



暗号モジュールの電源ノイズと情報漏洩に関する研究

藤本, 大介

(Degree)

博士 (工学)

(Date of Degree)

2014-03-25

(Date of Publication)

2015-03-01

(Resource Type)

doctoral thesis

(Report Number)

甲第6104号

(URL)

<https://hdl.handle.net/20.500.14094/D1006104>

※ 当コンテンツは神戸大学の学術成果です。無断複製・不正使用等を禁じます。著作権法で認められている範囲内で、適切にご利用ください。



博 士 論 文

暗号モジュールの電源ノイズと
情報漏洩に関する研究

平成 26 年 1 月

神戸大学大学院システム情報学研究科

藤 本 大 介

要旨

近年、モバイルPC、携帯電話、スマートカードの普及により、個人情報を持つ携帯デバイスがますます増加している。これらの携帯デバイスに含まれる秘密情報を保護するためには、暗号化を行い鍵を持たない他者からは解読できない形式にする必要がある。暗号化に使用されるアルゴリズムは現実的な時間で数学的に暗号解読が不可能である必要があり、規格の制定の際には多くの研究者によって、暗号化を破る攻撃が行われ安全性の評価が行われている。しかし、数学的に安全であるアルゴリズムであっても実際にLSI上に実装した場合、暗号化処理中に放射される電磁波や、消費電流量が漏れ情報として流出してしまう。これらの漏れ情報をサイドチャネル情報と言い、サイドチャネル情報を用いた暗号化回路攻撃手法をサイドチャネル攻撃と言う。暗号化回路が消費する電流による電圧変動を観測し攻撃するDifferential Power Analysis(DPA)が提案されている。暗号化回路の消費電流量は回路の動作に依存するため、大量の消費電流波形を収集できれば、回路内部の動作が予測でき秘密鍵が特定されてしまう危険性がある。DPAに代表される電力解析攻撃は電源電圧変動波形を取得するためのオシロスコープと波形を処理する計算機のみで構成でき、非常に安価なため脅威となっている。標準暗号として用いられているAES(Advanced Encryption Standard)であっても対策を施さずに回路実装を行った場合は電力解析攻撃によって秘密鍵が取得できることが報告されている。

そのため、電力解析攻撃に対する対策を設計段階で評価することは重要である。電力解析攻撃は内部データ遷移に依存するため多くの対策は入力データに依存しない遷移回数の論理を構築することで実現される。しかしながら、実際には論理セル間の遅延の差、消費電流のアンバランス、配線負荷のアンバランスなどからサイドチャネル情報が漏洩してしまう。そのため、物理デバイスレベルでの暗号化回路の消費電流シミュレーションを行うことが求められている。しかし、電力解析攻撃の評価のためには1万波形以上ものシミュレーションが必要であり、既存の回路シミュレータを用いるのは現実的ではない。

一方で、製造後の測定評価において、現在では実際に攻撃が行われる時と同様に評価ボード上に電源電圧取得端子を設けて電源ノイズ波形を

取得し電力解析攻撃ができないかを評価する手法が一般的である。しかし、チップ外部で得られる波形はボードの設計に大きく依存し、攻撃者がより高精度に電源ノイズを取得できる場合については対策ができていない。

また、暗号化回路の電力解析攻撃への耐性を評価する際に必要な電源ノイズの波形数が評価時間に大きく関わる。対策された暗号化デバイスであっても取得可能な時間で数十万波形を集めれば攻撃が可能になる場合があるためである。しかし暗号デバイスを設計するうえで数十万波形をシミュレーション、測定することは困難である。

本研究では、暗号化回路における電力解析攻撃への安全性評価技術として、物理デバイスレベルでの高速なシミュレーション、チップ内部での電源ノイズ波形取得技術、電力解析攻撃評価時に必要な波形を削減する技術を提案することを目標とする。

まず、シミュレーション技術においては CMOS 回路における消費電流が寄生容量の充電過程で発生するメカニズムに着目し、時系列的に充電される静電容量の列に置き換えてシミュレーションする容量充電モデルを提案する。静電容量の計算にはあらかじめ論理セルごとに遷移時に流れる電流を抽出しておき、高速であるデジタルシミュレーションと組み合わせる事で実現した。容量充電モデルによるシミュレーションによる電力解析攻撃の結果は実際のデバイスでの傾向とよく一致することを確認した。レイアウト情報を含む消費電流シミュレーションにおいてレイアウト情報を含まない回路シミュレータでの結果に対して 200 倍の高速化を達成した。

測定手法においては、従来チップ内の電源ノイズ観測に用いられてきたオンチップ診断技術であるオンチップモニタリング技術を応用した。チップ内での電源ノイズ観測のために暗号化回路とオンチップモニタを搭載したチップを試作し、チップ内外での電源ノイズの変化を評価した。結果、チップ外へは高周波成分が出て行かないという知見を得た。一方で、対策を施さない場合低周波成分にサイドチャネル情報が重畳することをつきとめた。この結果より、高周波成分に対する評価はチップ内における測定が必要であることが言える。

暗号化回路の評価時の波形数が膨大である問題については、回路開発者は秘密情報を持っているという利点を活かし、評価したい電力解析攻撃に合わせて暗号化デバイスからサイドチャネル情報が漏れやすい入力生成する手法を提案する。この手法を用いることでワーストケースで

の攻撃が成功できるかが評価できる．実際にシミュレーション，測定において1万波形を用いても攻撃できない電力解析攻撃対策実装を評価し，4000 波形程度で鍵の取得ができサイドチャネル情報が漏れているという結果を得た．この結果は1万波形より波形数を増やすと秘密情報を取得されてしまう可能性を示唆し，評価を1万波形で終了してしまうと評価として不十分であることを意味する．この評価の効率化手法により設計・製造時のサイドチャネル漏洩評価にかかる時間が大幅に削減される．

今後，暗号化回路を搭載したデバイスはますます増加する．そこで安全な暗号回路を設計する技術がより重要になる．本論文で提案した，シミュレーション技術は設計時の事前評価を可能にする．測定技術は製造後デバイスのより強固な評価となりうる．評価技術はシミュレーション，測定両者においてテスト時間を短縮する．これらの技術は安全な暗号回路のデザインフローを構築する上で有用である．

目次

1 緒論	1
1.1 研究背景	1
1.1.1 電力解析攻撃	4
1.1.2 電力解析攻撃対策	5
1.1.3 その他の攻撃手法	6
1.2 従来研究	7
1.2.1 VLSI 暗号回路における電力解析攻撃シミュレーション技術	7
1.2.2 VLSI 暗号回路における電源ノイズ測定技術	8
1.2.3 VLSI 暗号回路における電力解析攻撃への耐性評価技術	9
1.3 研究の概要と本論文の構成	10
1.3.1 VLSI 暗号回路における電力解析攻撃シミュレーション	10
1.3.2 VLSI 暗号回路における回路近傍での電源ノイズ測定	11
1.3.3 VLSI 暗号回路における電力解析攻撃への耐性評価	11
2 VLSI 暗号回路における電力解析攻撃シミュレーション	13
2.1 はじめに	13
2.2 容量充電モデル	13
2.3 電力解析攻撃シミュレーション	18
2.3.1 電力解析攻撃シミュレーションフロー	18
2.3.2 テストチップ	19
2.4 実験結果	23
2.4.1 サイドチャネル攻撃評価	26
2.4.2 他プロセスでのサイドチャネル漏洩評価	31
2.5 まとめ	31
3 VLSI 暗号回路における回路近傍での電源ノイズ測定	37
3.1 はじめに	37

3.2	オンチップ波形モニタリング技術	37
3.3	回路近傍での電源ノイズによる電力解析攻撃	38
3.3.1	テストチップ	40
3.3.2	測定評価環境	40
3.3.3	実験結果と考察	43
3.4	まとめ	51
4	VLSI 暗号回路における電力解析攻撃への耐性評価	55
4.1	はじめに	55
4.2	電力解析攻撃耐性評価手法	55
4.2.1	ハミング距離統一平文	57
4.3	提案手法による評価結果	61
4.3.1	テストチップ	61
4.3.2	実験結果	64
4.4	まとめ	69
5	結論	71
	謝辞	75
	参考文献	77
	発表論文一覧	85
	本研究に関する発表論文	85
	学術雑誌	85
	国際会議	85
	学術講演	86
	口頭発表	87
	技術報告	87
	その他の発表論文	87
	学術講演	87
	口頭発表	88
	図一覧	89
	表一覧	93

