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

AES暗号回路の設計・評価を効率的に行うサイドチャネル攻撃耐性検証法の一考察
Effective Evaluation Method for Designing AES Cryptographic Circuits with Resistance against Side Channel Attacks

伊藤 弘樹* 汐崎 充† 藤野 毅††
Hiroki Ito* Mitsuru Shiozaki† Takeshi Fujino††

あらまし 暗号回路動作時の消費電力波形を多量に取得して解析する Differential Power Analysis (DPA)などの電力解析攻撃に耐性を持つ耐タンパ暗号回路は数多く提案されてきた. このような耐タンパ暗号回路を設計する際，DPA 攻撃と同じように SPICE 等の回路シミュレータを用いて数十万～数百万の入力平文に対する消費電力波形を計算して，DPA 攻撃耐性評価を行っていては膨大な時間がかかり非現実的である．そこで，我々は使用波形数が少なく信頼性の高い攻撃耐性評価手法として Equivalent Byte Method (EBM)の提案をおこなってきた. この EBM では複数ある S-Box への入力データとラウンド鍵の値を特定値にすることで揃え，配線容量の不均一性等から生じる消費電力分布の偏りを少量の消費電力波形で抽出し，電力解析攻撃に対する耐性を十分に有しているかを評価する．本論文では，設計時の評価として消費電力解析ツールを用いた解析と，産業技術総合研究所が 130nm CMOS プロセスで試作したチップの測定に EBM を適用することで，消費電力のリーク要因を際立たせてサイドチャネル攻撃耐性検証時間が短縮できることを示し，EBM の有効性と実験結果に対する考察について報告する．

キーワード AES, サイドチャネル攻撃, SCA, 電力解析,DPA, Equivalent Byte Method, EBM

1 はじめに

近年，暗号回路動作中に生じる消費電力や漏洩電磁波などを利用し秘密情報を取得するサイドチャネル攻撃が脅威とされている．そのため，悪意を持つ攻撃者がサイドチャネル攻撃を利用し秘密情報を得ることが出来ないよう暗号モジュールに対策を施すことが急務となっている．中でも消費電力の均一化を図る「バランシング」を用いた Wave Dynamic Differential Logic (WDDL) [1]や，乱数を利用して消費電力を均一化する「乱数スイッチング手法」とバランシングを併用した Masked Dual-Rail Pre-charge Logic (MDPL) [2]，複数の独立した乱数を利用することですべての途中演算を隠すことが出来る独自の回路を AND 素子と置き換えた Masked And Operation (MAO) [3]，そして真の情報を分散して保持する秘密分散法の考えを取り入れることで出力時まで真の入力情報を隠す Threshold Implementation (TI) [4]の 4 種対策回路が引き合いに出されることが多い．この様な対策回路は設計段階でサイドチャネル攻撃耐性検証が必須であり, SPICE といった高精度回路シミュレータを利用して算出した消費電力情報を利用するのが良い. しかし，サイドチャネル攻撃耐性検証の一種である Differential Power Analysis (DPA) [5]などは一般的に数百万波形といった数多くの消費電力情報を統計的に解析するために，高精度回路シミュレータでは膨大な演算処理時間がかかり耐性検証は現実的に不可能となる．そのため，回路設計やレイアウト設計で，より少ない波形数で高信頼のサイドチャネル攻撃耐性検証を行えることが課題となる．また，ASIC や FPGA の実機を用いて測定した消費電力を利用する評価段階においても短時間でサイドチャネル攻撃耐性評価を行いたい要望は存在する. 我々は攻撃者（検証者）に有利な状況を作りだし，必要となる消費電力情報を削減して検証時間を短縮する Equivalent Byte Method (EBM) [6][7]を提案してきた.

* 立命館大学大学院理工学研究科, 滋賀県草津市野路東 1-1-1, Graduate School of Science and Technology Ritsumeikan University, Nojihigashi 1-1-1 Kusatsu Shiga 525-8577 Japan , ri001071@ed.ritsumei.ac.jp
† 立命館大学大学院総合理工学研究機構, 滋賀県草津市野路東 1-1-1, Research Organization of Science and Engineering Ritsumeikan University, Nojihigashi 1-1-1 Kusatsu Shiga 525-8577 Japan Address
†† 立命館大学理工学部, 滋賀県草津市野路東 1-1-1, Department of Science and Engineering Ritsumeikan University, Nojihigashi 1-1-1 Kusatsu Shiga 525-8577 Japan Address

本論文では EBM の有効性を示す為に入力パターンを変更して効果検証を行うと共に，消費電力測定ツール PrimeTime PX と実機測定を利用して取得した対策回路の消費電力を利用し一般的な検証方法との比較を行った．

続く第 2 章においては我々の提案する EBM の原理と効果検証を行い，第 3 章では PrimeTime PX と実測を利用して対策回路に EBM を適用した場合の評価を行っている．そして第 4 章でまとめと今後の課題について述べる．

2 Equivalent Byte Method (EBM)

一般的な電力解析攻撃を利用した検証よりも時間を大幅に短縮して攻撃耐性評価ができる Equivalent Byte Method（EBM)について説明する．そして，180nm CMOS プロセスにて作成した未対策テーブル AES 暗号回路を用いて EBM の効果検証を行う．

