能である．従って，シミュレーションによる DPA 評価のためには，論理シミュレータが適切であると言える．

(2)回路モデル(RTL/ネットリスト，遅延モード)

対象回路を RTL とするか，ネットリストとするかは，それぞれ一長一短があり，難しい問題である．前者は後者と比べると設計のより上流段階における評価が可能である半面，DPA に関わる消費電力情報(すなわち信号の遷移回数)の見積りが不正確になると予想される．消費電力情報の見積り精度を確認するために，市販のツール(SYNOPSYS 社の pe_shell,dc_shell)を使って両者を比較した結果，ネットリストを用いた見積りの方が実機に近い傾向を示した．従って，ネットリストを用いて論理シミュレーションを行う方が，より正確な評価が可能だと判断した．

提案手法では，配置配線以前に評価可能とするため，論理シミュレーションの遅延モードは仮想遅延とする．しかし，後述するように，対象デバイスを信号の伝搬遅延の無い理想的なものと想定した評価も可能となるよう工夫している．

(3)消費電力情報抽出方法

信号毎の遷移回数を求めるために，論理シミュレータとして，スイッチング情報抽出用の PLI(Programming Language Interface)をアドオンした Verilog-XL を選択した．論理シミュレーション中の 1 クロックサイクル毎の信号遷移情報を SAIF(Switching Activity Interchange Format)ファイルに出力する．論理シミュレーション終了後，各 SAIF ファイル(延べ数万ファイル)から信号の遷移回数を抽出し，対象回路の 1 クロックサイクル毎の総遷移回数を，オシロスコープで測定する電力波形ファイルと同じデータフォーマットでファイルに格納する．データファーマットを統一することで，以降の解析処理は実機の DPA と同じ環境を使うことができる．なお，2.1.の式(1)を用いた上記の方法ではなく，前述の市販の消費電力見積りツールを使用することも可能であるが，現状では前者の方が 100 倍以上高速であることを確認している．

3.3. 概略フロー

提案する論理シミュレーションによる DPA 評価の概略フローを図 6 に示す．

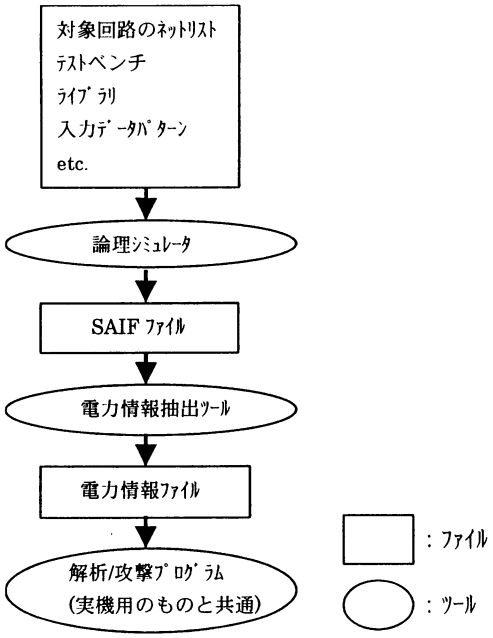


図 6　論理シミュレーションによる DPA 概略フロー

3.4. 実機評価結果との比較

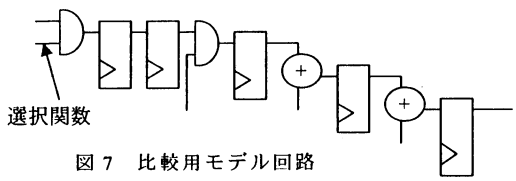


図 7　比較用モデル回路

図 7 のモデル回路について，実機の DPA 評価結果と論理シミュレーションによる DPA 評価結果を比較した例を図 8 に示す．図 8(上)は実機の DPA 評価結果であり，横軸は時間，縦軸は図 7 中の選択関数に基づく電力差分である．図 8(下)は論理シミュレーションによる DPA 評価結果であり，同上の選択関数に基づく回路中の信号の総遷移回数の差を，(図 8(上)と時間軸がほぼ一致するように)クロックサイクル毎に棒グラフ状に表示している．両者を比較すると，類似したリークの傾向(時刻，大きさ)が確認でき，論理シミュレーションによる DPA 評価が有効であることがわかる．