第1章

緒論

1.1 研究背景

近年、モバイル PC、携帯電話、スマートカードの普及により、個人情報を持つ携帯デバイスがますます増加している。スマートカードに着目して全世界での出荷数の推移を図 1.1 に示す。[1]2013 年には出荷数は 70 億を越えると予想され、クレジットカード、パスポート、交通などの様々な用途において ID などの秘密情報を保持している。これらの携帯デバイスに含まれる秘密情報を保護するためには、暗号化を行い鍵を持たない他者からは解読できない形式にする必要がある。暗号化に使用されるアルゴリズムは数学的に暗号解読ができないことが必要であり、規格の制定の際には多くの研究者によって、暗号化を破る攻撃が行われ安全性の評価が行われている。かつて米国標準暗号であった DES(Data Encryption Standard)[2] の例では 1977 年に仕様が公表され広く使用されていたが、鍵長が短いことが暗号としての弱点として挙げられていた。1994 年に松井による線形解読法による解読 [3] や 1998 年に DES cracker によるハードウェアを用いた鍵の全数探索による解読 [4] により暗号解読の危険性が現実的なものとなり、2002 年に AES(Advanced Encryption Standard)[5] により置き換えられた。AES においては攻撃手法として、大量の平文を暗号鍵によって暗号化できるという条件のもとで、暗号文から平文を逆算する選択平文攻撃 (Chosen-plaintext attack)[6] や複数の鍵で暗号・復号時に同様の動作をする部分があるものを関連鍵として扱い、鍵の傾向を探っていく関連鍵攻撃 (Related-key attack)[7], Biclique Cryptanalysis [8] が提案されている。どの攻撃においても現実的な計算量で暗号解読を行うには至っていない。このように暗号におけるアルゴリズムの標準化 [9]、安全性は厳しく評価されている。日本では、CRYPTREC[10] が暗号の評価を行い安全である暗号のリストを公表している [11]。

しかし、数学的に安全であるアルゴリズムであっても実際に LSI 上に実装した場合、暗号化処理中に放射される電磁波や、消費電流量が漏れ

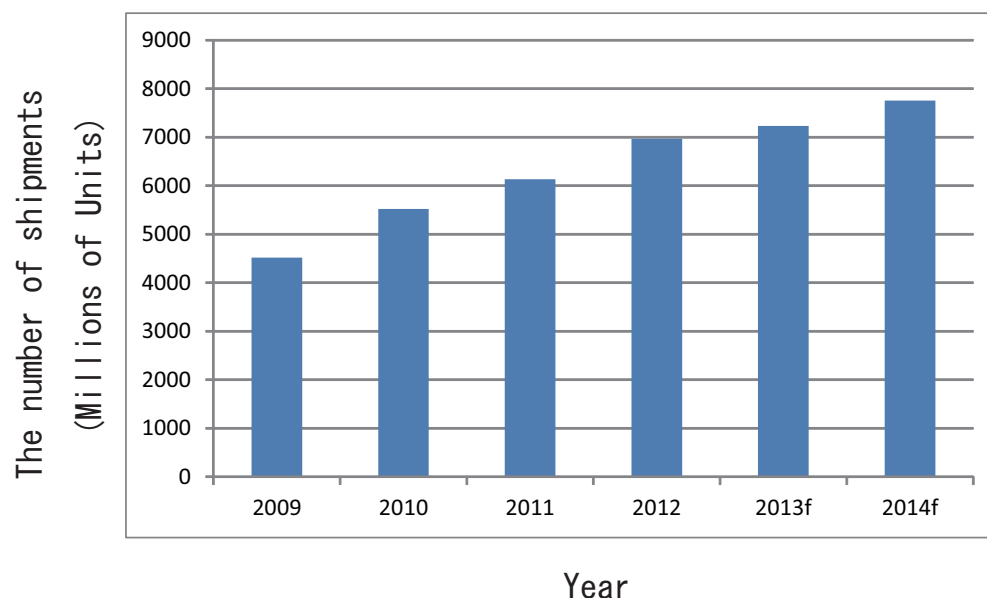


図 1.1: 全世界でのスマートカード出荷数の推移

情報として流出してしまう。これらの漏れ情報をサイドチャネル情報と言い、サイドチャネル情報を用いた暗号化回路攻撃手法をサイドチャネル攻撃 (SCA: Side-channel attack) と言う (図 1.2)。例えば、暗号処理の内容によって処理時間が変わるような暗号に対して Timing Attack [12] が提案されている。Timing Attack に関しては、アルゴリズム、実装レベルでの対策が可能である。一方対策が困難である攻撃として、暗号化回路が消費する電流による電圧変動を観測し攻撃する Differential Power Analysis (DPA) [13] が Kocher らによって提案されている。暗号化回路の消費電流量は回路の動作に依存するため、大量の消費電流波形を収集できれば、回路内部の動作が予測でき秘密鍵が特定されてしまう危険性がある (図 1.3)。DPA などの電力解析攻撃は電源電圧変動波形を取得するためのオシロスコープと波形を処理する計算機のみで構成でき、非常に安価なため脅威となっている。

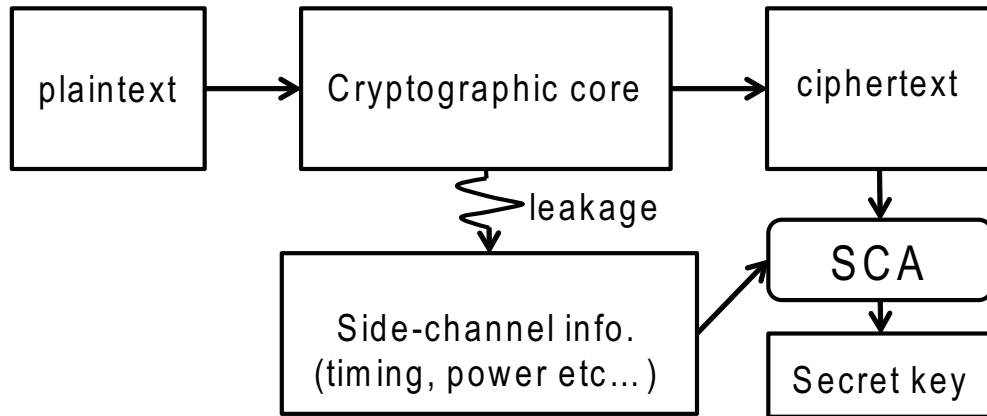


図 1.2: サイドチャネル攻撃イメージ

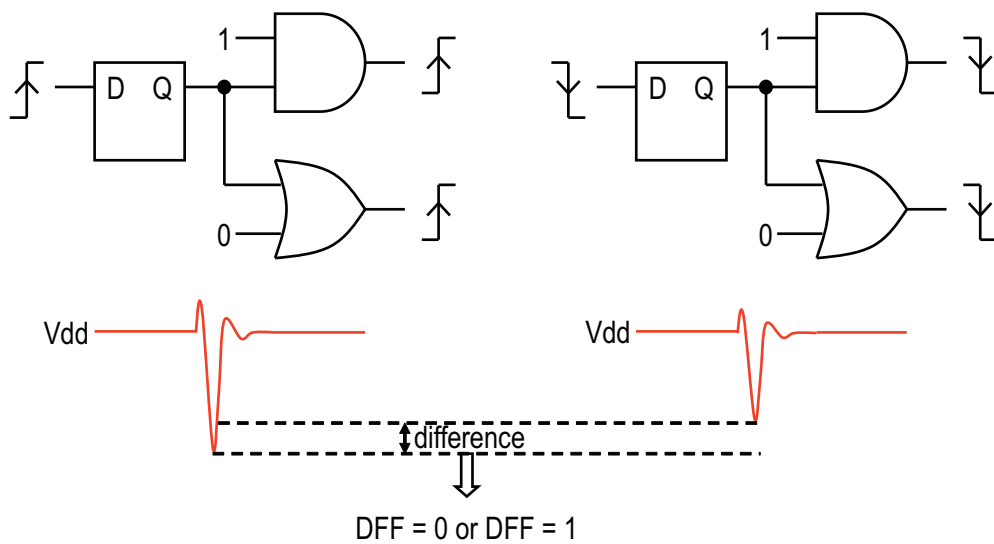


図 1.3: 消費電力による内部状態推定イメージ



ICカードやワイヤレスLANで広く用いられている共通鍵暗号方式であるAESにおいては、前述した通りソフトウェアで計算を行う攻撃においては暗号解読は成功していない。また、DESで存在していた弱鍵なども指摘されていない。一方で、ハードウェア攻撃においては、DPAを改良した電力解析攻撃手法の一つであるCPA(Correlation Power Analysis)では、数千～数万の異なる入力を行った場合の電源電圧変動波形を用いることで正しい鍵を特定できることがわかっている [14][15]。

