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

電力・電磁波解析攻撃におけるオンチップ・キャパシタの影響評価
Evaluation of On-chip Capacitor's effect on Power/Electromagnetic Analysis Attacks

中井 綱人* Tsunato Nakai　　汐崎 充† Mitsuru Shiozaki　　藤野 毅* Takeshi Fujino

あらまし 暗号回路の動作時に発生する消費電力や漏洩電磁波を用いることで，その暗号デバイスの秘密鍵情報を窃取するサイドチャネル攻撃の脅威が報告されている．ボード上に実装したデカップリングキャパシタは，サイドチャネル攻撃の一種である電力解析攻撃に対する防御対策となると報告されているが，チップ外に取り付けられたキャパシタは取り外し可能であり，抜本的な攻撃防止対策とはならない．そこで，チップ内に意図的に大容量のデカップリングキャパシタ（オンチップ・キャパシタ）を実装した AES 暗号チップと，回路レイアウトは全く同一であるがオンチップ・キャパシタを実装していない AES 暗号チップを試作し，電力解析攻撃と電磁波解析攻撃を各チップに行ってオンチップ・キャパシタが与える影響を実測評価した．その結果，電力解析攻撃ではハミングディスタンス型の CPA 攻撃が有効であり，オンチップ・キャパシタ付きチップでは攻撃に必要な波形数が増加していることから，攻撃耐性は向上していることが確認できた．一方，電磁波解析攻撃ではハミングウェイト型の CEMA 攻撃が有効であり，電力解析攻撃の場合とは逆にオンチップ・キャパシタ付きチップの方がより少ない波形数で攻撃できることがわかった．電磁波解析攻撃に関しては，プローブの種類や位置依存性も含めて実験を行ったので，評価結果と考察について報告する．

キーワード サイドチャネル攻撃，電力解析，電磁波解析，AES，CPA，CEMA，

1 はじめに

近年，暗号アルゴリズムは理論的に安全であっても，暗号デバイスの動作時に発生する消費電力や漏洩電磁波といった二次的情報を用いて，その暗号回路の秘密鍵情報を窃取するサイドチャネル攻撃が脅威とされている．サイドチャネル攻撃の一種である電力解析攻撃は 1999 年に Kocher らにより提案され，暗号回路内部のノード情報はその動作時に発生する消費電力との相関があることに着目した攻撃手法である[1]．電力解析攻撃は，攻撃性能の高さに加えてオシロスコープやパソコンといった比較的導入コストが安価な装置で容易に行えるため，危険性が指摘されている．また，電磁波解析攻撃は，2001 年に Grandolfi らにより提案され，暗号回路内部のノード情報はその動作時に発生する漏洩電磁波との相関があることに着目した攻撃手法である[2]．電磁波は，アンペールの法則から電流の周囲に発生し，その大きさは電流とその電流からの距離で決められる．つまり，測定位置が一定なら電流の大きさを見られることから，電力解析攻撃と同じように攻撃が可能である．電磁波解析攻撃は，測定位置が自由であるため暗号処理部近傍での攻撃ができると危惧されているが，一般的に電力解析攻撃と同じ対策で十分だと考えられてきた．

電力解析攻撃に対する対策として，内部情報と消費電力との相関を低減するデカップリングキャパシタを用いた対策が効果的であると報告されている[3]．しかし，この対策は，チップ外にデカップリングキャパシタを搭載することから，取り外しが可能であり根本的な対策になっていないのが現状である．そこで，取り外し出来ないように，チップ内に大量のデカップリングキャパシタを意図的に搭載したオンチップ・キャパシタ付き AES 暗号回路を試作した．そして，試作したオンチップ・キャパシタ付き AES 暗号回路に対して，電力・電磁波解析攻撃を行い，オンチップ・キャパシタの与える影響につ

* 立命館大学理工学部，〒525-8577，滋賀県草津市野路東 1-1-1，Department of Science and Engineering Ritsumeikan University, 1-1-1 Nojihigashi, Kusatsu, Shiga, Japan, {ri0004pk@ed, fujino@se}.ritsumei.ac.jp
† 立命館大学大学院総合理工学研究機構，〒525-8577，滋賀県草津市野路東 1-1-1，Research Organization of Science and Engineering, Ritsumeikan University, 1-1-1 Nojihigashi, Kusatsu, Shiga, Japan, mshio@fc.ritsumei.ac.jp

いて評価した．その結果，電磁波解析攻撃は電力解析攻撃とは異なる攻撃結果が得られた．本論文では，電磁界プローブの種類やプローブ位置[4,5]に関する検討も加えた実測評価結果と考察を報告する．