付録には，DES[3]の暗号回路について，上記と同じように実機の DPA 評価結果と論理シミュレーションによる DPA 評価結果を比較した例を示した．どちらの図も，DPA の選択関数は S_1-S_8 の 8 つの S-Box 入力(計 48 ビット)とし，S-Box 毎の 6 ビットの入力それぞれに基づく差分波形を 1 組にまとめ，計 8 組(48 ビット分)の差分波形をまとめて示している．2 つの図に現れた

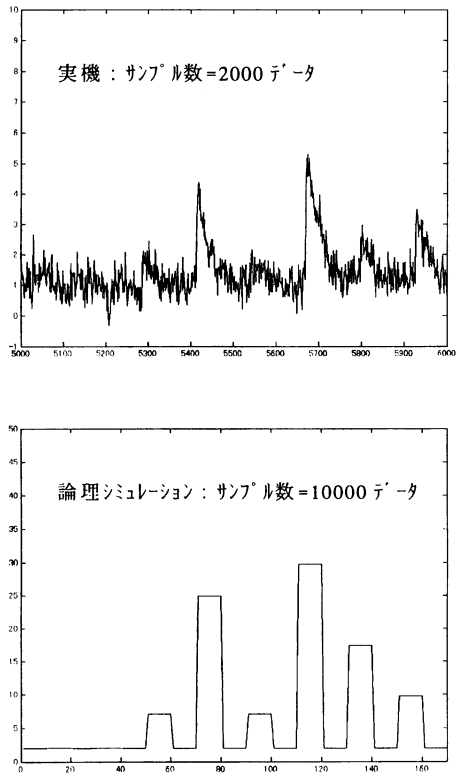


図 8　DPA 評価結果比較

リークの傾向はよく一致しており，前述のモデル回路のように単純な回路だけでなく，暗号回路全体のレベルでも提案手法が有効であることがわかる．

3.5. 電力情報抽出ツールの拡張機能

3.2.や 3.3.で触れた電力情報抽出ツールには，次のような機能拡張を行った．

(1)インスタンス指定

SAIF ファイルから信号の遷移回数を抽出する際，指定したインスタンス内の信号のみを選択する機能を持たせた．この機能を用いると，一度のシミュレーションで，複数の回路部分の個別評価が可能である．

(2)信号の伝搬遅延を 0 と見なした評価

1 クロックサイクル内での遷移回数が奇数回である信号のみを 1 回遷移したものしてと扱い，遷移回数が偶数回である信号は遷移しなかったものとして扱う機能を追加した．この機能を用いると，信号の伝搬遅延の無い理想的なデバイスにおけるスタティックなリークを評価可能である．

4. 過渡遷移とリークの波形

第2章の考察から，電力差分波形のスパイクとして現れるリークは，DPAの選択関数の予測値の正誤がそれぞれ1/2の確率であるランダムな状態から，全て正解である偏った状態に遷移する際に消費される(平均的な)電力であると言うこともできる．再びランダムな状態に戻る際にも同等の電力が消費される(図9参照)．

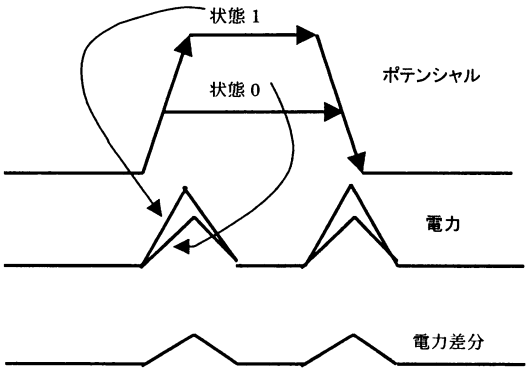


図9　リークのイメージ

従って，スタティックなリークのみを考えると，通常は連続したクロックサイクルで極性(山/谷)の揃ったスパイクが現れることになる[4]．しかし，実際には信号の過渡遷移の影響でいろいろなバリエーションが存在する．典型例を図10に示す．

