Copyright© 2013 The Institute of Electronics, Information and Communication Engineers

SCIS 2013 The 30th Symposium on Cryptography and Information Security
Kyoto, Japan, Jan. 22- 25, 2013
The Institute of Electronics, Information and Communication Engineers

イベントモデルシミュレーションによるサイドチャネル情報取得の効率化

Efficient Acquisition Of The Side-Channel Information Using Event Model Simulation Methods

浅井 稔也* 吉川 雅弥*
Toshiya Asai Masaya Yoshikawa

あらまし サイドチャネル攻撃では，暗号回路の動作時に観測可能な電力や電磁波などのサイドチャネル情報を繰り返し取得し，これらを統計的に処理することで，内部に存在する鍵情報を推定する。このサイドチャネル攻撃に対して，LSI 設計時に攻撃耐性の評価と，回路及び実装上の対策を講じることが重要であることはいうまでもない。本稿では設計段階での電力解析攻撃耐性評価に関し，多数回の暗号化シミュレーションを必要とする消費電力情報取得工程の効率化手法を提案する。提案手法はイベントモデリングを使って，SPICE シミュレーション相当の精度を保ちつつ論理シミュレーション＋αの現実的な処理時間で消費電力情報を取得する。ここで，既製の EDA ベンダー製ツールを使用した場合と比較して，精度・処理時間のバランスの点で優位性を持つことを目標とした。また，AES 試作チップの設計データを使って提案手法の有効性を確認した。

キーワード サイドチャネル攻撃，電力解析攻撃，消費電力シミュレーション，AES，LSI

1 はじめに

情報セキュリティ技術は，ネットワークやストレージなどのインフラの発展，企業や個人で扱う機密情報の増加に伴い，急速にその重要性を増してきた。機密情報隠蔽のための主要技術は暗号化技術である。現代の暗号は計算量的にその解読がほぼ不可能である事を前提に成り立っており，さらには，処理効率や実装方法など様々な面で安全性を検証されたものが標準化され広く普及している。一方で，近年，暗号回路の動作時に観測可能な電力や電磁波などのサイドチャネル情報を繰り返し取得し，これらを統計的に処理することで，内部に存在する鍵情報を推定するサイドチャネル攻撃と，その対策手法の研究が進められている。このようなサイドチャネル情報を介した攻撃を想定し，それらに対する対策を施した設計を行うことは，暗号の実装設計において必須の課題となっている。そこで本研究では，現実的な脅威である電力解析攻撃を対象に，設計段階での耐性評価を実現する検証プラットフォームを開発するための検討を行う。

電力解析攻撃は消費電力波形の観測データを用いて鍵推定を行うもので，観測が比較的容易であるため，サイドチャネル攻撃の中でも最も危険性が高いと言える。代表的な攻撃方法として差分電力解析（Differential Power Analysis：DPA）[1] や相関電力解析（Correlation Power Analysis：CPA）[2]，相互情報量解析（Mutual Information Analysis：MIA）[3]，等が報告されている。このような攻撃を防ぐために，暗号ハードウェアの設計時に対策を施し，さらに，その対策効果を十分に確認しておくことは必須であると言える。

本研究では，暗号処理 LSI の電力解析攻撃に対する耐性を設計時に検証するにあたり，その消費電力情報の取得方法の効率化を目標とし，高速かつ精度の高い電力データの取得方法を提案する。従来，EDA ベンダー製の LSI 設計ツールを用いて多数回の暗号化処理シミュレーションを行い，消費電力波形を取得していたが，この消費電力波形の精度と，シミュレーションに要する時間の双方のバランスに着目すると，既製のツール群は電力解析攻撃の耐性検証を十分かつストレスなく行う性能を有しているとは言い難い。そこで，本研究では，最初にまず，数回の暗号化処理から成る短めの SPICE シミュレーションによって検証回路部分のモデリング作業を行い，次に論理シミュレータによる必要回数分の暗号化処理シミュレーションを実行し，先のモデリング結果と合成する手段をとることで消費電力波形を算出するようにした。こうすることで，消費電力シミュレーションの精度と速度のバランスを，攻撃耐性検証作業により適するように改善することが出来た。