AES はデータレジスタで保持した値を SubBytes(S-box), ShiftRows, MixColumns, AddRoundkey の 4 種類の処理を何回もループさせること

で暗号化を行う。ループさせる回数は使用する鍵の長さで決まっており 128bit で 10 回、192bit で 12 回、256bit で 14 回となる。本論文では一番短い 128bit での実装を用いる。

一般的に CPA では AES 暗号化の最終ラウンドに着目する [14]。Mix-Columns はこのラウンドでのみ行われなため、8bit の S-box 毎に独立して演算が行われるので攻撃者が逆算するのに都合が良いためである。

最終ラウンドにおいて、16 個の 8bit 部分鍵について $k(0 \leq k \leq 255)$ がそれぞれ仮定される。そこで、暗号化の出力である暗号文を用いてそれぞれの 8bit S-box に関してデータ遷移の数であるハミング距離 H_k ($0 \leq H_k \leq 8$) が求められる。ハミング距離はそれぞれの S-box に対して 256 個の候補となる鍵についてそれぞれ算出する。

$$corr_k(t) = \frac{cov(W(t), H_k)}{\sqrt{var(W(t))}\sqrt{var(H_k)}} \quad (1.1)$$

$$cov(W(t), H_k) = \frac{1}{N} \sum_{i=1}^N (W_i(t) - \overline{W(t)})(H_{k,i} - \overline{H_k})$$

$$var(W(t)) = \frac{1}{N} \sum_{i=1}^N (W_i(t) - \overline{W(t)})^2$$

$$var(H_k) = \frac{1}{N} \sum_{i=1}^N (H_{k,i} - \overline{H_k})^2$$

さらに、 N 個の消費電力波形 $W_i(t)$ ($0 \leq i \leq N-1$) を異なる入力平文を用いた暗号化演算について取得する。この波形を用いて 256 個の鍵候補についてのハミング距離を求めることができる。 H_k と $W_i(t)$ の相関係数 $corr_k(t)$ は式 1.1 により求められる。 $\overline{W(t)}$, $\overline{H_k}$ はそれぞれ W_t, H_k の平均値を表している。最後に、8bit の候補鍵のうち最も高い相関係数を得られた k を取得し、秘密鍵と考える。

1.1.2 電力解析攻撃対策

電力解析攻撃に対して様々なロジックレベル、物理実装レベルでの対策回路が提案されている。対策手法は大別してハイディングとマスキングの 2 種類である。ハイディングは暗号化回路によって発生するサイドチャネル情報を秘匿する手法である。ダミー処理をランダムに挿入し暗

号処理タイミングを毎回変えることで暗号処理の処理時間や時間位置を秘匿する手法や背景ノイズを増加させサイドチャネル情報を秘匿する手法、消費電流の変化を小さくする手法などがある。ハイディング実装として SABL(Sense Amplifier Based Logic)[16] や WDDL(Waveform Dynamic Differential Logic)[17]、電源イコライザ [18] が提案されている。マスキングは暗号処理中のある演算に対してランダムなマスク処理を行うことで消費電力が処理に依存しないようにする手法である。ランダムマスクによる消費電力を越えて秘匿することはできないのでハイディングと組み合わせることが多い。実装として MAO(Masked AND Operation) [19]、MDPL(Masked Dual-Rail Pre-Charge Logic) [20]、TI(Threshold Implementations) [21] などが挙げられる。

上記のような対策を施した場合であっても、回路実装に際して発生する寄生成分による信号タイミングのずれや消費電流のアンバランス、ランダムマスクの消費電力の偏りなどによってサイドチャネル情報が漏れてしまうという問題がある [22][23]。そのため、設計時に電力解析攻撃に対して耐性を持つかを評価する技術が重要となっている。

1.1.3 その他の攻撃手法

また、暗号に対する攻撃技術は日々進歩し、新たな情報漏洩が定義されてきている。プロファイリングにより攻撃に必要な波形数を減らすテンプレートを作成するテンプレート攻撃 [24] [25] [26]、ハミング距離などの電力モデルをつかわず、波形自体を電力モデルへと利用し相関値を高める Correlation-Enhanced Power Analysis Collision Attack [27]、暗号回路の内部推定情報と測定情報の相互情報量を利用する相互情報量解析 (Mutual Information Analysis)[28] や AES のループアーキテクチャに着目したクロック間のデータ衝突を利用した Clockwise Collision Analysis [29]、クロック間衝突と磁界プローブによる攻撃を組み合わせた CCEMA(Clockwise Collision ElectroMagnetic Analysis)[30]、機械学習を応用した攻撃 [31][32] などが提案されている。これらの新しい攻撃に対してもサイドチャネル情報漏洩の評価を行うことが必要となり、設計者にとって評価コストが増すこととなる。

本論文では、暗号化回路における電源消費電流に着目し、電力解析攻撃のシミュレーションモデルの提案、チップ内回路近傍測定による暗号コアのサイドチャネル漏洩評価、電力解析攻撃への耐性を効率的に評価する手法について論ずる。

1.2 従来研究

暗号化回路の安全性評価においていくつかのシミュレーションモデル、測定技術、評価技術が提案されている。本章では、それらの従来研究について簡単に述べる。

1.2.1 VLSI 暗号回路における電力解析攻撃シミュレーション技術

安全な暗号化デバイスを製造することにおいて、シミュレーションによりサイドチャネル情報の漏洩を見積もることは非常に重要である。以下に提案されているサイドチャネル漏洩におけるシミュレーション手法をあげる。

Hartog らによって提案された PINPAS はマイクロプロセッサ上でのソフトウェア実装における消費電流波形をシミュレーション可能である [33]。シミュレーションは命令レベルで行われ、命令と入出力に対応した消費電流を加算し見積もる手法である。

Aigner らによって提案された手法ではマイクロコントローラ上で System-C で記述された AES の安全性を評価できる [34]。シミュレーションで用いるのは内部データのハミング重みと何種類かのハミング距離を組み合わせたモデルであり、これらを用いてサイドチャネル情報漏洩を評価する。また、HDL で記述した AES に対する評価としてデータの遷移から消費電流を見積もる手法も提案されている。HDL を用いた評価ではアーキテクチャレベルから論理合成後のゲートレベルまでの広い範囲で評価が可能である。

また、Kirschbaum らにより論理シミュレーションを用いた Toggle Counting モデルが提案されている [35]。各タイミングでの内部セルの遷移回数をカウントし、消費電力の指標としている。Place and route 後の遅延情報 (SDF: Standard delay format) を用いることでタイミングの精度を向上させている。これと似た手法に Chen らが提案して FPGA を用いた Toggle Counting 手法 [36] がある。FPGA 上に実装した Toggle Counting 回路を用いることでソフトウェアによるシミュレーションよりも高速化が実現できる。一方で FPGA に実装しているため ASIC とは構成回路、遅延情報が異なる可能性がある。Toggle Count によるリークを提案した例としては Mangard らによる Masked AES への攻撃がある [37]。

物理デバイスレベルでは SPICE を用いてシミュレーションを行った例

表 1.1: 暗号化回路におけるサイドチャネル情報漏洩シミュレーション

Design Level	Device	Language	Simulator
Low Level	Microcontroller	Assembly	PINPAS
High Level	Microcontroller	System-C	SCARD
RTL	ASIC	HDL	SCARD
After Synthesis	ASIC	HDL netlist	SCARD
After place and route	ASIC	HDL netlist	Toggle Counting
MOS	ASIC	SPICE netlist (partial)	SPICE

がある [38]. この場合暗号化回路を構成するあるファンクションについてシミュレーションを行い、サイドチャネル情報の漏洩が無いかを評価することになる. そのため、回路全体での配置配線時に発生する配線遅延や結合時の負荷のアンバランスが評価できない.