図10のケース1は，過渡遷移の影響が小さいもの，ケース2は比較的大きな影響があるもの，ケース3は過渡遷移の影響がかなり大きなものである．過渡遷移の影響が大きいものほど，DPAの選択関数の信号値が0から1に遷移する時の方が逆の場合よりも，遷移が伝搬する確率が大きいと考えられる．

実際にDPA評価結果を見てDPA耐性を判定する場合には，図10のようなスパイクが観測されるとノイズではなくリークであると判断することになる．

5. おわりに

本論文では，CMOSデバイスにおけるリークの発生メカニズムを検討し，リークモデルを構築した．さらに，効率と精度を両立した論理シミュレーションによるDPA評価手法も提案し，その有効性を示した．提案手法のさらなる高速化，高精度化が今後の課題である．

リークは，DPAの選択関数の信号レベルに応じた信号の遷移確率の偏りと過渡遷移によって発生／増幅するものであり，単に中間変数の値を予測不能にするだけでは十分な対策とはならないと考える．十分な対策を実現するためには，DPAの選択関数の信号レベルと

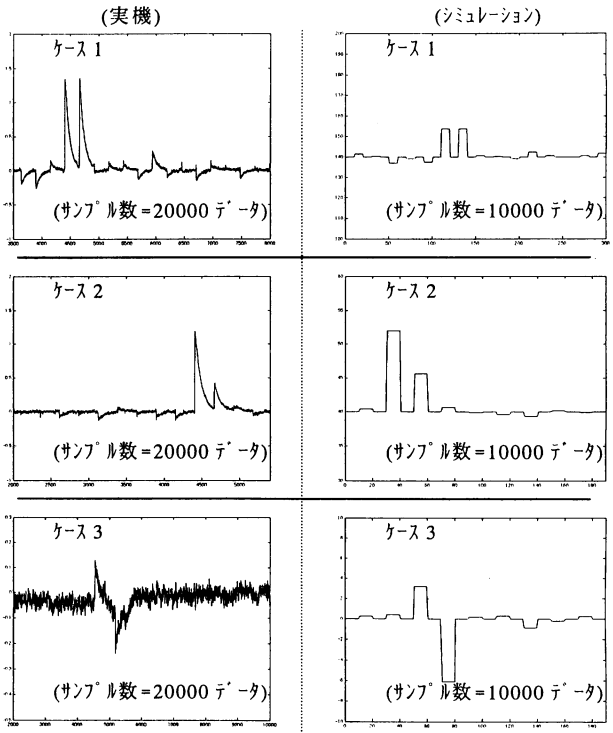


図10　DPAリークのスパイク典型例

信号の遷移確率の相関を無くさなければならない．

著者らは，信号の伝搬遅延についてさまざまな条件を想定して，第2章で示した式(4),(5)を適用すると，特定の条件を満たした場合のみ発生するリークが存在することも確認し[5]，このようなリークに対しても有効な対策手法を提案している[6]．

文　献

[1] P. Kocher, J. Jaffe, B. Jun, "Differential power analysis", In Advances in Cryptology - CRYPTO'99, volume 1666 of Lecture Notes in Computer Science, pp. 388-397, Springer-Verlag, 1999.