本提案手法により，LSI 設計工程における耐タンパ検

* 名城大学 理工学部 情報工学科 〒468-8503 愛知県名古屋市天白区塩釜口 1-501. Department of Information Engineering, Meijo University, 1-501 Shiogamaguchi, Tenpaku-ku, Nagoya, 468-8502, Japan

証の消費電力情報取得効率を改善し，問題が見つかれば早期に論理設計にフィードバックして対策に結び付けることができる。さらに，標準暗号である AES[4]を実装した LSI の試作設計データを使った評価実験により，提案手法の有効性を確認した。

2　関連する研究

電力解析攻撃の対策手法は，暗号処理回路中の秘密情報が消費電力情報にリークしてしまうのを防ぐことを目的としている。対策回路としては，MaskedAND[5]，RSL[6][7]のような乱数による攪乱を利用した対策手法，乱数と秘密分散による Threshold Implementation[8]や，また，WDDL[9]のような相補動作によるキャンセリングを利用した対策手法, MDPL[10]のように乱数と相補動作の双方を利用した対策手法などが挙げられる。これらの対策の適用は，サイドチャネルリークによる脆弱性が懸念される限り，もはや必須の要求仕様であり，設計段階においてその対策効果を十分に検証しておく必要がある。もちろん，対策による攻撃耐性改善の効果は，チップを試作し，SASEBO[11]のような評価プラットフォームを利用して攻撃実験を行うことでも確認することができるが，設計段階での基礎評価シミュレーションを十分に行う事で改善効果を確認し，さらに動作マージンをも保証した設計を行うことが肝要である。

ここで，耐性の検証を行うにあたり生じる課題として，解析の精度と，処理に要する時間のトレードオフの問題がある。十分に正確で十分に高速な解析は困難であり，むしろ，解析に要する波形数が多いことから設計工数はかなり大きなものとなる。検証工数は大別すると，消費電力シミュレーション自体にかかる工数と，次の段階として，先に求めた消費電力を使って電力解析攻撃の種々の攻撃手法を試行し，脆弱性の大小を判定する工数，の 2 種類がある。後者に関する効率改善手法として，筆者らは回帰分析と攻撃環境モデリング手法を使った評価の効率化の提案を行った [12]。また，前者に関しては，現状では EDA ベンダーのツール群を用いて消費電力を求めるのが常である。

ところが，数万～数十万回の暗号化処理時の各消費電力波形を正確に求めることは, 一般の論理シミュレータ，SPICE シミュレータで提供されている機能を持って実現しようとしても精度と処理時間のバランスのとれた使い勝手のよいシミュレーションを行うことはかなり困難であると言わざるを得ない。この点は攻撃耐性検証作業を設計工程に取り入れる際の大きな障害となっている。EDA ベンダーの製品を利用する場合，従来では，Synopsys 社の製品である PrimeTime PX を用い，論理シミュレータと組み合わせて消費電力波形を算出し，これを用いて電力解析攻撃シミュレーションを行っていた。しかしながら，PrimeTimePX が出力する電力波形の細部を, SPICE シミュレータが出力するそれと比較した場合，精度の点で必ずしも同等とは言えない。前者は，使用してみる限り，各々のセルの消費電力値をある時間ホールドした矩形波を重ね合わせたような電力波形を出力している。ただ，もう一方の SPICE シミュレータは，その処理時間が，本用途に適用するにはあまりにも大きすぎて非実用的である。この問題に関連する研究報告として，文献[13]では，内部セルを多数の単純なキャパシタンスモデル群と見做し，サイドチャネルリークの解析に適した非常に高速な消費電力シミュレーションを実現する手法が提案されている。文献[13]では，さらに，配線の寄生容量成分をキャパシタンスモデルに取り込むことで精度の高いシミュレーションを実現している。この報告からも分かるように，消費電力シミュレーションでは精度と軽量化を両立したモデリングが鍵であると言える。

本研究では以上の点を考慮し，文献[13]の手法とは異なり，既製の EDA ベンダーのツール群を活用しつつ，消費電力シミュレーションの効率を改善する手法について提案する。