これらの手法を表 1.1 にまとめる.

いずれの手法についても、マイクロコントローラ上のソフトウェア実装や HDL ネットリストレベルでの論理処理にとどまっており実際の物理現象とは乖離があると考えられる. また物理デバイスレベルでの SPICE を使ったシミュレーションでは回路の一部のみにとどまっている.

1.2.2 VLSI 暗号回路における電源ノイズ測定技術

暗号化回路の標準測定環境として SASEBO(Side-channel Attack Standard Evaluation BOard) が産業技術総合研究所から提案されている [39]. SASEBO は世界中で広く使われており標準環境となりつつある. SASEBO 上には従来提案されている測定手法のための素子が標準で搭載されている.

電力解析攻撃で用いられる測定手法に電源ラインに直接プローブを設ける手法がある [40]. この手法では $1\ \Omega$ 程度の小さい抵抗を電源ラインに挿入し、両端の電圧差を測ることにより電源ラインに流れる電流値を取得する手法である (図 1.5(a)). また、単に $1\ \Omega$ 抵抗のチップ側を観測することでも電圧変動を観測することが可能である [41][42]. 本論文では後者を比較対象として用い、 $1\ \Omega$ 法として扱う.

一方で、磁界プローブを用いチップ上や電源ライン上に流れる電流を取得する測定手法がある [40](図 1.5(b)). 磁界プローブを用いる場合は専用端子をボードに設ける必要が無く、チップ直上などにもアクセスができる場合によれば、 $1\ \Omega$ 法よりも精度の良い波形が取れる場合がある [43][44][45].

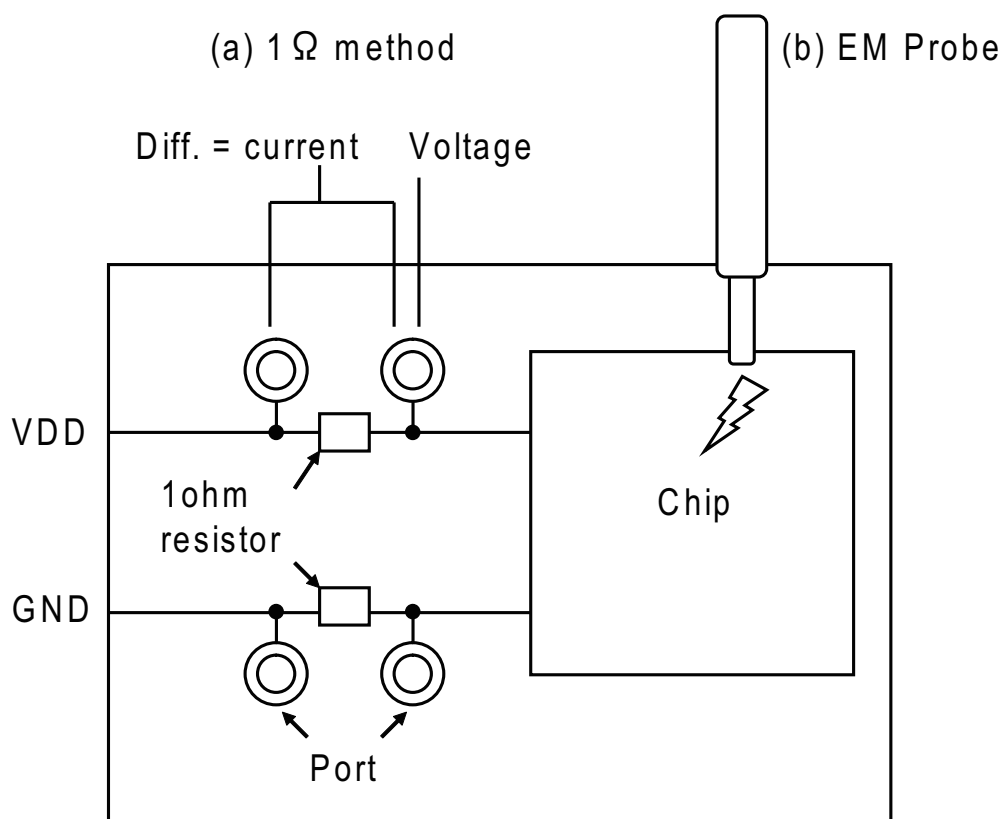


図 1.5: 電力解析攻撃における測定手法

将来的に磁界プローブが小さくなりチップ内で局所性を取得できた場合局所性からより強力な攻撃ができる可能性も指摘されている [46]. その反面電流が流れる位置を探索する必要があり、またポジショナーなどの設備が無い場合測定の再現を行うことが困難であると考えられる.

1.2.3 VLSI 暗号回路における電力解析攻撃への耐性評価技術

暗号化回路のサイドチャネルに対する安全性を確保するためには設計段階でのサイドチャネル攻撃耐性評価が欠かせない. 一般的な暗号回路の設計評価フローを図 1.6 に示す. 論理合成後、配置配線後において設計が安全であるかをシミュレーションによって評価する. このとき問題となるのは実際に電力解析攻撃を行うには 1 万回以上のシミュレーションが

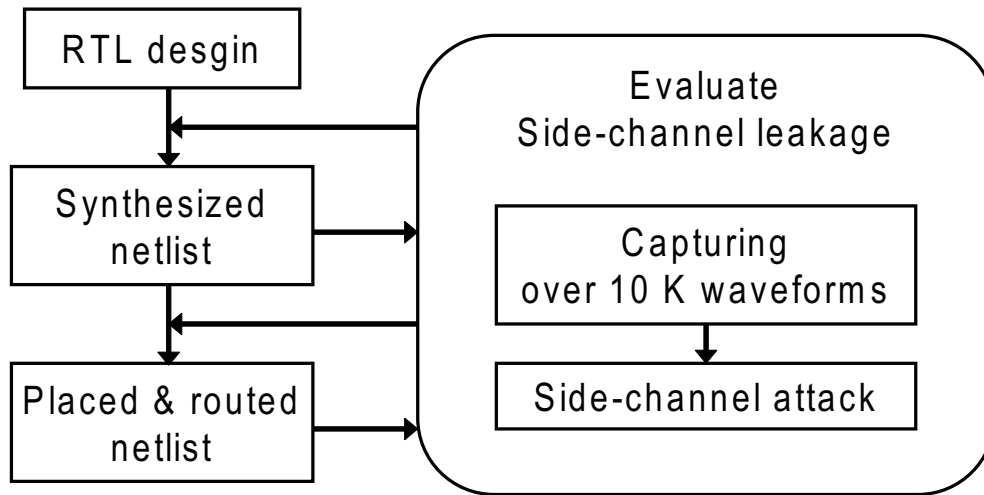


図 1.6: 電力解析攻撃に対する耐性評価フロー

必要になることである。安全性の指標となる規格では Common Criteria [47] において 100 万波形による評価、草稿段階ではあるが ISO17825[48] において Level3 として 1 万波形、Level4 として 10 万波形での評価が求められる。SASEBO においても 10 万波形での評価が行われている [49]。

現在では、暗号回路内でサイドチャネル情報が漏れやすい非線形関数などの一部の回路において SPICE シミュレーション等の精度の高いシミュレーションを行うまたは、論理シミュレーションを行った後チップを製造し、評価する手法が一般的である [50][51]。評価手法としては、現在提案されている攻撃に対して網羅的に波形を取得し実際に攻撃を行うことになる。

1.3 研究の概要と本論文の構成

1.3.1 VLSI 暗号回路における電力解析攻撃シミュレーション

暗号化回路設計において脅威となる電力解析攻撃に対してシミュレーションを行うことは重要である。従来のシミュレーションでは、アルゴリズムレベル、データ遷移レベルでしか評価することができておらず物理レベルとの乖離があることが課題である。一般的に用いられる回路シ