2.1 EBM とは

図 1 に示す AES 暗号回路における 10 ラウンド目を解析対象としてサイドチャネル攻撃耐性評価を行う場合を例にとり，EBM の適用方法を解説する．

EBM は Sub Bytes 処理に使用される S-Box 回路が図 1 のように複数個存在し並列処理される構造の AES 暗号回路に適用が可能である．

EBM の適用には以下 2 つの条件を使用する．

1. 10 ラウンド目の拡張鍵（Key10）へ，1byte 単位で同じ値を 16byte すべてに入力できるような，暗号鍵（Initial key）を設定する．

＜例＞ Key10 = (0x 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00)

2. 10 ラウンド目の入力値（R_in10）へ，1byte 単位で同じ値を 16byte すべてに入力できるような，平文（plain text）を設定する．

＜例＞ R_in10 = (0x E1 E1 E1 E1 E1 E1 E1 E1 E1 E1 E1 E1 E1 E1 E1 E1)

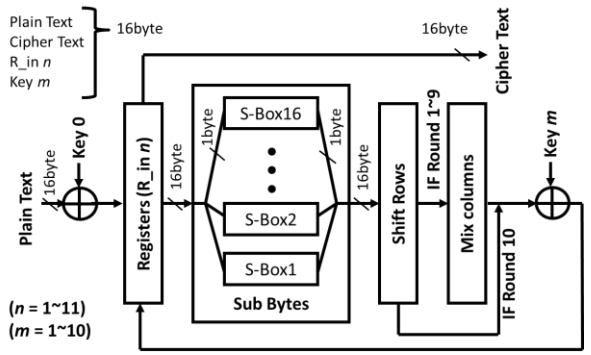


図 1. AES 暗号回路の構成

この 1，2 の条件を満たす平文と暗号鍵は図 2 のように，Key10 から 1～9 ラウンド目の拡張鍵（Key1~9）と暗号鍵を逆算し，更にこの鍵を用いて R_in10 から平文を逆算することで作成することが出来る．今回，10 ラウンド目に EBM を適用した例を示したが，すべてのラウンドに対して使用することが可能である．

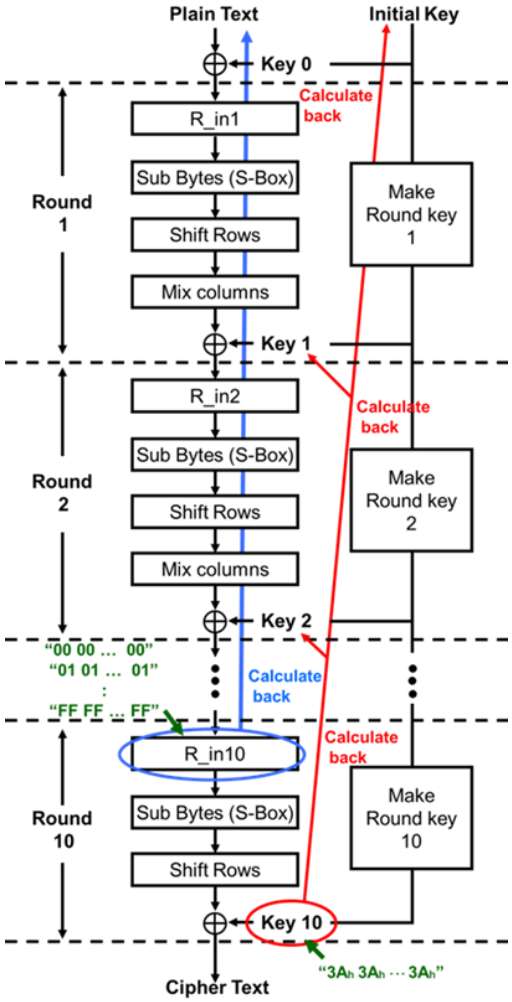


図 2. 平文と入力鍵の設定方法

2.2 EBM の原理

電力解析攻撃の一種である Hamming Weight DPA (HWDPA)を例に EBM の原理について述べる．

図 3 は AES 暗号回路の 10 ラウンド目に HWDPA を行う場合の模式図である．HWDPA ではラウンド 10 の開始時点でレジスタに格納されている値（R_in10）の HW を利用する．図 3 に記すように，既知の値である R_in11（cipher text と同等）と推定拡張鍵（Key10）を使って R_in10 の値を逆算する．そして，R_in10 の HW に応じて暗号処理時に発生した消費電力情報をグループ分けした後，平均消費電力差分を計算する．使用した拡張鍵と消費電力に相関があると，推定拡張鍵が正しいときに消費電力差分が最大となる．

我々の提案する EBM では信号の中間値に依存した遷移パターンにより暗号回路が生む消費電力分布に現れる偏りを明確にし，中間値と消費電力分布の相関を際立たせる事を目的としている．対策回路の多くは消費電力の

均一化を図って暗号鍵と消費電力の相関をなくすようにしているが，使用論理ゲートや配線容量に伴う遅延ばらつき等により，十分な攻撃耐性が実現できていないと指摘されているものも多い．我々の提案する EBM はそのようなレイアウトを含むタイミング情報の微少なばらつきなどが DPA 等のサイドチャネル攻撃に結びつかないかを評価する．