本論文の構成は以下の通りである．第2章では試作したオンチップ･キャパシタ AES 暗号回路について述べ，第3章では攻撃評価手法と実験環境について述べる．そして，第4章でオンチップ・キャパシタが電力・電磁波解析攻撃に与える影響について実測評価した結果を示す．第5章では電磁波解析攻撃について電磁界プローブ位置の依存性や電磁界プローブの種類による効果について報告する．最後に，第6章ではまとめと今後の課題を述べる．

2　オンチップ･キャパシタ付き AES 暗号回路

本稿で評価するチップは，180nm CMOS プロセスで設計・試作した AES 暗号回路である（図1参照）．試作チップには Sbox をテーブル方式で実装した未対策 AES 暗号回路と，合成体方式で実装した AES 暗号回路が搭載されている．図2のレイアウト図に各回路がどこに配置されたかを示す．テーブル方式の AES 暗号回路はチップ左上に配置され，合成体方式の AES 暗号回路がチップ右下に配置されているのがわかる．特に，今回評価する暗号化処理回路（ENC）はチップの角に配置されている．

この未対策 AES 暗号チップと全く同じレイアウトを使用し，大量のデカップリングキャパシタを意図的に搭載した AES チップも試作した．今後，この回路をオンチップ・キャパシタ付き AES 暗号回路と呼ぶ．未対策 AES チップとオンチップ・キャパシタ付き AES チップの変更点は，フィラーセルを MOS 容量付きフィラーセルに置き換えたことと，IO セルと回路を囲っている電源グランドとの間に MOS 容量を挿入した点である．全て合わせておよそ 1nF の容量が付く見積りである．

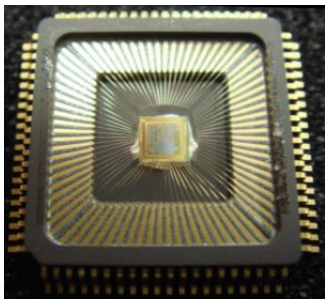

図1　試作した AES 暗号チップ写真

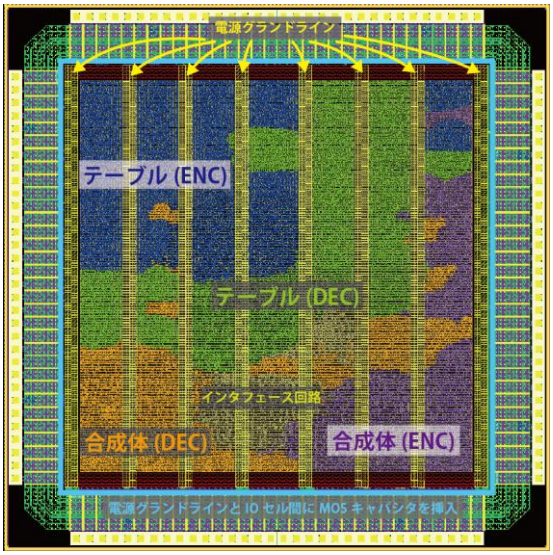

図2　試作 AES 暗号チップのレイアウト図

3　攻撃評価手法と実験環境

本章では試作した未対策 AES 暗号回路とオンチップ・キャパシタ付き AES 暗号回路に対して行った攻撃手法と攻撃評価を行った実験環境についてまとめる．

3.1　攻撃評価手法

未対策 AES 暗号回路とオンチップ・キャパシタ付き AES 暗号回路に行う電力解析攻撃手法として消費電力と内部状態の相関係数を用いて秘密鍵情報を解析する相関電力解析（Correlation Power Analysis：CPA）[6]を，電磁波解析攻撃手法として相関電磁波解析（Correlation Electromagnetic Analysis：CEMA）を用いて評価した．攻撃ラウンドは最終 10 ラウンド目，使用波形数は 1 万とした（図3参照）．評価に使用した CPA と CEMA は，Sbox 回路の入力値"1"のビット数を見るハミングウェイト型（HW）とレジスタのビット遷移数を見るハミングディスタンス型（HD）についてそれぞれ評価しており，これ以降 HW/HD-CPA，HW/HD-CEMA と記載する．