ミュレータである SPICE では電力解析攻撃に必要な複数の波形をシミュレーションするのは現実的ではない。そこで本研究では、デジタル回路の消費電流を静電容量の充電で表現する容量充電モデルを用いて、高速かつ物理デバイスレベルでの消費電流シミュレーションを提案する。評価には実際のデバイスで測定された消費電力波形との比較を行い、シミュレーションモデルの性能を示す。また物理デバイスレベルでの回路シミュレータである高速 SPICE との比較を行いその高速性能を評価する。

1.3.2 VLSI 暗号回路における回路近傍での電源ノイズ測定

電力解析攻撃は主にチップ外部での測定波形で行われる。現在、電力解析攻撃への耐性を評価するための測定においても評価用のボード上に専用の電源ノイズ取得ポートを設けているが、依然としてチップ外部での測定を行っている。しかし、外部に漏れ出すサイドチャネル情報は外部の実装に影響され変化するため、チップ内での評価が欠かせない。本論文では、チップ内部の電圧変動を検出するオンチップモニタ技術を暗号化コアのサイドチャネル情報の取得に適用することを提案する。従来行われていたチップ外部での測定結果と比較し、チップ内部で電源ノイズを取得する優位性について述べる。

1.3.3 VLSI 暗号回路における電力解析攻撃への耐性評価

電力解析攻撃への耐性を設計時に評価するためには、シミュレーションにより実際に電力解析攻撃を行う手法が主である。しかし、電力解析攻撃では電源ノイズ波形を統計的に評価し、内部動作を特定し秘密情報を抜き取るために 1 万波形以上のシミュレーションを行う必要がある。設計時にこのような時間のかかるシミュレーションを行うことは現実的ではない。そこで本論文では、評価する暗号回路の電力解析攻撃対象となる回路動作に着目し、サイドチャネル情報が漏洩しやすいテストパターンを生成する手法を提案する。この手法の有用性を確かめるために、2 章で示す容量充電モデルと実際の回路で測定を行った波形を用いて対策された AES において攻撃に必要な電源ノイズ波形の数が減少することを確認する。

第2章

VLSI暗号回路における電力解析攻撃シミュレーション

2.1 はじめに

暗号化アルゴリズムのVLSI実装において、サイドチャネル攻撃が脅威となっている。サイドチャネル攻撃のひとつである電力解析攻撃では、暗号化回路内の秘密鍵は暗号化回路の出力データと暗号化回路の消費電流波形を解析することで取得可能である。たとえ論理的に対策を施しサイドチャネル攻撃への耐性をもった実装であっても、実際にデバイスを製造した場合、遅延や負荷のアンバランス、デバイスの消費電流のアンバランスによりサイドチャネル情報が漏れてしまう可能性がある。そこで、設計段階で物理デバイスレベルでの高速なシミュレーション技術が求められているが、現在物理デバイスレベルでのサイドチャネル攻撃の評価に耐えるシミュレーションモデルは提案されていない。そこで、本研究では物理デバイスレベルでの高速な電源ノイズシミュレーションモデルである容量充電モデルを応用しサイドチャネル攻撃評価に利用可能なシミュレーションモデルの提案を行う。

2.2 容量充電モデル

CMOSデジタル回路は一般的に論理回路で構成され、スタンダードセルを用いた論理合成フローによって設計される。ここでは暗号化回路、特に消費者向け製品ではCMOSテクノロジーで実装され上記のフローに則ると仮定してモデリングを行う。

デジタル回路の消費電流シミュレーションには、フルトランジスタレベルの回路を回路シミュレータにより解くもしくは、Synopsys社 PrimeTimePXのようなスタンダードセルライブラリの消費電力テーブルとデジタル回路の遷移情報から消費電力を見積もる [52]、または、回路の消費

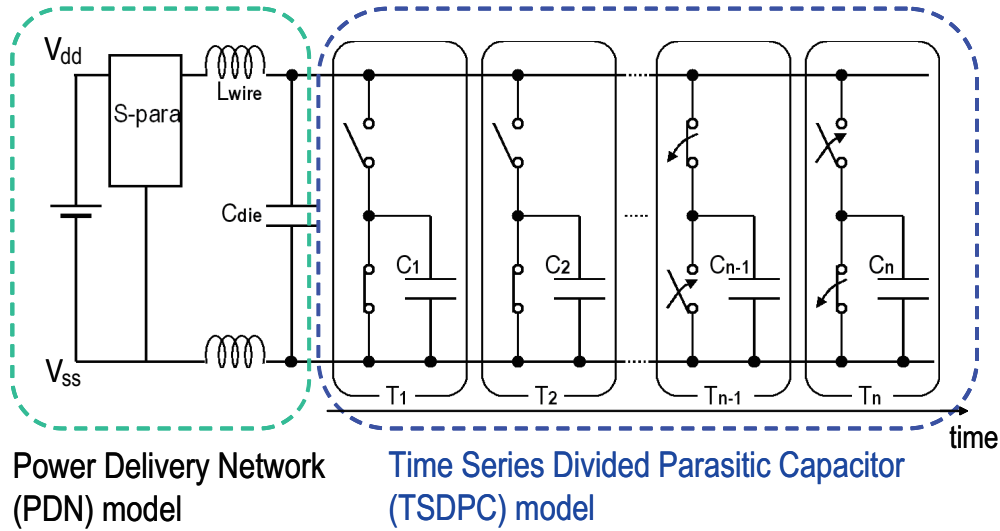


図 2.1: 容量充電モデルの等価回路

電流を何らかのモデルに置き換えて見積もる手法などがある．フルトランジスタレベルでのシミュレーションは計算コストが高く消費電流の解析を行う上で現実的ではない．PrimeTimePX を用いた消費電流解析では高速に単位時間あたりの消費電流を見積もることはできるが，連続的な波形ではないため離散化，量子化誤差が大きいと考えられる [53]．消費電流のモデルとしてトランジスタの寄生容量の充電過程に着目した容量充電モデル (TSDPC : time series divided parasitic capacitance model) が提案されている [54][55]．

容量充電モデルでは微小時間区間における大量の論理ゲートのスイッチング動作を一つのキャパシタに置き換え， V_{dd}, V_{ss} 間に挿入する．このキャパシタが対応する微小区間内で充電される．キャパシタのサイズは微小区間内で充電されるデジタル回路の寄生容量の和である．

動的な電源電流は容量充電モデルの連続的な充電によって表現する．スイッチトキャパシタを列状に接続し，各キャパシタは $T_1, T_2 \dots T_m$ の対応するタイミングで充電される．時間 T_n でキャパシタが充電される時，直前に充電されていた T_{n-1} に相当するキャパシタは放電される．この様な回路の簡単化によって回路シミュレータによって解く回路ネットワークのサイズは劇的に減少し，電源電流シミュレーションが高速化される．また，図 2.1 の回路に示すとおり，回路内部の消費電流が電源，基板ネットワークを流れる際に電源ノイズと呼ばれる電圧変動が発生する．