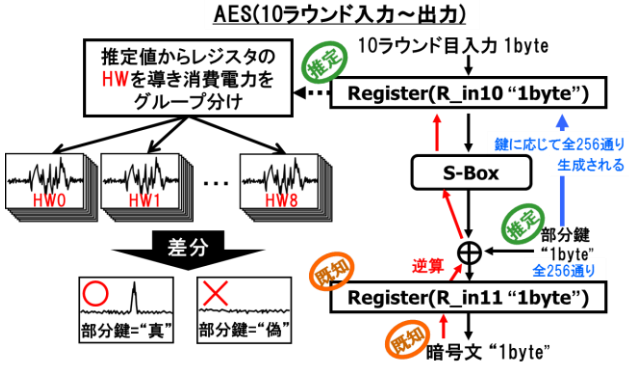


図 3. HWDPA の流れ

一般的なサイドチャネル攻撃を利用した検証より EBM を使った方が効率良くサイドチャネル攻撃に対する脆弱性を評価できる原理について説明する．ここでも簡単化のため 10 ラウンド目を例に説明する．サイドチャネル攻撃は key10 の全 16byte のうち 1byte に注目した攻撃が可能であり，鍵の推定に必要な試行回数を大幅に削減できるという点が大きな特徴である．

遷移パターンに応じた消費電力分布がサイドチャネル攻撃を可能する要因である事から，図 3 のように注目する 1byte に応じた消費電力を攻撃に利用することが理想的である．しかし，一般的に AES 暗号回路は全 16byte すべてを同時に処理を行っているため，必要部分以外の消費電力も同時に測定値に加算される．通常のサイドチャネル耐性検証において R_in10 は byte 毎に不規則な値が入力され key10 も任意の値が入力されため，注目部分とそれ以外の処理は全く無関係である．そのため，全く違う遷移パターンから生じる消費電力は別物となり同時に観測された時にはノイズとして作用する[8]．しかし，EBM ではすべての byte が R_in10 と key10 毎に等しいため，図 4 のように Byte1 から Byte16 までのすべての byte に応じた処理も遷移パターンが等しくなり，発生する消費電力が等しくなるので攻撃のターゲットとした鍵 byte 以外の消費電力がノイズにならない．そのため遷移パターンに応じた消費電力はパターン間の差異が非常に明確となる．よって解析効率が上昇すると共に，リーク要因の特定が容易になる．

2.3 効果検証

EBM の効果検証を行うためサイドチャネル攻撃標準評価ボード SASEBO-RII に搭載した 0.18nm CMOS プロセス未対策テーブル AES 暗号回路に対し①通常検証，

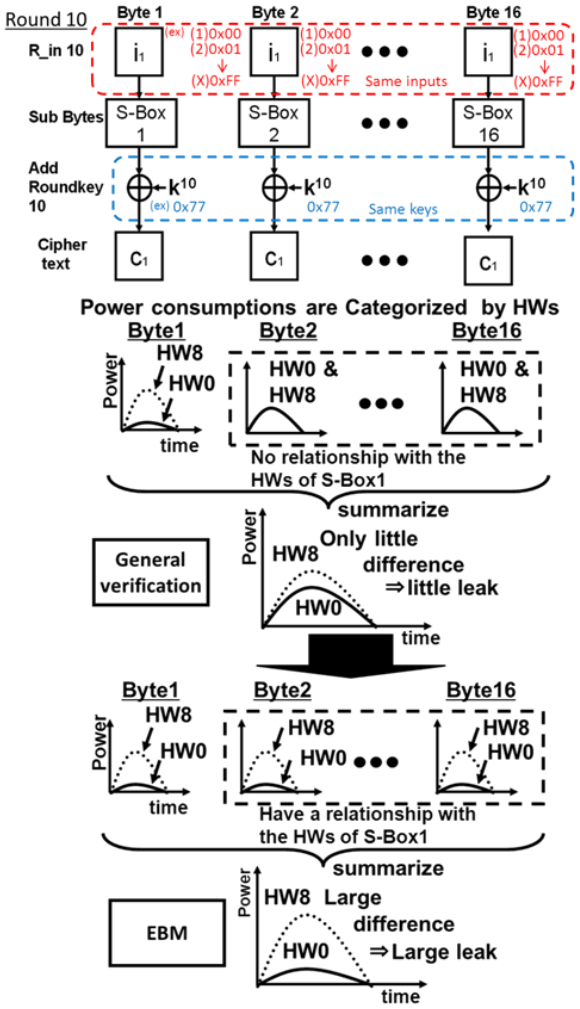


図 4. 遷移パターンに応じた消費電力の変化

②1byte 動作検証，③EBM の 3 種類で検証を行った．②1byte 動作検証は解析対象 byte に応じた消費電力のみをサイドチャネル攻撃に利用する場合を考えているが，今回は全 16byte が並列に動作するチップを利用しているため，注目する byte 以外をすべて毎回同一の値を入力することで疑似的に解析対象 byte のみの消費電力傾向を作り出した．それぞれの R_in10 と Key10 は下記のように設定した．

① 通常検証
R_in10：乱数値（平文を乱数により生成）
Key10 ：0x 13 11 1D 7F E3 94 4A 17 E3 07 A7 8B 4D 2B 30 C5

② 1byte 動作検証
R_in10：先頭の 1Byte 目のみ 0 ⇒ 255 までのカウントアップを繰り返し入力，それ以外は常に 0 を入力
Key10 ：0x 77 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63