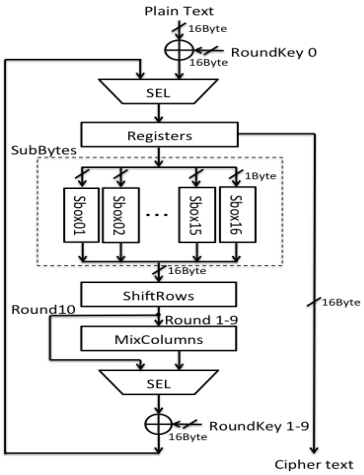

図3　AES 回路の構成

3.2 攻撃評価環境

攻撃評価を行った実験環境についてまとめる．電力解析攻撃と電磁波解析攻撃共にサイドチャネル攻撃標準評価基板 SASEBO-RII [7]を使用，オシロスコープは Agilent 社 DSO9104A を使用した．サンプリングレート 20GSa/s，帯域幅 1GHz である．電力解析攻撃はグランド側の消費電力波形を測定して行った．電磁波解析攻撃には森田テック社の EMC スキャナ WM7400，電磁界プローブとして水平円形コイル型の HC010 及び HC020 と垂直扁平コイル型の VF010，アンプとしてゲイン 50dB，周波数レンジ 10-1000MHz の LNA- 1050 を使用した．電磁波解析攻撃を行った実験環境を図 4 に示す．使用した各電磁界プローブの測定分解能は，それぞれ HC010 が 0.35mm，HC020 が 0.55mm，VF010 が 0.10mm である．以上の実験環境を表 1 にまとめて示す．

表 1　攻撃評価の環境

オシロスコープ	Agilent DSO9104A			
	サンプリングレート	20GSa/s		
	帯域幅	1GHz		
電力解析攻撃	グランド側			
電磁波解析攻撃	EMCスキャナ	WM7400		
	電磁界プローブ			
	コイル形状	水平円形コイル		垂直扁平コイル
		HC010	HC020	VF010
	分解能	0.35mm	0.55mm	0.10mm
	アンプ(LNA-1050)			
	周波数範囲.	10-1000MHz		
	ゲイン	50dB		

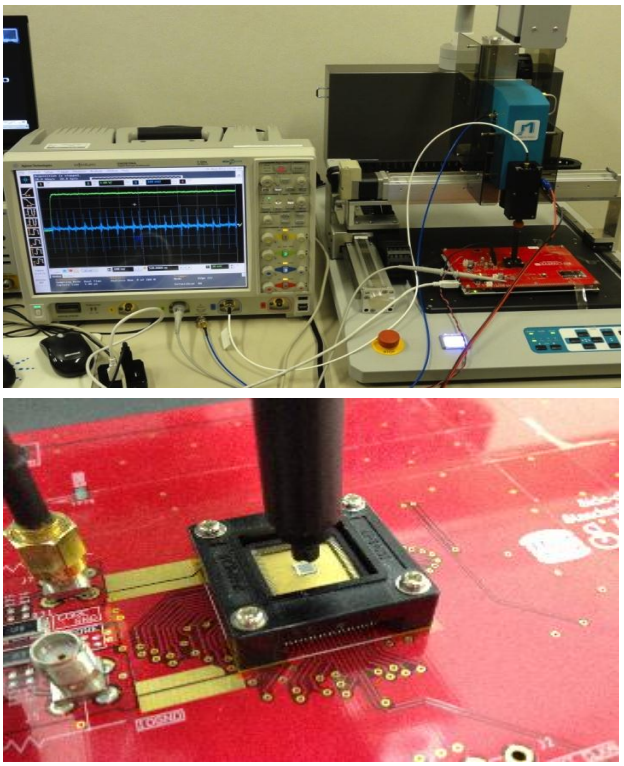

図 4　電磁波解析攻撃の実験環境

4　オンチップ・キャパシタが電力・電磁波解析攻撃に与える影響

本章では未対策 AES 暗号回路とオンチップ・キャパシタ付き AES 暗号回路に電力解析攻撃及び電磁波解析攻撃を行った結果について述べる．

4.1 オンチップ・キャパシタと電力解析攻撃

電力解析攻撃における未対策 AES 暗号回路とオンチップ･キャパシタ付き AES 暗号回路の評価結果を示す．はじめに，実測した電力波形を図 5 と図 6 に示す．図 5 が未対策 AES 暗号回路（キャパシタ無し）の実測波形で，図 6 がオンチップ・キャパシタ付き AES 暗号回路の実測波形である．Sbox の実装方式は共に合成体方式である．未対策 AES 暗号回路と比較すると，オンチップ・キャパシタ付き AES 暗号回路の消費電力波形は平滑化されており，キャパシタを追加した効果が明らかに見て取れる．