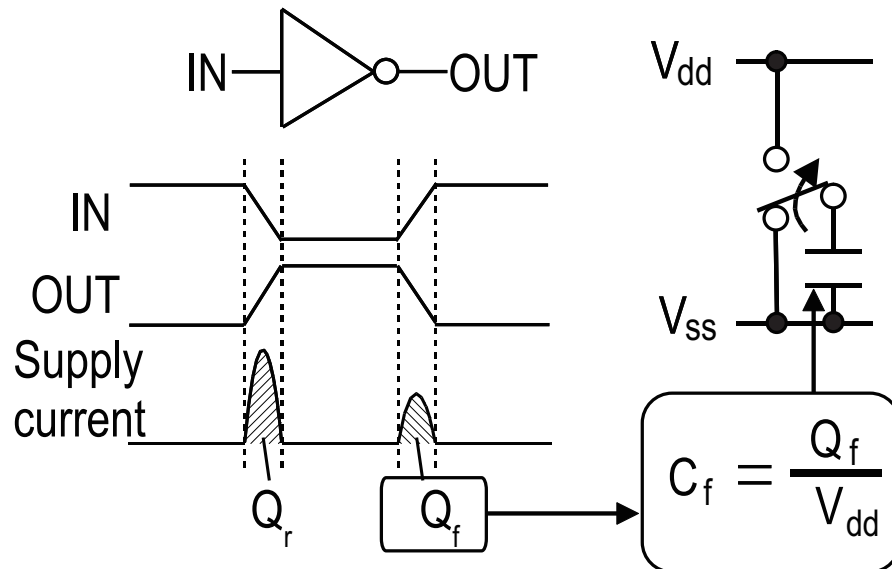


図 2.2: 容量充電モデルにおけるスタンダードセルの寄生容量値導出

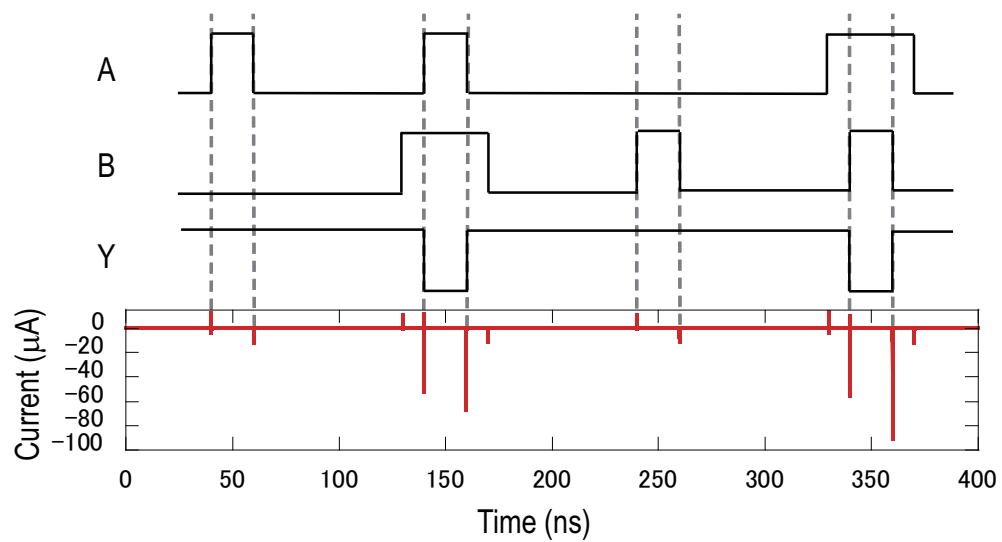


図 2.3: 2 入力 NAND ゲートの消費電流シミュレーション

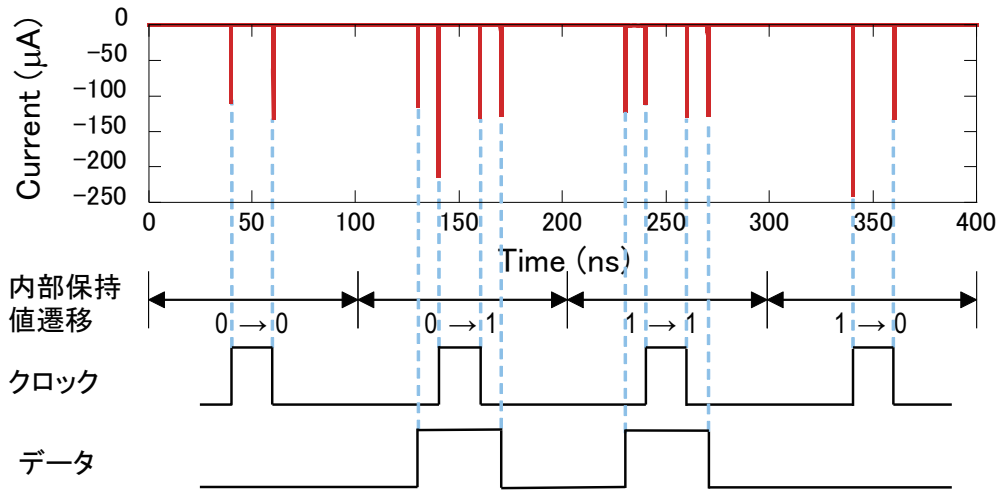


図 2.4: DFF の消費電流シミュレーション

論理ゲートセルが遷移したとき、エネルギーの総和は $C_{\text{load}} * V_{\text{dd}}^2$ で表すことができる。 C_{load} はセルの総負荷容量である。 C_{load} のサイズは図 2.2 に示すようにデジタル回路内の各スタンダードセルにおいてスパイスなどの回路シミュレータを用いて消費電流をシミュレーションして行う。従来の容量充電モデルでは論理ゲートの出力が変化した場合の消費電流を統合し計算量を減らしていたが、サイドチャネル攻撃ではより微小な消費電流が重要となるため統合せずにすべての入力変化に対して消費電流を抽出した。2 入力 NAND ゲートを例にとるとすべての論理変化は 8 パターンの入力値遷移が考えられる (表 2.1)。SPICE によるシミュレーション結果は図 2.3 のようになる。同じ出力遷移 ($0 \rightarrow 1, 1 \rightarrow 0$) の場合でも消費電流量が異なる事がわかる。DFF (Delay Flip Flop) などの順序回路においては内部保持値の変化が消費電流を考えるうえで重要となる。DFF の SPICE シミュレーション結果を図 2.4 に示す。内部保持値が変化するタイミングで大きな消費電流が流れていることがわかる。また、出力値が変化しないクロックの立ち下がり時にも比較的大きな消費電流が流れるのも特徴的である。このように各スタンダードセルの特徴に合わせた消費電流抽出が重要となる。

容量充電モデルのシミュレーションフローを図 2.5 に示す。入力論理遷移のシミュレーションは Verilog などの高速な論理シミュレータを利用し高速化を行う。入力論理遷移を元に微小区間 ΔT 内に充電される静電容量の値を決定する。微小区間 ΔT での静電容量の値は微小時間内で同時

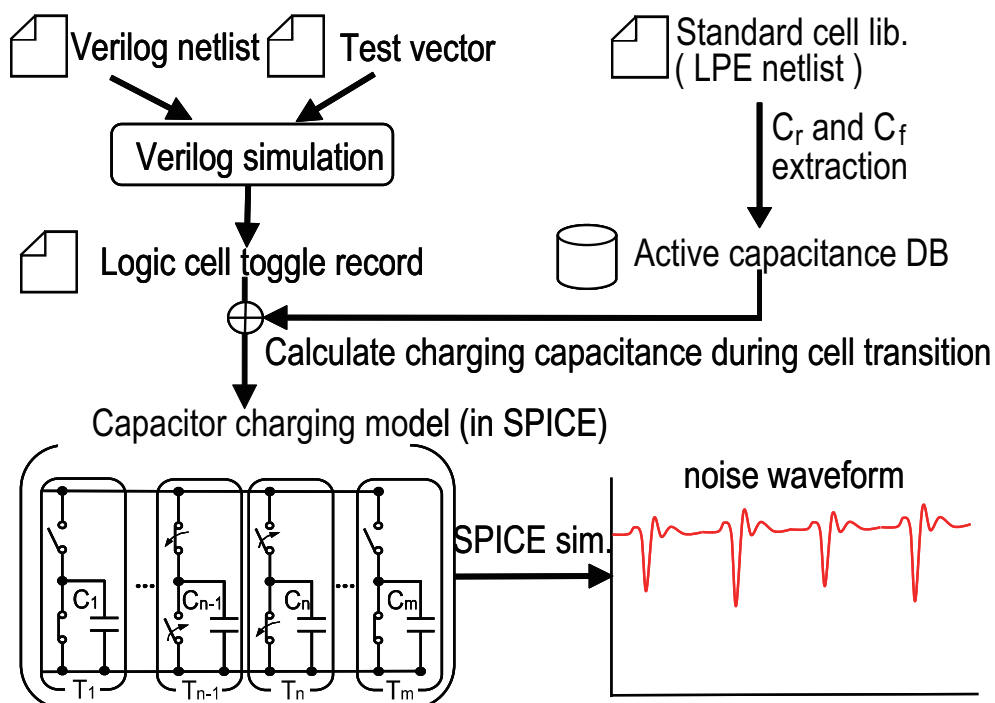


図 2.5: 容量充電モデルモデリングフロー

表 2.1: 2 入力 NAND ゲートの全入力遷移

A	B	Y
1→0	0	1→1
0→1	0	1→1
1→0	1	1→0
0→1	1	0→1
0	1→0	1→1
0	0→1	1→1
1	1→0	1→0
1	0→1	0→1

に遷移したセルの C_{load} の和で表現可能である。微小区間毎に求めた静電容量を並列に接続し、微小区間毎に対応した静電容量がスイッチにより繋がり充電される様な回路に置き換え、回路シミュレータに解かせることで連続時間波形を取得する。このように、容量充電モデルは一般的な CMOS デジタル回路に適用可能なフローで構築される。また、周波数成分の解析のための長時間の電源ノイズ波形を得るために容量充電モデルのキャパシタの数を増やすことも容易である。キャパシタの数は精度とシミュレーション時間のトレードオフとなるので熟慮する必要がある。