3　イベントモデルシミュレーション

本研究の提案手法は，暗号 LSI の設計工程で電力解析攻撃に対する耐性を評価するための消費電力波形の効率的な取得方法に関するものである。

提案手法はモデリング工程と暗号処理シミュレーション工程の 2 つの手順で実現する。図 1 に 2 つの手順の概要を示す。以下，全体のフローを簡単に説明する。

手順 1 では，まず，ある検証対象となるブロックに着目する。AES の場合であれば，例えば，ある SubBytes 変換回路に着目する。そこに含まれる全てのセルについて, 各々がスイッチング動作をしたときの各セルの VDD 側, VSS 側の電流波形を SPICE シミュレーションにより算出し，SPICE 精度の電流波形モデルを作成する。ここでは配置配線後の SPICE ネットリストを使うこともできるので，各セルの遷移イベントに対して実装状態に対応した非常に高精度な電流波形モデルを得ることができる。

次に，手順 2 では，まず電力解析攻撃シミュレーショ

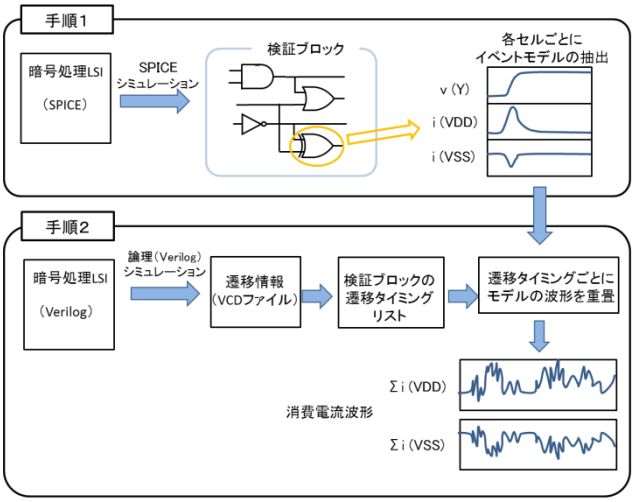

図1　イベントモデルシミュレーション

ンに必要な回数分の暗号処理シミュレーションを論理シミュレータを用いて行う。ここでは，SDF ファイルを取り込んだディレイシミュレーションを行うものとする。このとき，TYP，MIN，MAX のどのスピードを選択するかということと，手順 1 における SPICE シミュレーションの環境温度の両者をある程度整合がとれたものになるように設定する。そして，論理シミュレーションにより得られる遷移タイミング情報を整理し，検証対象ブロックの各セルの出力がどのタイミングで立ち上がり，また，どのタイミングで立ち下がるかというデータのリストを作成する。その後に，このリストに基づいて定義される時系列上に，手順 1 で得た電流波形モデルをはめ込んでいく作業を行う。この作業を終えた時点で検証対象ブロックの全てのセルの VDD 側，VSS 側の電流波形が得られる。

さらに，これらのセルごとの電流波形を全セルについて重畳することで検証対象ブロック全体での VDD 側，VSS 側電流波形を得ることができる。

また，この手法の応用として，AES の最終ラウンドのような攻撃シミュレーションに必要なタイミングについてのみ電流波形モデルをはめ込むようにし，他のラウンドについてはこの手順をスキップすることで，手順 2 の処理時間とデータサイズの削減が実現できる。