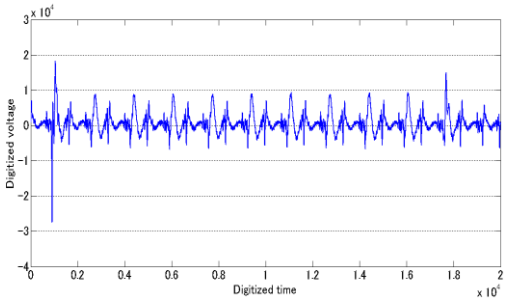

図 5　未対策 AES（キャパシタ無し）の実測波形

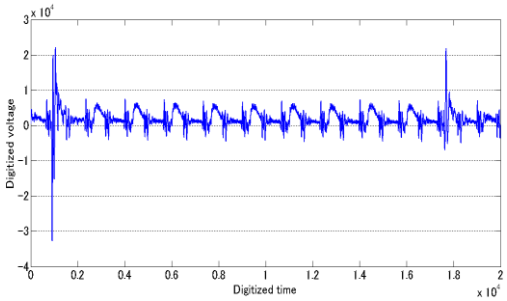

図 6　オンチップ・キャパシタ付き AES の実測波形

HW/HD-CPA を行った結果を図 7 と図 8 に示す．図 7 は未対策 AES 暗号回路（キャパシタ無し）における CPA 攻撃結果で，図 8 はオンチップ・キャパシタ付き AES 暗号回路における CPA 攻撃結果である．各 CPA 攻撃結果は 1 万波形で解析できた部分鍵の数の遷移を示しており，縦軸は解析できた部分鍵の数（全 16Byte），横軸は解析に用いた波形数（最大 1 万波形）である．ここで，TBL はテーブル方式実装，CMP は合成体方式実装を意味する．

図 7 から，キャパシタ無しの場合，テーブル方式は 1,000 波形程度で HD-CPA により全ての秘密鍵が判明することがわかる．合成体方式もテーブル方式には劣るが 5,000 波形程度で HD-CPA により全鍵が判明している．HW 型の攻撃は両実装方式とも HD 型ほどの効果が無く，鍵解析により多くの波形数を必要としていることがわかる．図 8 から，オンチップ・キャパシタを挿入することにより全ての攻撃において鍵解析に必要な波形数が増えており，オンチップ・キャパシタの効果により攻撃が難しくなっていることが明らかにわかる．このことから，電力解析攻撃に対してデカップリングキャパシタは多少なりとも対策になっている．

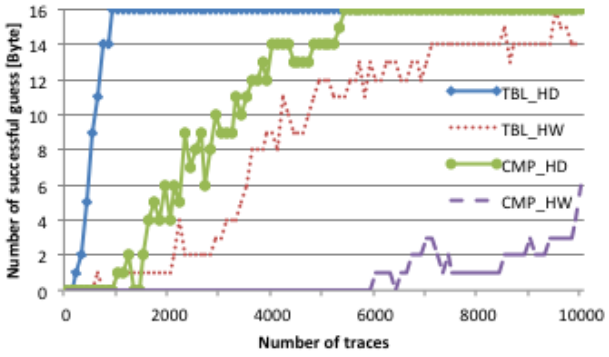

図 7　未対策 AES（キャパシタ無し）の CPA 攻撃結果

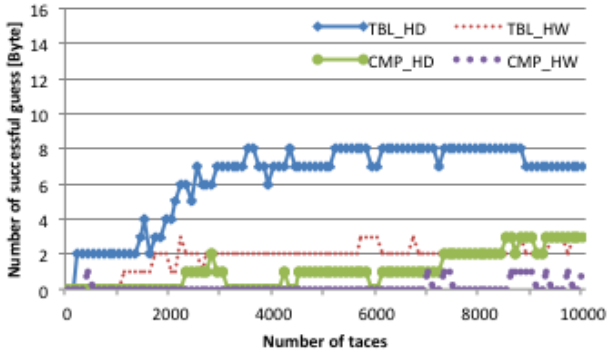

図 8　オンチップ・キャパシタ付き AES の CPA 攻撃結果

4.2 オンチップ・キャパシタと電磁波解析攻撃

次に，電磁波解析攻撃におけるオンチップ・キャパシタの効果を調べた結果を示す．測定条件を合わせるため，電磁界プローブには水平円形コイル型 HC020 を使用，電磁界プローブ位置をチップ中心に設定して測定を行った．1 万波形で解析できた部分鍵の数の遷移を図 9，図 10 に示す．図 9 は未対策 AES 暗号回路（キャパシタ無し）における CEMA 攻撃結果で，図 10 はオンチップ・キャパシタ付き AES 暗号回路における CEMA 攻撃結果である．

図 9 から，未対策のテーブル方式 AES は 1 万波形で HD-CEMA により 11 バイト，HW-CEMA により 6 バイトの部分鍵が解明された．未対策の合成体方式 AES は 1 万波形で HD-CEMA により 4 バイト，HW-CEMA により 3 バイトの部分鍵が判明した．

一方で，オンチップ・キャパシタ付きのテーブル方式 AES では 1 万波形で HD-CEMA により 11 バイトと未対策と変わらなかったのに対して，HW-CEMA では 5,000 波形で 16 バイト全ての秘密鍵が解明された．合成体方式 AES に関しても HD-CEMA により 1 バイトと減少しているのに対して，HW-CEMA では 1 万波形で 6 バイトと解析された部分鍵の数が増えている．