③ EBM
R_in10：各 byte に同一な，0 ⇒ 255 までのカウントアップを繰り返し入力

Key10：0x 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77

それぞれ 1 万波形の消費電力を取得し，HW にてグループ分けを行った後に HW0 と HW8 の平均消費電力を比較した．消費電力測定には Agilent Technology のオシロスコープ DSO6104A（サンプリングレート 1GHz/s）を使用しており，実験結果として図 5 が得られた．

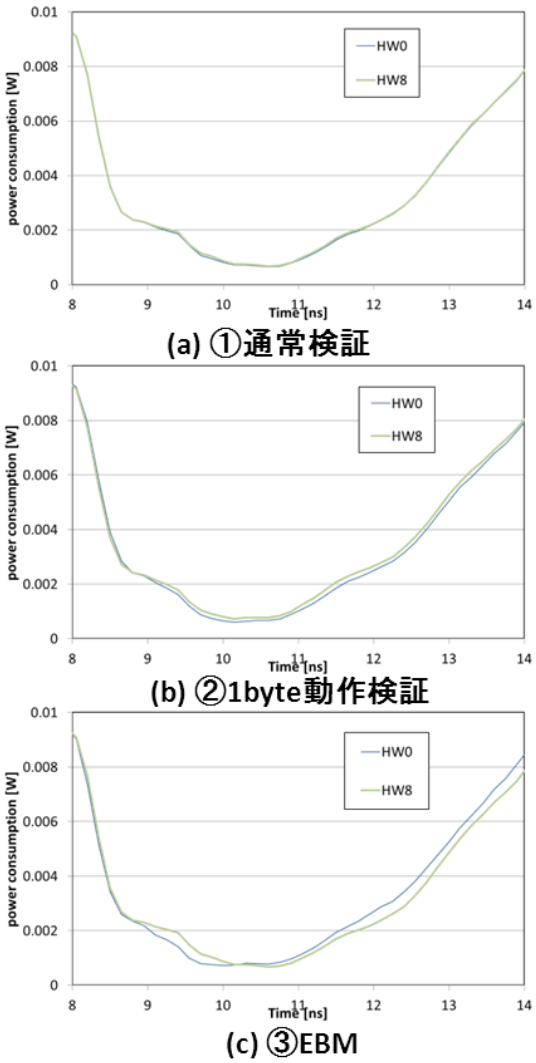


図 5. 各条件下での HW0 と HW8 の平均消費電力

リークの要因となる HW0 と HW8 の平均消費電力のズレが①通常検証<②1byte 動作検証<③EBM の順に大きくなっていることがわかる．これは①通常検証と②1byte 動作検証の間ではノイズ要因となっていた解析対象以外の Byte で生じる消費電力が一定になり見えなくなったことで出来た差であり，②1byte 動作検証と③EBM 間の差は動作を一定化することで見えなくなっていた byte における処理が解析対象と同傾向の消費電力を生み，それが積み重なることで作られたと考えることが可能である．このことから EBM が有効に動作していることが確認できた．

3　EBM を用いた対策回路検証

本章では SASEBO-RII [9]を利用した実機測定と Synopsys 提供の消費電力測定ツール PrimeTime PX を用いたシミュレーションを行い，通常検証と EBM 間で対策回路のサイドチャネル攻撃耐性検証にどの程度差が現れるか確認した結果を示す．加えて実機測定評価では暗号回路の入力パターンを変更した場合に検証効率に現れる結果の比較も行っている．また PrimeTime PX は比較的高速に暗号回路全体の消費電力測定が可能であることから設計段階で有効にサイドチャネル攻撃耐性を検証できるツールと考え評価を行った．

3.1　実機測定評価

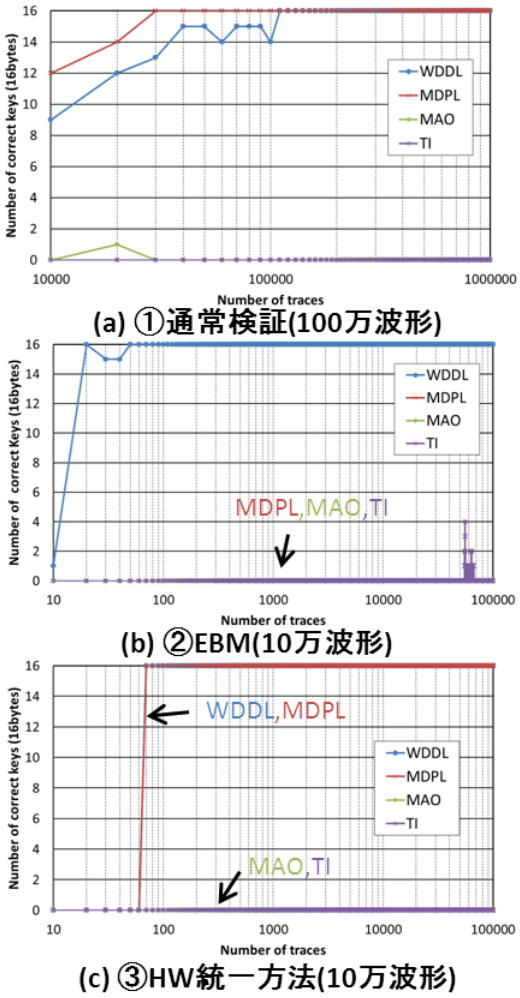
実機測定には SASEBO-RII に産業技術総合研究所提供の 130nmCMOS プロセスで作成した AES 暗号回路[10]を使用した．チップの仕様上，一部暗号鍵の変更が出来ないため EBM 使用時に Key10 を byte 毎に同一とすることが出来ないが，消費電力を HW でグルーピングする攻撃のみを使用している事と Key10 との EXOR 処理以降に非線形素子が存在していない事から処理内容に応じた消費電力差がほぼ無く影響はほとんど無いと考えられる．