以降，3.1 節で手順 1 のモデリング工程について，3.2 節で手順 2 の暗号処理シミュレーション工程についてさらに具体的に説明する。

3.1　手順 1．「モデリング」

ここでは，標準暗号 AES のハードウェア実装回路を検証対象とし，ある任意の SubBytes 変換回路の各セルをモデリングする際の手順を例に説明を進める。

モデリング手順を図 2 に示す。モデリングに先立ち，検証対象ブロックの SPICE シミュレーションを実行する必要がある。回路情報ネットリストは，EDA ツールが生成した工程ごとのネットリストが使用可能である。つまり，配置配線前，配置配線後のいずれのネットリストでもよく，寄生抽出情報を加えるかどうかの選択も可能である。ネットリストのフォーマットは SPICE であるので，verilog ネットリストを元にするのであれば SPICE ネットリストへ変換作業を行っておく。ただし，扱うネットリストは，図 2 の CASE1，CASE2 に示すように SPICE シミュレータの機能を活用した 2 種類のネットリスト構成が可能である。CASE1 は全体を SPICE ネットリストで表現する方法であり，CASE2 は暗号回路，もしくはさらにその中の秘密情報のリーク源と成り得るクリティカルな回路については SPICE ネットリストで記述し，他を Verilog ネットリストとするミックスレベルシミュレーションを用いる。ミックスレベルシミュレーションでは，Verilog シミュレータと SPICE シミュレータが連携動作をしながらシミュレーションが実行される。暗号回路以外の回路が大きい場合には CASE2 の方法が有効である。

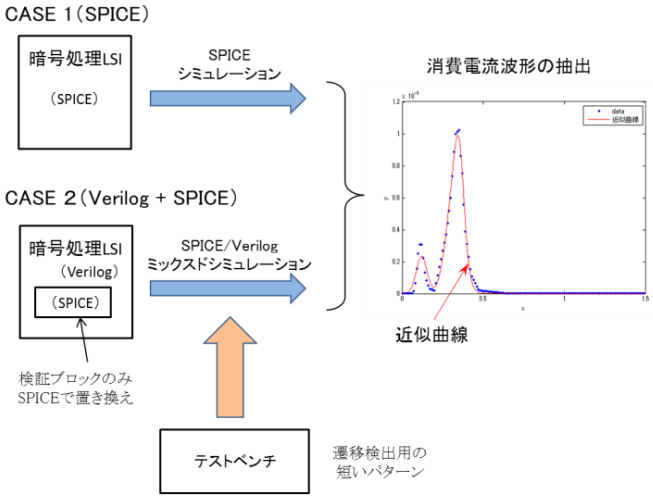

図2　SPICEシミュレーション

CASE1 または CASE2 の SPICE シミュレーションでは，SubBytes 内の各ノードが最低 1 回ずつ立ち上がり遷移，及び，立ち下がり遷移をする程度の短いテストベンチを作成し，先に準備した SPICE ネットリストと合わせて SPICE シミュレーションを実行する。詳細配置配線終了後のネットリストであり，寄生抽出が済んでいれば，SPICE ネットリストと一緒に寄生抽出データを読み込んでやることで，配線寄生容量を考慮したシミュレーションを実行でき，より正確なモデリングが可能となる。

SPICE シミュレーションを終えたら，次に検証対象となる SubBytes 変換回路に含まれる各々のセルに着目し，あるセルの出力が立ち上がり，もしくは立ち下がり遷移をしたときのそのセルの VDD ピンに流れる消費電流波形と VSS ピンに流れる消費電流波形をシミュレーション出力データから抽出し，立ち上がり遷移時の消費電流波形 i(VDD)，i(VSS)のモデリング波形として保存する。両者の時間的な基準は出力ピンの立ち上がり，もしくは立ち下がりスタートタイミングとする。

出力ピンの立ち上がり時と立ち下がり時の i(VDD)，i(VSS)波形は別々に抽出してモデル化する。

セルが AND や OR の単一ゲートであればセルの内部動作は単純であるが，AND-OR 構成等の複数ゲートを組み合わせたスタンダードセルや，フリップ・フロップの場合，消費電流を精密に求めるには各入力ピンの状態を考慮する必要がある。しかし，今回のルールでは，次段のセルに対して充放電する成分にのみ着目し，スタンダードセル内部のみで遷移するケースについては省略することでモデリングを簡略化している。モデリングする時間波形の Duration はプロセスや回路にも依存するが，2～3[nsec]程度，Resolution は 0.05[nsec]程度でよいと思われる。