以上の結果より，電磁波解析攻撃では，デカップリングキャパシタにより HD 型の攻撃は変わらない，もしくは攻撃困難になっているのに対して，HW 型の攻撃はデカップリングキャパシタを挿入した方が攻撃しやすくなっていると言える．特に，注目すべきは 1 バイトの部分鍵が判明するのに必要な波形数である．HW 型の攻撃は電力解析攻撃と比較しても少ない波形数で鍵解析ができており，測定箇所によって非常に脅威となると考えられる．そこで，次の 5 章では電磁界プローブの位置依存性と電磁界プローブの差異に関して電磁波解析攻撃の追加実験を行った結果について報告する．

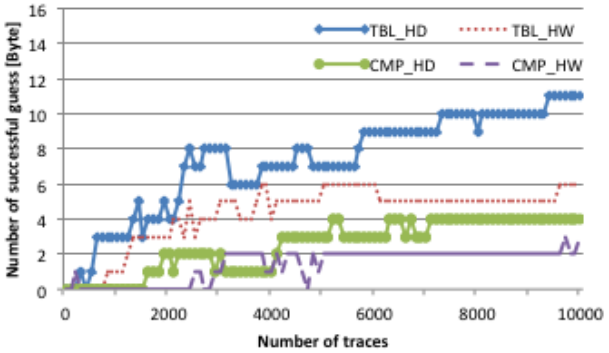

図 9　未対策 AES（キャパシタ無し）の CEMA 攻撃結果

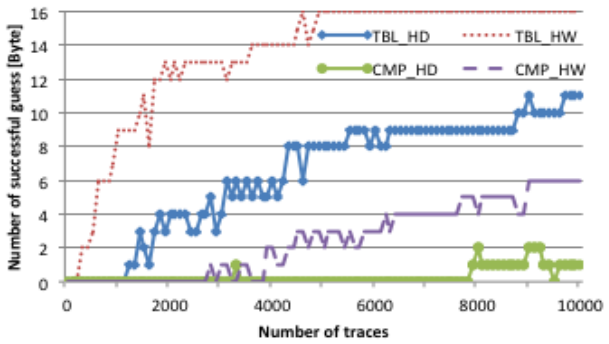

図 10　オンチップ・キャパシタ付き AES の CEMA 攻撃結果

5　電磁波解析攻撃における電磁界プローブとプローブ位置の効果

本章では，電磁波解析攻撃の特性を調べるために，電磁界プローブの測定位置と電磁界プローブの種類によって攻撃結果に与える影響を示す．

5.1　電磁界プローブの位置依存効果

まず，電磁界プローブ位置の関係性を調べた．実験には，未対策 AES 暗号回路に対して水平円形コイル型 HC020 を使用して行った．測定位置は図 11 に示す 4 カ所で測定を行い，比較評価を行った．

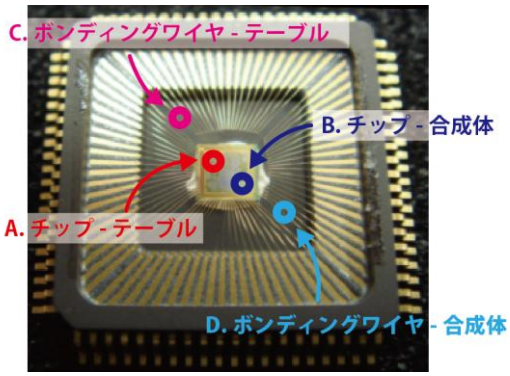

図 11　測定位置

テーブル方式 AES が集中している位置 A（チップ－テーブル）での CEMA 攻撃結果を図 12，合成体方式 AES が集中している位置 B（チップ－合成体）での CEMA 攻撃結果を図 13 に示す．位置 A ではテーブル方式が 5,000 波形で HD-CEMA により全ての鍵が解明し，容易に攻撃できているが，合成体方式は攻撃困難である．逆に，位置 B ではテーブル方式が攻撃困難であるのに対して，合成体方式が 2,000 波形で HD-CEMA により全ての鍵が判明している．

チップ中心位置での CEMA 攻撃結果（図 9）と比較すると明らかに HD 型の攻撃効率が上がっている．そこで，AES 暗号回路の中でもラウンドレジスタが，どこに配置されているのかを調べた．ラウンドレジスタの配置場所を示したレイアウト図を図 14 に示す．今回測定した位置Aと位置Bはおよそラウンドレジスタの直上であるため，レジスタの遷移情報が取得しやすく HD 型の解析効率が上昇したと考えられる．電磁界プローブ位置を測定位置（A，B）から少しずらすとクロックに同期する波形ピークが下がることからも推測できる．以上の結果より，電磁波解析攻撃は電磁界プローブの位置とレイアウト，特にプローブ直下にどのような回路が配置されているかに大きく依存することがわかる．