EBM の有効性を示す為に検証方法として通常検証，EBM に加え入力 HW 統一方法を加えた 3 パターンを利用した．各種条件は以下の通りである．

①通常検証（100 万波形取得）
R_in10：R_in10：乱数値（平文を乱数により生成）
②EBM（10 万波形取得）
R_in10：各 byte に同一な，0 ⇒ 255 までのカウントアップを繰り返し入力
③HW 統一方法
R_in10：同一平文中で各 Byte に HW の大きさが等しい値を HW0 → HW1 → … → HW8 → HW0 …の繰り返しで入力する．なお数値はランダムで選択される．
<例> HW2 の入力
R_in10 = 0x 50 0C 14 A0 30 22 81 09 0C 12 05 48 60 81 41 60

＊10 ラウンド目の拡張鍵は全条件において同一である．
Key10　：0x 13 11 1D 7F E3 94 4A 17 E3 07 A7 8B 4D 2B 30 C5

耐性検証には攻撃として HWCPA と HW0 と HW1～HW8 の平均電力差分を利用する Zero-Value DPA（ZVDPA）[11]の 2 種類の電力解析攻撃を用いた．HWCPA 利用した検証結果が図 6 であり，ZVDPA を利用した結果が図 7 である．また検証結果のまとめを表 1 に示す．

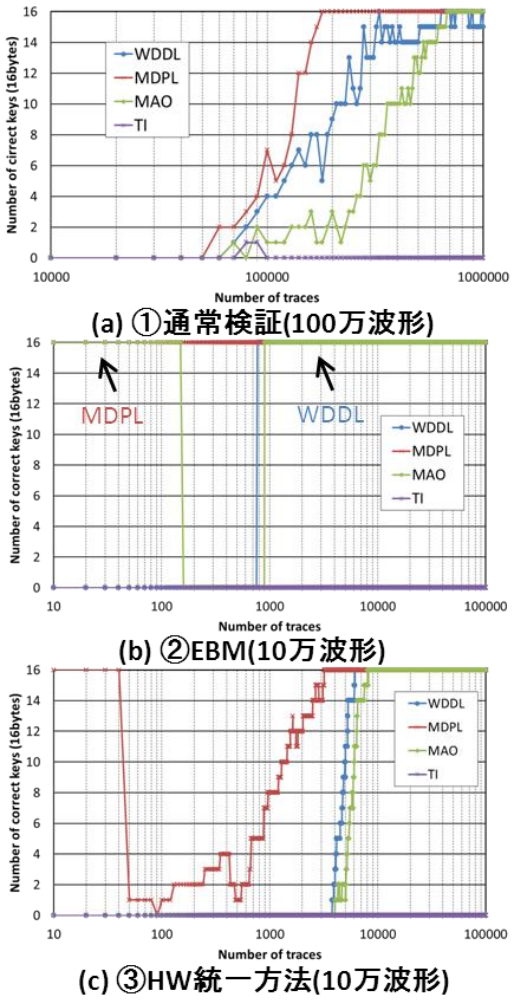


(a) ①通常検証(100万波形)

(b) ②EBM(10万波形)

(c) ③HW統一方法(10万波形)

図 6. 対策回路に対する HWCPA



(a) ①通常検証(100万波形)

(b) ②EBM(10万波形)

(c) ③HW統一方法(10万波形)

図 7. 対策回路に対する ZVDPA

まず①通常検証と②EBM の比較を行う．HWCPA において通常検証では 11 万波形使用時点で WDDL，3 万波形使用時点で MDPL のすべての鍵を解析することが可能であったが，EBM を使用すると WDDL，MDPL どちらも 70 波形使用時点ですべての鍵を解析出来た．また ZVDPA については 100 万波形使用時点で WDDL の Key10 を 15byte 解析し，MDPL，MAO ではそれぞれ 18 万波形使用時点，68 万波形使用時点で全 16byte の鍵を特定することが可能であった．そして EBM を使用すると，WDDL では 770 波形使用時点，MDPL では 10 波形使用時点，MAO では 900 波形使用時点ですべての鍵を解析することが出来た．このように EBM は通常検証に比べ格段に効率的に耐性検証が可能であることが確認できたと共に，リーク要因を発生させていないであろう TI を妥当に評価できていると考えられる．

次に R_in10 にすべての Byte で同一の入力を与える事の有効性について検討を行うため EBM と HW 統一方法の比較をする．表 1 より WDDL に対する HWCPA 以外は EBM が HW 統一方法に比べ効率的であることが確認できる．また TI の解析はどちらの方法でも解析は不可能であった．このことから R_in10 に byte 毎に HW を