まとめると，各セルの出力が遷移したとき，同じ基準時間スケール上で VDD 電流，VSS 電流の時間波形を抽出してサンプリングデータ化する作業がモデリングであ

る。セル出力の遷移時のみに着目しており，このモデルをイベントモデルと呼ぶことにする

Duration が 2[nsec]，Resolution が 0.05[nsec]の場合であれば，40 サンプルの時系列データで電流波形を表現できる。また，MATLAB 等に取り込んで処理することを前提にすれば同ツールの機能を使って図 2 の右の波形のように近似処理を行い，モデルのデータ量を削減することも有効である。この例では，3 項のガウス近似を行っている。近似について，MATLAB の Curve Fitting ToolBox を用いていくつかの近似手法を試してみたところ，本用途には 3 項のガウス近似を使うことで，過剰適応も起きず，複数の元波形に対して大きく外れるようなケースもあまり見られなかった。3 項のガウス近似であれば 1 つの曲線を 6 つのパラメータで表現することができ，データサイズを削減するのに有効である。

検証対象ブロック内の全てのセルに対し，SPICE シミュレーション結果のデータを検索しながら，以上述べたようなモデリング作業を順次行っていく。セルによっては出力信号のスムーズな遷移イベントが抽出しにくいものもあるが，その場合，波形に僅かな補正を加えることで，うまく抽出することができる場合もある。以上は，波形処理スクリプトを作成して実行させることで，まとめて処理することが可能である。このようにして，対象とする検証ブロック内の全セルのモデリングを終えるまで繰り返すことで，セル出力遷移時の電流モデル（イベントモデル）のデータベースを作成することができる。

なお，複数の SubBytes 変換回路や全 SubBytes 変換回路のモデリングを同時に行うことも可能ではあるが，扱うセル数，ノード数がかなりの数に増えてしまうので，データを整理する際のメモリ使用量が大きくなり，必ずしも効率的とは言えない。むしろ，1 つのバイト系統で独立してモデリングし，個々にイベントモデルデータベースを作成していくほうが効率的なケースが多いと思われる。処理手順については，適宜調整が必要である。

3.2　手順２．暗号処理シミュレーション

次に所望の暗号化回数分の論理シミュレーションを行う。Verilog テストベンチを作成し，回路全体の Verilog ネットリストと組み合わせ，SDF（Standard Delay Format）ファイルのバックアノテーションを指定してディレイシミュレーションを行う。

ここでの論理シミュレーションは，そのシミュレーション結果である VCD（Value Change Dump）ファイルをもとに，検証ブロックの各セルの出力がどのような遷移をどのタイミングでするのか，その情報を抽出したタイミングデータリストを得ることが目的である。

ここで問題なのは，論理シミュレータが出力する遷移タイミングと，SPICE シミュレータが算出するそれとの間でどうしても誤差が生じてくることである。ディレイシミュレーションは，TYP，MIN，MAX のタイミング

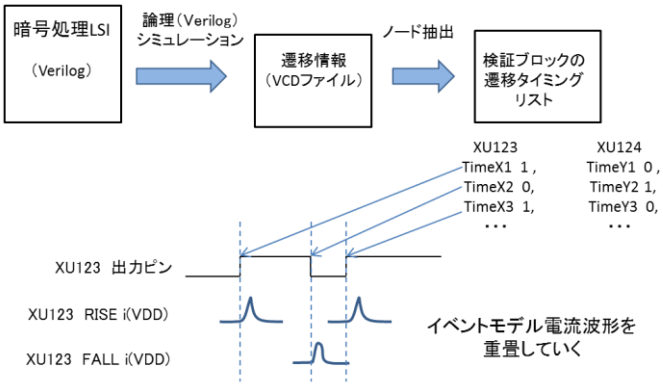

図3　暗号処理シミュレーション

指定でディレイシミュレーションを行うのに対し，SPICE シミュレーションでは温度，電圧など細かな制御が可能なためである。このため，本提案手法では，スイッチングタイミングに関しては，論理シミュレータによるディレイシミュレーション結果をマスターとするようにし，例えば TYP ディレイの場合は，SPICE シミュレータでの環境設定もほぼ Typical 値となるよう設定して誤差を抑えるようにする必要がある。