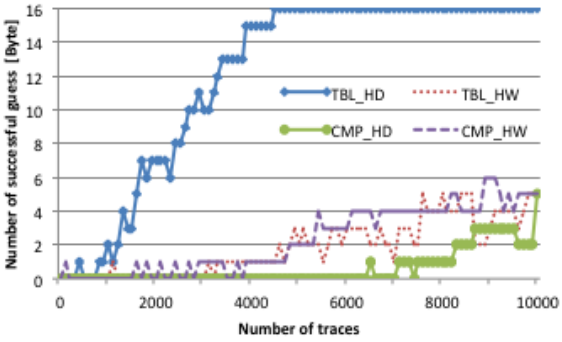

図 12　位置 A（チップ－テーブル）における CEMA 攻撃結果

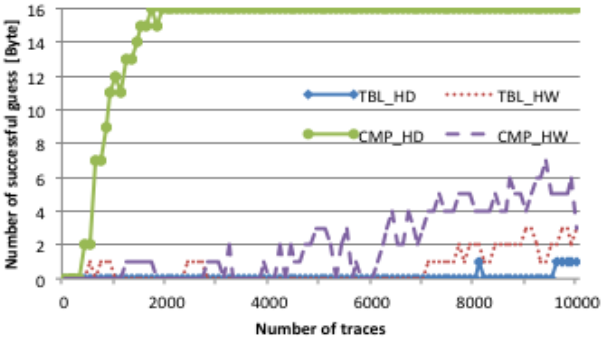

図 13　位置 B（チップ－合成体）における CEMA 攻撃結果

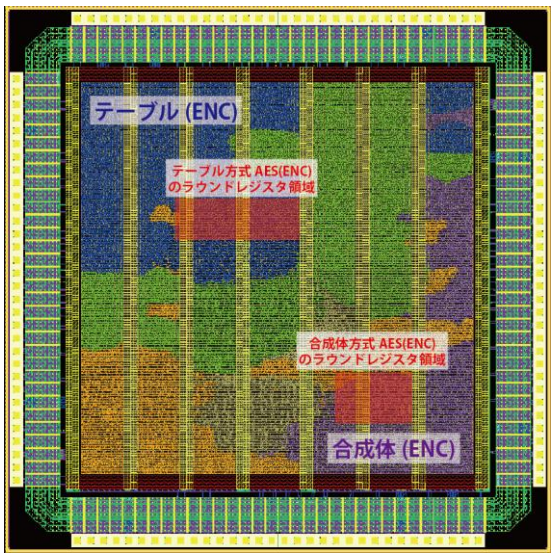

図 14　ラウンドレジスタの位置

次に，テーブル方式 AES が集中する位置に近い電源・グランドパッドに接続しているボンディングワイヤ上の位置 C（ボンディングワイヤ－テーブル）での CEMA 攻撃結果を図 15，合成体方式が集中する位置に近いボンディングワイヤ上の位置 D（ボンディングワイヤ－合成体）での CEMA 攻撃結果を図 16 に示す．位置 A，B の評価結果と同じ傾向であるのが，テーブル方式

AES が集中している箇所に近い位置 C ではテーブル方式が攻撃しやすく，逆に合成体 AES が集中している箇所に近い位置 D では合成体方式が攻撃しやすい点である．しかし，位置 A，B の評価結果と異なるのは，位置 D でもテーブル方式の方が合成体方式よりも少ない波形数で多くの秘密鍵が解明している点である．この傾向は電力解析攻撃で得られた結果（図 7 参照）に近く，チップ全体の消費電流が各ボンディングワイヤに流れ，そこから発生する漏れ磁場を測定していると考えれば，ある程度説明付くと考えられる．