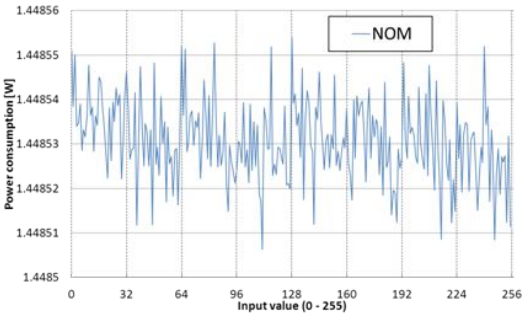
表 1. 対策回路に対する解析結果

Counter measure	通常検証		EBM		HW統一方式	
	HWCPA	ZVDPA	HWCPA	ZVDPA	HWCPA	ZVDPA
WDDL	110000	1000000 (15keys)	70	770	50	6130
MDPL	30000	180000	70	10	FALSE	3190
MAO	FALSE	680000	FALSE	900	FALSE	8150
TI	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

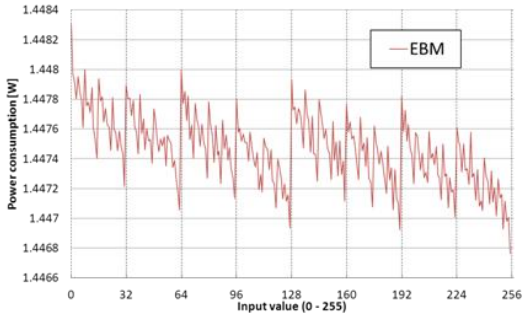
・FALSE : Cannot reveal any key.
・**Keys : the number of reveal keys using one million traces

そろえた入力を入れるよりも，すべての byte に対して同一値を入力することの有効性が確認できた．これは HW が同一であるといえど内部処理において違いが生まれるため，全く同一の値を入力する EBM はロスが少ないことが原因であると考えられる．

最後に EBM が対策回路においてもより効果的にリークを拾うことが出来た原因を確認するために，時間軸に対し HWCPA 利用時に最も高い相関値が表れる一点において，入力値に応じた平均消費電力を算出する．図 8 に WDDL に対し通常方式と EBM 使用時の入力値別平均消費電力を示す．入力値の振り分けには拡張鍵の初めの 1byte 目（Byte1 対象）を利用している．

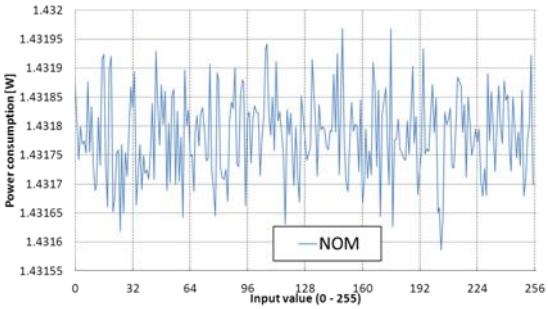


(a) ①通常検証(100万波形)

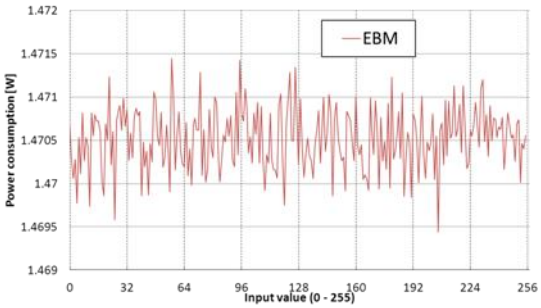


(b) ②EBM(10万波形)

図 8. WDDL における入力別消費電力



(a) ①通常検証(100万波形)



(b) ②EBM(10万波形)

図 9. TI における入力別消費電力

通常検証を見ると 0 から 255 までを 8 分割するとすべての区間で右肩下がりになっている傾向が確認できる．これが EBM になると明確に右肩下がりの特徴を抽出出来ていることが確認できる．また同様に MDPL，MAO においても入力の傾向を強調していることが確認できた．しかし図 9 に示す TI における入力値別消費電力については通常方式と EBM で同一の傾向はなく，測定毎に消費電力傾向が変化し，サイドチャネル攻撃の要因となるリークは確認できなかった．このことから対策回路においても解析可能なものに対しては EBM の原理が適用され，耐性検証の効率化が可能であることがわかった．一方で解析不可能なものについては特徴をもったリーク要因が存在していないことも確認できた．

3.2 PrimeTime PX を利用した評価

PrimeTime PX を利用したシミュレーションでは WDDL と MDPL の耐性検証を行った．シミュレーションには論理合成のみを施したネットリストを使用し，ネットの遅延情報を含む sdf ファイルは利用していない．耐性評価には以下の２つの条件で AES 暗号回路を動作させ得られた消費電力波形に対し HWCPA，ZVDPA を使用している．

①通常検証（10 万波形取得）
R_in10：乱数値（平文を乱数により生成）
Key10 ：0x 77 02 22 DD 19 F0 01 E8 52 9C 5E 72 40 6E 3A A1
②EBM（WDDL：256 波形，MDPL：1 万波形 取得）
R_in10：各 byte に同一な，0 ⇒ 255 までのカウントアップを繰り返し入力
Key10：0x 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77

WDDL に対し耐性評価を行い HWCPA と ZVDPA の攻撃結果として図 10 が，時間軸に対する HW 別の平均消費電力通常検証では 10 万波形，EBM では 256 波形を使用し図 11 が得られた．