[2] P. Kocher, J. Jaffe and B. Jun. "Introduction to Differential Power Analysis and Related Attacks". http://www.cryptography.com/dpa/technical/index.html

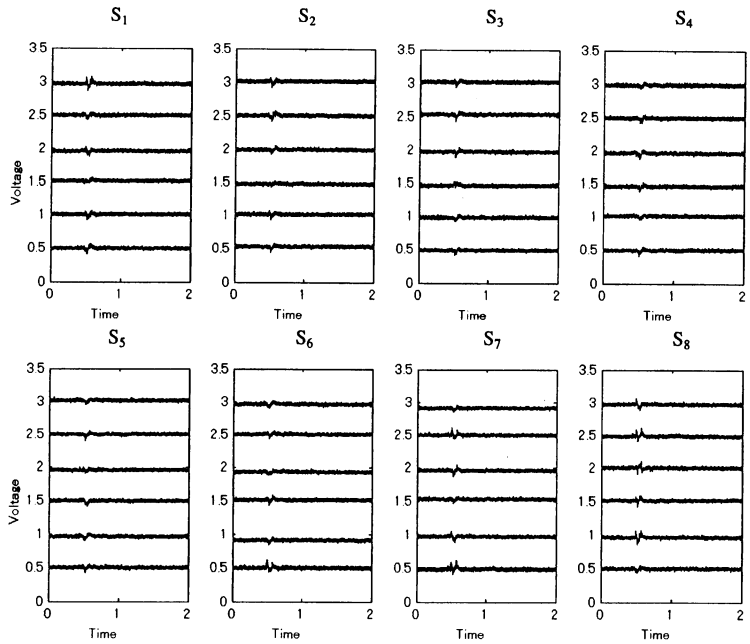
[3] US National Bureau of Standards, "Data Encryption Standard", Federal Information Processing Standard (FIPS), Publication 46-2, 1993.

[4] Suresh Chari,Charanjit Jutla, Josyula R. Rao, Pankaj Rohatgi,"A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards", AES round 2, 1999.

[5] 市川，鈴木，佐伯: データマスクを利用したDPA対策に対する攻撃, ISEC2004, 2004.7

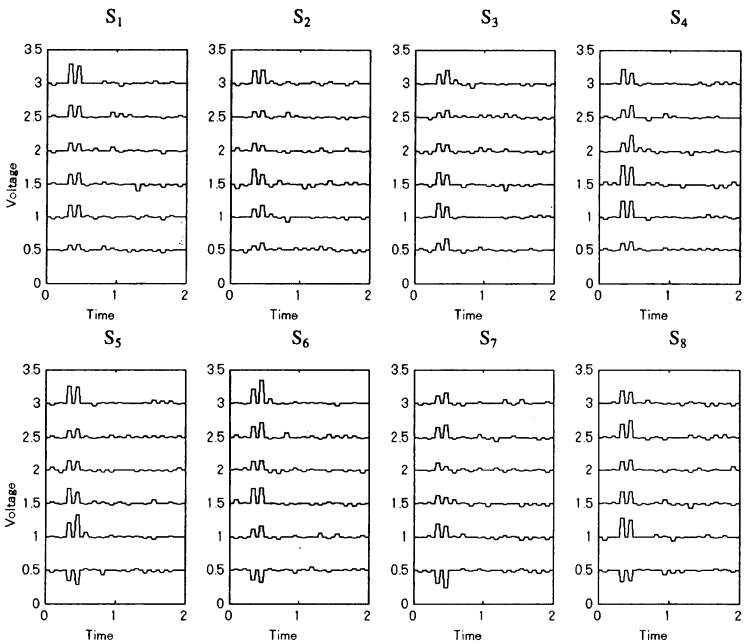
[6] 鈴木，佐伯，市川: 遷移確率を考慮したDPA対策手法の提案, ISEC2004, 2004.7

付録. S-Box 入力を選択関数とした DES 回路の電力差分計算結果



a) 実機 FPGA(Virtex1000)を用いた DPA 評価結果(*) (ｻﾝﾌﾟﾙ数=20000 ﾃﾞｰﾀ)

(*)開発言語：Verilog-HDL 論理合成：Synplify version 7.0.3 配置配線：ISE version 4.1.03i



b) 論理シミュレーションによる DPA 評価結果(**) (ｻﾝﾌﾟﾙ数=10000 ﾃﾞｰﾀ)

(**)評価対象は，実機 FPGA 用のネットリスト(論理合成結果)の暗号コア部分