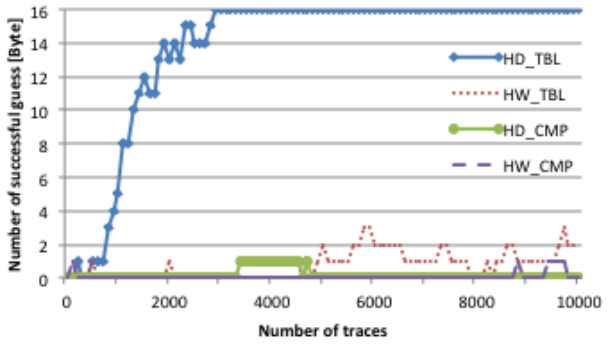

図 15　位置 C（ボンディングワイヤーテーブル）における CEMA 攻撃結果

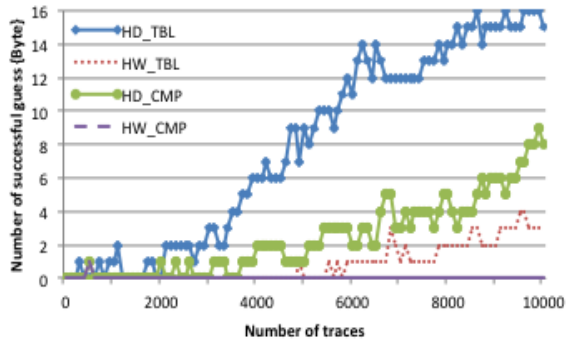

図 16　位置 D（ボンディングワイヤー合成体）における CEMA 攻撃結果

以上より，ボンディングワイヤからの漏れ磁場は消費電力と相関がある程度あり，電力解析攻撃対策を施せば電磁波解析攻撃にも有効であると考えられる．しかし，チップ直上における電磁波解析攻撃は電力解析攻撃とは異なり，電磁界プローブ近傍でどのような回路が処理しているかレイアウトに大きく依存するため，場合によっては非常に脅威であると考えられる．

5.2　電磁界プローブの効果

使用する電磁界プローブの差異が電磁波解析攻撃に与える効果を調べるため，未対策の合成体方式 AES に対して CEMA を行った．電磁界プローブ位置は位置 B に固定した．

まず，水平円形型コイルにおいて位置分解能の違いが CEMA 攻撃に与える影響を調べた．比較した電磁界プローブは HC020（位置分解能 0.55mm）と，それよりも位置分解能が 0.35mm と小さい HC010 である．比較結果を図 17 に示す．HD-CEMA に関しては位置分解能が大きい HC020 の方が 2,000 波形と少ない波形数で全ての秘密鍵が解明できた．しかし，HW-CEMA は位置分解能が小さい HC010 の方が同じ波形数でも解明している部分鍵の数が多く有効であるとの結果が得られた．単純に位置分解能が大きければ（もしくは，小さければ）電磁波解析攻撃に有効であるとは全く言えない．電磁界プローブが測定できる範囲と，その範囲内でどのような回路が動作しているのかに大きく関係していると思われるので，今後，レイアウトと合わせて実験評価を繰り返して原因を追求していきたい．

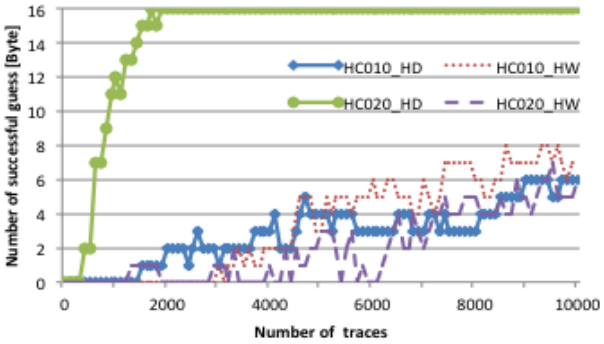

図 17　水平円形コイルの分解能が CEMA 攻撃に与える影響

次に，電磁界プローブを垂直扁平コイル型に変えて評価を行った．使用プローブは VF010 である．垂直扁平コイルは水平円形コイルと異なり，コイルの向きによって取得できる磁場が異なるので，図 18 に示すようにプローブ向き 0 度と 90 度の 2 通りで CEMA を行った．結果を図 19 に示す．ここでプローブ向き 0 度のときの HD/HW-CEMA 結果を HD/HW_0 とし，プローブ向き 90 度のときの HD/HW-CEMA 結果を HD/HW_90 とする．電磁界プローブの向きが縦の 8 本通している電源グランドラインに合わせた 90 度のとき CEMA 攻撃ができており，そこから 90 度回転させた 0 度ときには CEMA により 1 バイトの部分鍵も解明できていない．従って，電源ラインやグランドラインに電流が流れた際の漏れ磁場が情報漏洩に繋がっていると考えられる．また，水平円形コイルの結果（図 13）と比較すると鍵の解析速度が異なり，HW 型の攻撃では垂直扁平コイルの方が多くの鍵解析に成功している点は興味深い．今回はその点に関して考察，追加実験できなかったが，今後調査する予定である．