各セルの出力の遷移タイミング情報が得られたら，タイムライン上のその遷移タイミングのポイントに対し，手順 1 で作成した，出力遷移－i(VDD)－i(VSS)の対応関係をあてはめていく。その様子を図 3 に示している。図中の XU123 というセルの出力ピンが TimeX1 で立ち上がり，TimeX2 で立ち下がり，TimeX3 で再び立ち上がるとする。この場合，TimeX1 と TimeX3 の時点で，立ち上がりイベントモデルの VDD，VSS 電流波形を，TimeX2 時点で立ち下がりイベントモデルの VDD，VSS 電流波形をあてはめる。こうすることで XU123 の VDD ピンと VSS ピンの電流波形を生成することができる。同様の操作を繰り返し，各々のセルに流れる i(VDD)と i(VSS)の時間波形を生成することができる。全てのセルについて i(VDD)，i(VSS)が求まったら，検証ブロック全体，ここでは SubBytes 変換回路全体について，これらの電流波形を重畳して，そのブロック単位での Σi(VDD)，Σi(VSS)の波形を求めることができる。

こうして求めた電流波形は，ほぼ SPICE シミュレータを使って算出した波形に近い形となる。ただし，論理シミュレータの検証能力を超える中途半端な遷移や細かなグリッチについては無視されてしまうため，SPICE シミュレーションと同じ精度を実現することはできないが，処理速度の点では SPICE シミュレータのそれに対して大幅に高速化することが可能である。

さらには，電力解析攻撃を行うラウンドの遷移箇所に限ってイベントモデルのあてはめを行うようにすれば，攻撃検証タイミングのみの詳細な電流波形を得ることができるので，さらなる高速化とデータサイズの節約が可能となる。

4　評価実験と考察

4.1　実験要領

提案手法の有効性を検証するために，0.18μm のプロセスで試作した AES 暗号処理チップの設計データを用いて実験を行った。実験では 3 種類の手法で求めた消費電力波形を比較した。1 つ目は本提案手法によるもの，2 つ目は Synopsys 社の VCS と PrimeTimePX の組み合わせで算出した消費電力波形，3 つ目は同じく Synopsys 社の SPICE シミュレータである CustomSim を用いて算出した結果である。

PrimeTimePX を使った方法は，処理速度が SPICE シミュレータに比べて非常に高速である為，従来，設計段階での多数の暗号化消費電力波形を取得する際にはこの PrimeTimePX を用いた波形取得に頼っていた。また，SPICE シミュレータは，多くの種類の製品がリリースされているが，その中でも高速 SPICE シミュレータの範疇に含まれるものが本用途には適している。高速とは言っても数万回の暗号化波形を得るには処理時間，出力データサイズ，共に大きくて実用には適さなくなってくるので，部分的に詳細なシミュレーションをしたい場合に用いることがある。

CustomSim は，速度と精度のバランスを設定により変えることができ，本実験では最も高速の設定とした。実験用のマシンには，CPU: Xeon W3565 3.2GHz，Memory: 8GB のスペックのものを用いた。

また，モデリング，消費電力波形の生成処理には Mathworks 社の MATLAB を用いた。

4.2　イベントモデルの作成

3.1 節で説明した手順に従って，内部セルの出力ピンの立ち上がり，立ち下がり遷移時の i(VDD)，i(VSS)波形を求める。まず，モデル作成用に数回の暗号化を実行させるテストベンチを作成し，CustomSim を使って SPICE シミュレーションを行った。ここでは，配置配線後のネットリストを用い，寄生抽出データを取り込んでシミュレーションを行った。このシミュレーションの実行時に，任意の SubBytes に含まれる全てのセルごとに i(VDD)，i(VSS)をダンプするよう指定する。

シミュレーションが終わったら，そのシミュレーション結果データを MATLAB に取り込み，各セルについて出力ピンの状態がきれいに立ち上がり遷移をするポイント，及び立ち下がり遷移をするポイントをサーチする。

合成体方式[14]の SubBytes 実装でテストしたところ，3 回ほどの暗号化処理で，SubBytes 変換回路のほぼ全てのセルで遷移ポイントを見つけることができた。遷移するポイントが見つかったら，それらのタイミングにおける i(VDD)，i(VSS)の時系列データを SPICE シミュレーション結果からサンプリングする。ここでは，2[nsec]の期間分の v(Y)，i(VDD)，i(VSS)の 3 種類の時系列データ，つまり，3.1 節で説明したイベントモデルが作成されるようにした。なお，v(Y)はセルの出力ピン Y の電圧波形を示す。各波形のサンプリング周期は 0.05[nsec]にした。