デジタル回路はシリコンチップに実装され一般的に FR-4 ボードに実装される。電源、グラウンド雑音波形は電源ネットワーク (PDN: power delivery network) に寄生しているインピーダンスを含んでいる。これらの寄生インピーダンスは、消費電流の周波数成分においてフィルタリングもしくは増幅をもたらす。電源ネットワークはシミュレータによって抽出でき、容量充電モデルに並列に接続することでオフチップインピーダンスを考慮した消費電流シミュレーションも可能となる。

2.3 電力解析攻撃シミュレーション

2.3.1 電力解析攻撃シミュレーションフロー

消費電流による電源ノイズと暗号処理の相関はサイドチャネル攻撃に対する脆弱性の原因となる。暗号化処理の特定のクロックにおいて暗号化の中間値が更新される場合、その区間の消費電流量は CPA に用いることができる。

1 章で述べた AES の最終ラウンドは、処理開始から 10 サイクル後のクロックである。図 2.6 に AES 回路に対する CPA を示す。測定やシミュレーションによって AES 回路の 10 サイクル目における消費電流の波形を取得し、数式 1.1 で示したデータレジスタのハミング距離との相関値を求める。16 バイトの秘密鍵を 1 バイト 毎に区切り、そのそれぞれに対して最も相関値の高くなる鍵候補を統計的に求める。

CPA フローをシミュレーションで実現するためには、AES モジュールの暗号処理の容量充電モデルに入力する 128bit の平文を変化させ生成する必要がある。秘密鍵への攻撃が成功するには 10000 波形以上もの異なる平文に対する消費電流波形が必要となるため、シミュレーションの高効率化が求められる。

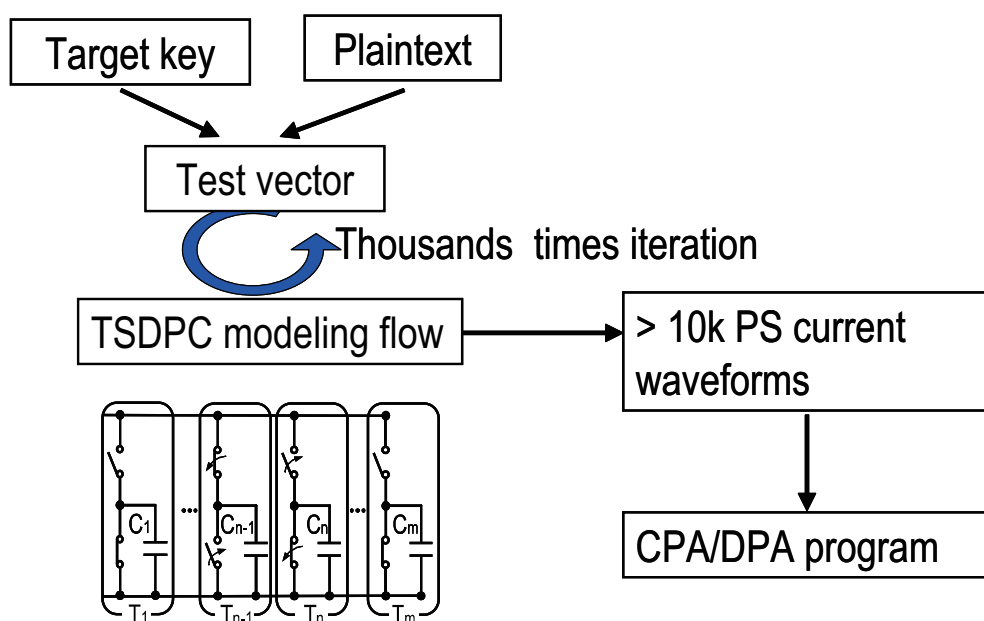


図 2.6: 容量充電モデルを用いた CPA フロー

2.3.2 テストチップ

AES 暗号アルゴリズムの実装の異なる様々な AES モジュールを図 2.7 に示すような 65 nm CMOS テクノロジーを用いたチップで製造した。

本論文では 4 種類の S-box の実装が異なるモジュールを対象に、実装による CPA への耐性の差を評価する。それらの実装はそれぞれ Composite S-box, PPRM1 S-box, PPRM3 S-box, Table S-box であり、ゲート数を表 2.2 に示す。これらの実装の差は消費電流や面積に最適化したかの条件が違うのみで、電力解析攻撃には対策されておらず秘密鍵が特定されることが期待される。

消費電力の測定は図 2.9 に示す SASEBO-R ボードにテストチップを搭載し図 2.8 に示すような実験環境で行う。消費電流はテストチップの電源ピンを通り外に流れ出し SASEBO 上の観測端子にてオシロスコープにより取得する。容量充電モデルをもちいたシミュレーションとの比較のため SASEBO を用いて消費電流波形を 10000 個の平文に対して測定する。

表 2.2: AES 暗号化回路における異なる S-box 実装間の規模差

S-box	Silicon area [μm^2]	# of gates
Compsite	21,852	53,417
PPRM3	27,110	66,249
Table	36,470	84,512
PPRM1	97,306	235,389