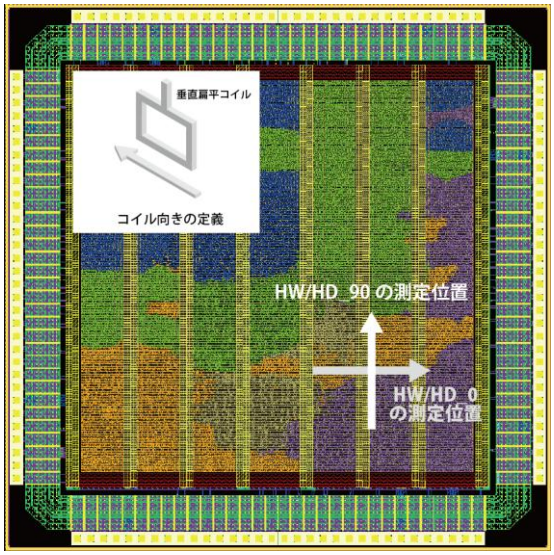

図 18　垂直扁平コイルによる測定位置

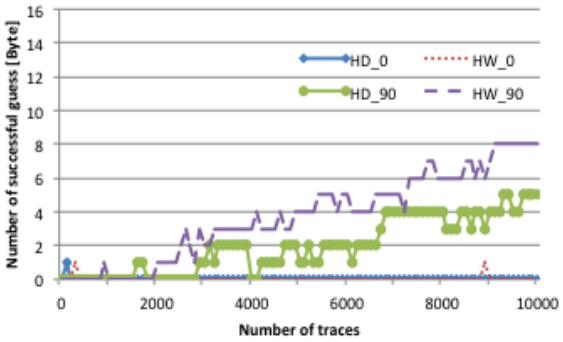

図 19　垂直扁平コイルの方向が CEMA 攻撃に与える影響

6　まとめと今後の課題

オンチップ・キャパシタが電力・電磁波解析攻撃に与える影響を調べるため，回路レイアウトは同一でオンチップ・キャパシタのみを挿入した試作 AES 暗号チップに対して CPA 攻撃，CEMA 攻撃を行った．また，電磁波解析攻撃に関しては電磁界プローブ位置や使用プローブに大きく依存するため, その効果を実測により調べた．今回行った実測評価結果より以下のことがわかった．

- 電力解析攻撃の対策として，完全ではないがオンチップ・キャパシタは有効である．
- 電力解析攻撃は，キャパシタの有無に関わらず HD 型の方が攻撃しやすい．
- 電磁波解析攻撃に対してオンチップ・キャパシタは対策にならない．
- 特に，HW 型の電磁波解析攻撃に対してはオンチップ・キャパシタにより情報リーク量が増える．
- チップ直上における電磁波解析攻撃では，プローブ近傍での処理情報を効率がよく取得でき，非常に脅威である．
- ボンディングワイヤからの漏れ磁場を用いた電磁波解析攻撃は電力解析攻撃と関係性がある．
- 電磁界プローブの位置分解能によって解析結果が異なる．
- 垂直扁平コイル型の電磁界プローブは向きによって攻撃結果が異なる．電源・グランドラインにコイルの向きを合わせて攻撃を行うと有効である．

今回の実験を通して，電力解析攻撃では全く見えない情報リークが電磁波解析攻撃によって窃取できることがわかった．しかし，その原因は明確に追求できておらず多くの問題点を残した．今後は原因究明のための実験評価を進めると伴に，電磁波解析攻撃の対策について検討する予定である．

謝辞

本研究は JST，CREST「ディペンダブル VLSI システムの基盤技術」の一環として行われた．180nm CMOS プロセスでの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じてローム(株)の協力で行われた．関係各位に感謝いたします．

参考文献

[1] P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis,” Proc. Crypto’99, LNCS1109, pp.388-397, 1999

[2] K. Gandolfi, C. Mourtel, and F. Olivier, “Electromagnetic Analysis: Concrete Results,” CHES2001, Proceeding volue, 2162 of LNCS, Springer-Verlag, 2001

[3] 片下敏宏，佐藤証，菅原健，本間尚文，青木孝文，“CPA に対するデカップリングキャパシタの影響の予備検証，” SCIS2009, 2009

[4] 菅原健，鳥塚英樹，本間尚文，佐藤証，青木孝文，山口正洋，“最近傍から計測した磁界を用いた差分電磁波解析，” SCIS2009, 2009

[5] 落合隆夫，山本大，伊藤孝一，武仲正彦，鳥居直哉，内田大輔，永井利明，若菜伸一，岩本貢，太田和夫，崎山一男，“電磁波解析における局所性と放射磁界方向について，” SCIS2011, 2011

[6] E. Brier, C. Clavier, and F. Olivier, “Correlation Power Analysis with a Leakage Model,” CHES 2004, pp.135-152, 2004

[7] “Side-cannel Attack Standard Evaluation Board,” “http://staff.aist.go.jp/akashi.satoh/SASEBO/ja/index.html”