このイベントモデルを，後に行う暗号処理シミュレーションで得られる遷移タイミング情報と組み合わせて最終的な消費電力波形を算出する。

4.3　消費電力シミュレーションの比較

次に 3.2 節で述べたように論理シミュレーションを行い，その結果の各イベントに対してイベントモデルの電流波形を重畳させていく。これにより，Σi(VDD)，Σi(VSS)の時系列波形を求めることができる。

提案手法により求めた電流波形を，既存の EDA ツールの結果と比較してみる。図 4 は，Synopsys 社の消費電力波形生成ツールである PrimeTimePX の結果である。また，図 5 は同時刻の消費電力について，提案手法により求めた結果である。図 4 の波形は，拡大すると，ある期間ホールドされた波形のようになっているのがこのツールの出力の特徴である。これに対し，提案手法は消費電力波形をよりきめ細かく描けているように見える。実際，これと同時刻の SPICE シミュレーション波形と比較しても似た波形が合成出来ている。

次に，表 1 に処理時間を比較した結果を示す。ここでいう処理時間であるが，まず，PrimeTimePX は，論理シミュレーションの結果である VCD ファイルを元に，消

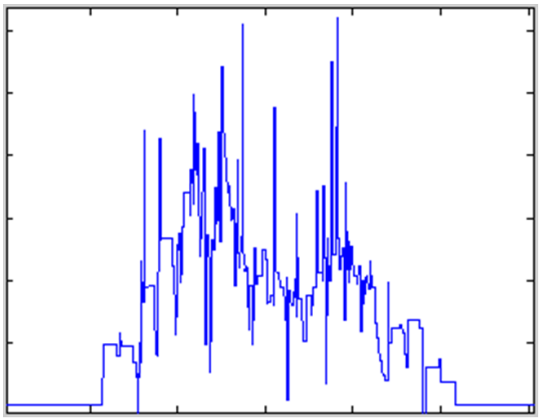

図4　消費電力波形（PrimeTime PX）

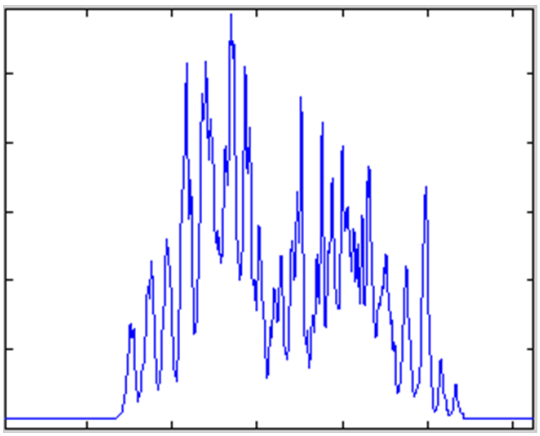

図5　消費電力波形（提案手法）

費電力波形データを生成するのに要する時間，提案手法については，論理シミュレーションの結果から抽出したタイミング情報と先に準備したイベントモデルを使って消費電力波形データを生成するのに要する時間，SPICE シミュレーションについては，SPICE シミュレータを使って消費電力波形を抽出するのに要する時間である。前 2 者は，論理シミュレーションの時間を除外している為，必ずしもフェアな比較にはなっていないが，いずれにせよ，SPICE シミュレーションに要する処理時間は本用途への適用を考えた場合，現実的ではない処理時間となっている。表 1 での処理時間は，暗号化 100 回分の処理時間である。提案手法では，イベントモデルのはめ込み作業だけの実行時間であり，かなり高速な処理が実現出来ている。

	消費電力波形生成時間 （100回の暗号化に要した時間）
PrimeTime PX	63[sec]
提案手法	4.5[sec]
CustomSim（SPICE）	3368[sec] (56min.8sec.)