まず WDDL はシミュレーション利用時に EBM を使用する利点がある．EBM は入力が全 256 パターンのため乱数による対策方法を有していない，よって WDDL においてはシミュレーションを 256 波形で消費電力パターンを網羅することが可能である．さらに通常検証では 10 万波形を利用しても HWCPA，ZVDPA で Key10 の解析が全くできなかった結果に対し，EBM では HWCPA で 30 波形，ZVDPA で 10 波形使用時点にすべての鍵が解析可能であることが確認できる．また図 11 をみると通常検証側では多少しか確認できなかった HW0 と他の HW とのズレが EBM では明確に確認できるようになっている．シミュレーションにおいてネットの遅延情報を利用していないため，今回のズレが生じた原因は AND ゲートと OR ゲート間の伝達スピードの違いにより生まれたと考えられる．このことから正確に配置配線を行い「バランシング」を成立させても論理素子自体の伝達速度差からリークが生まれ，サイドチャネル攻撃が可能であると考えられる．

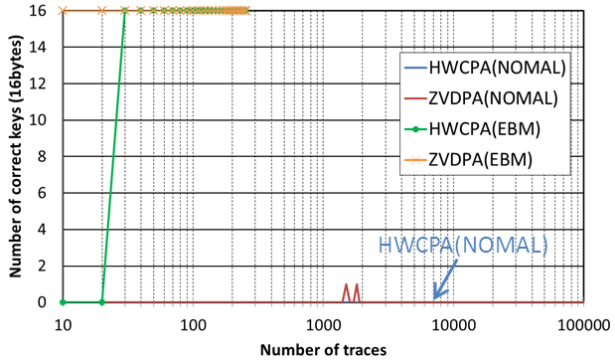


図 10. WDDL に対する HWCPA と ZVDPA

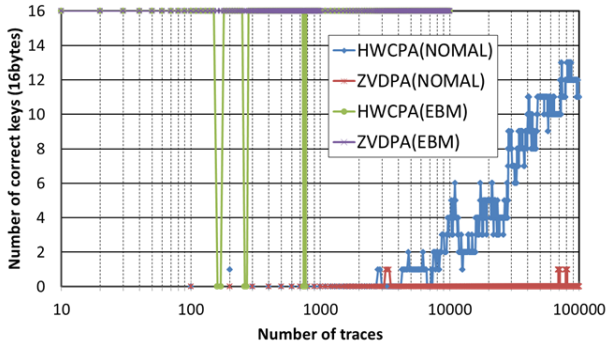


図 12. MDPL に対する HWCPA と ZVDPA

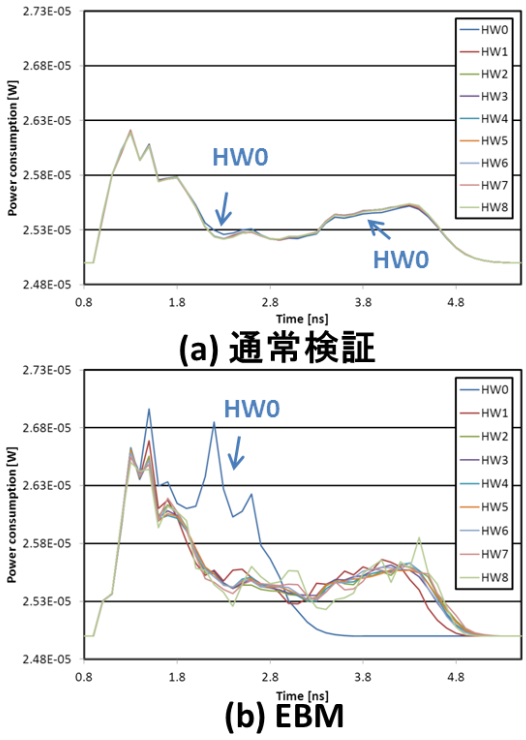


図 11. WDDL における時間軸に対する HW 別消費電力

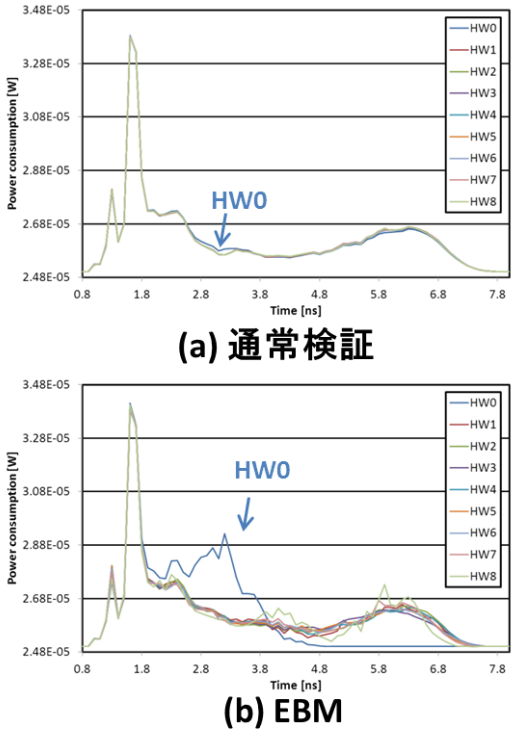


図 13. MDPL における時間軸に対する HW 別消費電力

次に MDPL の耐性検証を行った．MDPL は対策方法として「乱数スイッチング」を利用している為，消費電力の全パターンを網羅したことを確認することはできない，よって今回は EBM 条件で 1 万波形を取得した．HWCPA と ZVDPA の攻撃結果として図 12 が，時間軸に対する HW 別の平均消費電力通常検証では 10 万波形，EBM では 1 万波形を使用し図 13 が得られた．