表1　処理時間の比較

5　まとめ

本研究では，暗号 LSI の設計工程で電力解析攻撃に対する耐性検証を行うにあたり，消費電力波形を得るためのシミュレーションの効率化と高精度化を既製の EDA ツール群を活用して行う手法について提案した。実際に AES 試作チップの設計データを用いて評価実験を行ったが，提案手法は，MATLAB 上でいくつかの補助ツールを作成する必要があったものの，ほぼ，既製の EDA ツール群の機能を活用して消費電力波形を効率よく取得することができた。

このような検証用途を想定した場合，既製の EDA ツールはその要求を十分満たすだけの機能を備えているとは言い難い。ここで，既製の EDA ツール群で，もしこういうことが出来たらという要望を簡潔に述べると，検証対象としたい回路に関して，SPICE に近い精度での電流シミュレーションをさらに高速に行いたいということ，また，回路を選択して，かつ攻撃対象タイミングだけを選択して内部パラメータのダンプを行う機能，などがあれば，さらに使い勝手が改善されると思われる。

例えば，本研究で提案したイベントモデルの作成についても EDA ツールにいくらかの機能追加が実現できればさらに簡便なモデル作成が可能になると思われる。

今後の研究課題としては，電磁波解析攻撃に対する耐性検証のシミュレーションに本提案手法が活用できると考えているので，引き続き検討を進めていく予定である。

謝辞

本研究は JST,CREST「ディペンダブル VLSI システム基盤技術」の研究の一環として行われた。また，東京大学大規模集積システム設計教育研究センターを通し，シノプシス社の協力で行われたものである。関係各位に感謝する。

参考文献

[1] P.C.Kocher, J.Jaffe, B.Jun, “Differential Power Analysis”, Proc. of International Cryptology Conference’99, pp.388-397, 1999.

[2] E.Brier, C.Clavier, F.Olivier, “Correlation Power Analysis with a Leakage Model”, Proc. of Cryptographic Hardware and Embedded Systems 2004, pp.16-29, 2004.

[3] B.Gierlichs, L.Batina, P.Tuyls, B.Preneel,“Mutual Information Analysis”, CHES 2008,pp.426-442,2008.

[4] NIST, “Advanced Encryption Standard (AES) ”, FIPS PUB 197, http://csrc.nist.gov/publications/fips/index.html

[5] E.Trichina, “Combinational Logic Design For AES SubByte Transformation On Masked Data”, Cryptology ePrint Archive, pp.2003-236, 2003.

[6] D.Suzuki, M.Saeki, K.Simizu, A.Satoh, “A Design Methodology for a DPA Resistant Cryptographic LSI with RSL Techniques”, Proc. of Cryptographic Hardware and Embedded Systems 2009, pp.189-204, 2009.

[7] 岩井克彦，柴谷恵，汐崎充，藤野 毅，「ドミノ RSL 方式 DES 暗号回路に対する DPA 攻撃脆弱性評価と対策法の提案」，SCIS2012, 2C2-3, 2012.

[8] S.Nikova,C.Rechberger,and and V.Rijmen, “Threshold Implementations Against Side-Channel Attacks and Glitches”, Proc .of ICICS2006, LNCS4307, pp.529-545, 2006.

[9] K.Tiri,I,Verbauwhede, “A Logic level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation”, Proc. of Design, Automation and Test in Europe2004, pp246-251, 2004.

[10] T.Pop, S.Mangard, “Masked Dual-Rail Pre-charge Logic:DPA-Resistance Without Routing Constraints”, Proc .of Cryptographic Hardware and Embedded Systems 2005, LNCS3659, pp.172-186, 2005.

[11] Side-channel Attack Standard Evaluation Board (SASEBO) Webpage，http://www.rcis.aist.go.jp/

[12] 浅井稔也，吉川雅弥，「ゲートレベル設計工程における電力解析耐性の脆弱性検証手法」，SCIS2012, 3C2-3, 2012

[13] 藤本大介，永田真，片下敏宏，佐々木明彦，堀洋平，佐藤証，「容量充電モデルを用いた高速なサイドチャネル攻撃評価手法」，SCIS2012, 1C2-6, 2012

[14] 森岡澄夫，佐藤証「共通鍵暗号 AES の低消費電力論理回路構成法」，情報処理学会論文誌，Vol.44, No.5, pp.1321-1328，2003.