通常検証と EBM 使用時の HWCPA，ZVDPA 結果を比較すると，通常検証では 10 万波形利用しても全 16byte 中 11byte しか解析できなかった結果に比べて EBM 利用時には 780 波形で Key10 すべての byte を解析可能であった．また ZVDPA においては通常検証 10 万波形使用でまったく鍵解析が出来なかったが，EBM では 10 波形で全鍵の解析が可能であった．図 12 を見ても WDDL と同様に HW0 とその他の HW とのズレが非常に大きく明確になっていることが確認できるので，攻撃効率が大幅に上がっていることが確認できる．MDPL においても HW0 における AND 論理や OR 論理の伝達スピードがどちらも他の HW グループより速いため「乱数スイッチング」で論理の入れ替えを行ってもリークが生じると考えられる．

PrimeTime PX を利用した解析結果をまとめた表 2 を見ると，明らかに EBM を利用した評価が効率的であることが確認できる．

今回のシミュレーションで WDDL の消費電力 1 万波形の取得には合計で 5 時間程度が必要となっている，また MDPL においては更に回路規模が大きいため倍以上の時間が必要である．つまり 10 万波形を取得するために 50 時間以上用いて出来なかった評価を 10 数分程度で可能となることがわかった．

表 2. PrimeTime PX を利用した対策回路解析結果

Counter measures	通常検証		EBM	
	HWCPA	ZVDPA	HWCPA	ZVDPA
WDDL	FALSE	FALSE	10	30
MDPL	FALSE	100000 (11keys)	10	780

・FALSE : Cannot reveal any key.
・**Keys : the number of reveal keys using one million traces

4　まとめと今後の展望

本論文では耐タンパ暗号回路の設計・評価時点で必須のサイドチャネル攻撃耐性検証のうち，特に AES 暗号回路全体を動作させて行う検証方法の期間を短縮化する手法である Equivalent Byte Method の有効性を確認した．実機測定では各種対策回路の消費電力傾向を際立たせることでリークを効率的に捉え，少なくとも 400 倍の効率化に成功した．また PrimeTime PX を利用したシミュレーションでも同様にリークを明確にし，効率化を図ると共にリーク要因の検討にも利用が可能であることを確認した．

今後の課題として，EBM の利用できる検証環境の確認を行うと共に，各環境において検証に必要な波形数変化をパラメータ化することでサイドチャネル攻撃耐性評価の基準化を行いたいと考えている．

謝辞　本研究は JST，CREST「ディペンダブル VLSI システムの基盤技術」における研究の一環として行なわれた．またチップ試作は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，ローム（株）の協力で行われた．SASEBO-RII を用いたサイドチャネル攻撃環境の情報提供には産総研情報セキュリティ研究センター佐藤証様，片下敏宏様にご協力を頂いた．関係各位に感謝いたします．

参考文献

[1] K. Tiri, I. Verbauwhede, ”A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation,” DATE’04, vol.1, pp.10246-10251, 2004.

[2] T. pop, S. Mangard, “Masked Dual-Rail Precharge Logic：DPA-Resistance Without Routing Constrain,” CHES2005, LNCS3659, pp.172-186, Springer-Verlag, 2005

[3] E. Trichina, “Combinational Logic Design for AES SubByte Transformation On masked Data,” Cryptology ePrint Archive, 2003/236, 2003.

[4] S. Nikova and C. Rechberger, and V. Rijmen, “Threshold Implementations Against Side-Channel Attacks and Glitches,” The 8th International Conference on Information and Communications Security (ICICS 2006), LNCS4307, pp. 529-545, Springer-Verlag, Dec. 2006.

[5] P. Kocher, J. Jaffe, B. Jun, “Differential Power Analysis,” In M. Wiener, editor, Advances in Cryptology CRYPTO’99, vol.1666 of Lecture Notes in Computer Science, pp.388-397, Berlin, Heidelberg.

[6] 伊藤弘樹，汐崎充，A. Hoang，藤野毅，“AES 暗号回路における耐タンパ性検証効率化手法の検討，”暗号と情報セキュリティシンポジウム 2012 （SCIS2012），3C1-6，2012.

[7] H. Ito, M. Shiozaki, A. Hoang and T. Fujino, “Efficient DPA-Resistance Verification Method with Smaller Number of Power Traces on AES Cryptographic Circuit,” DSD2012, DOI 10.1109, pp.735-738, Izmir, Turkey, 2012.

[8] K. Tiri, I. Verbauwhede, “A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation,” DATE’04, vol.1, pp.10246-10251, 2004.

[9] Side-channel Attack Standard Evaluation Board http://www.morita-tech.co.jp/SAKURA/en/index.html

[10] 産業総合研究所 RCIS　Crypto LSI http://www.rcis.aist.go.jp/special/SASEBO/CryptoLSI-ja.html

[11] Goli´c, J.D., Tymen, C.: Multiplicative Masking and Power Analysis of AES. In: Kaliski Jr., B.S., Ko¸c, C¸ .K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp.198–212. Springer, Heidelberg, 2003.