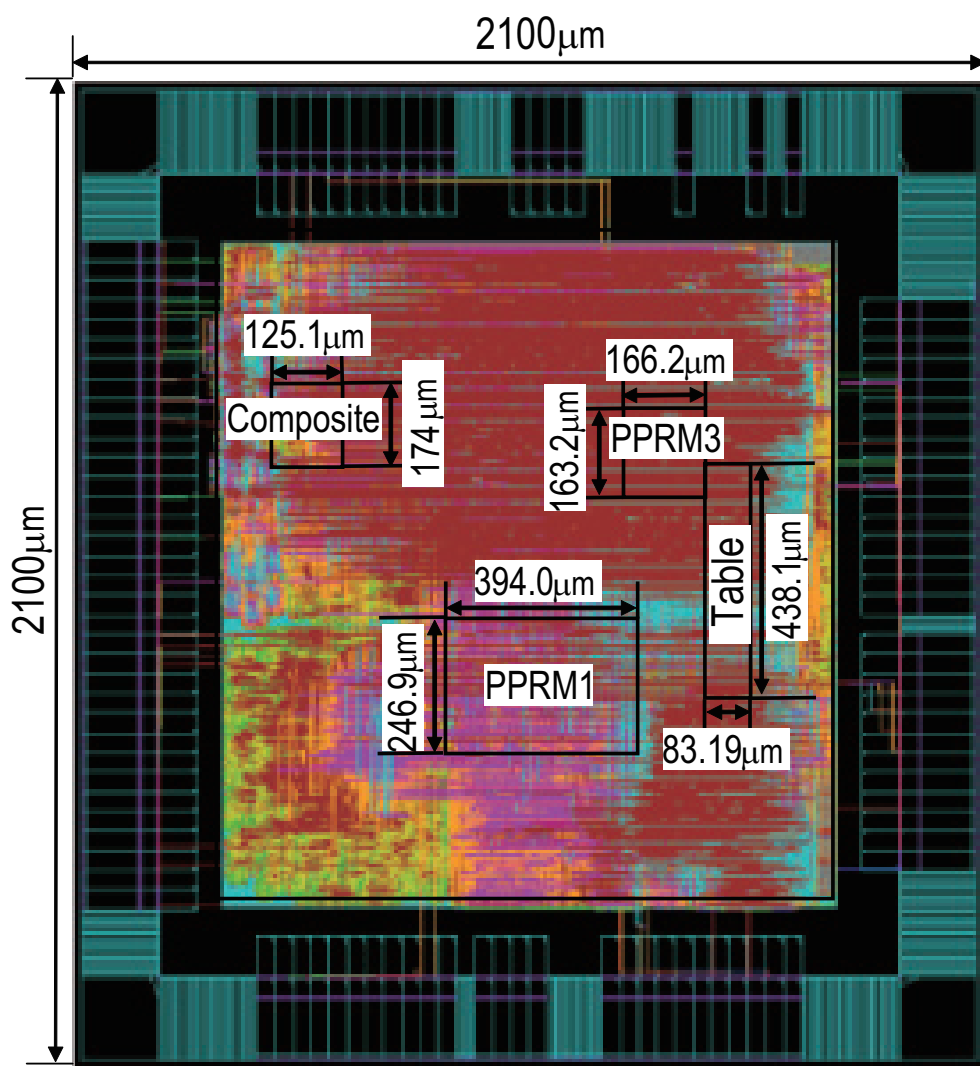


図 2.7: 65nmCMOS チップのレイアウト

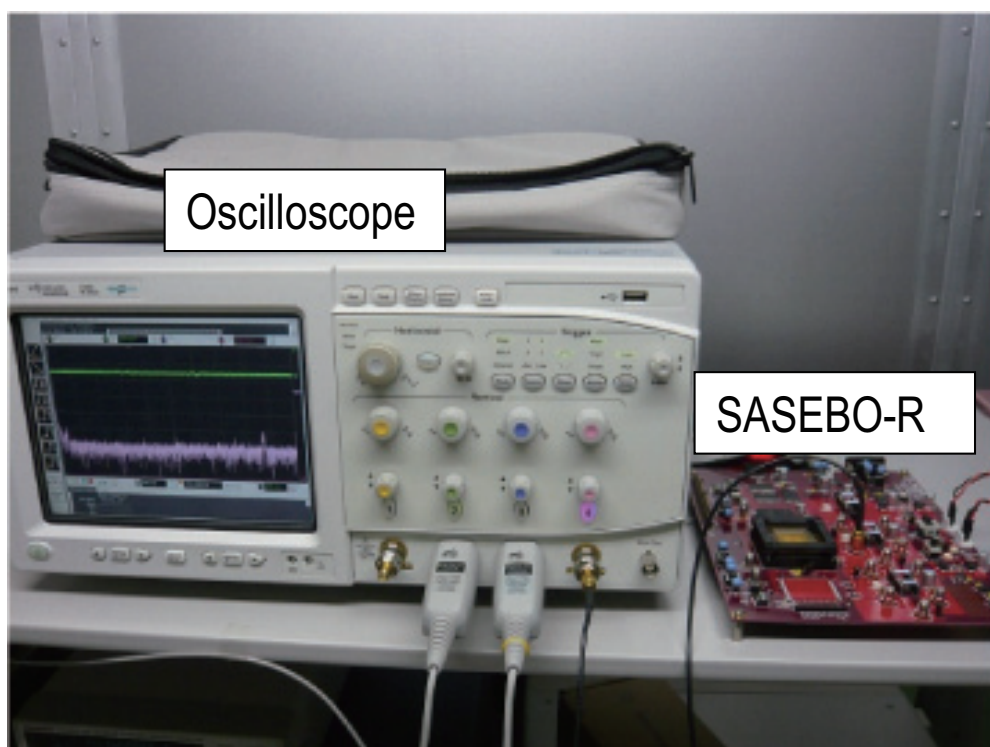


図 2.8: 測定環境

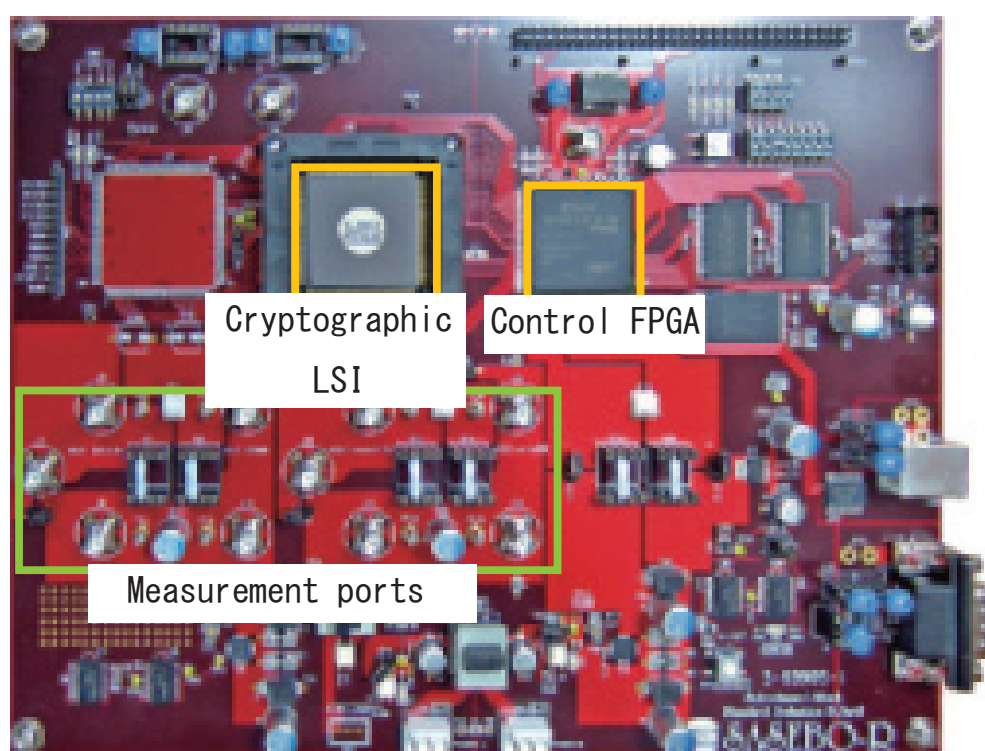


図 2.9: SASEBO-R ボード

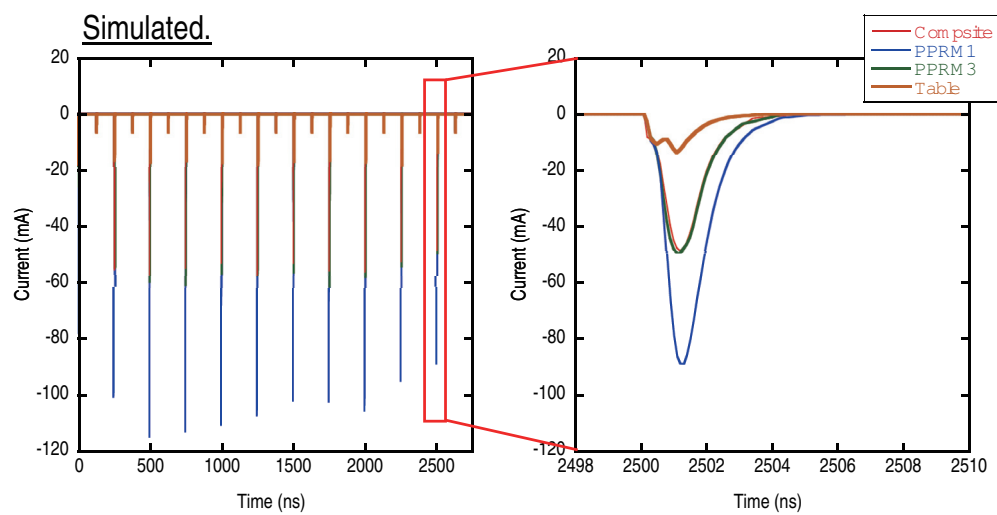
2.4 実験結果

消費電流波形のシミュレーションには容量充電モデルを使用する．容量充電モデルの時間分解能は 100 ps ($=T_{n+1} - T_n$) とした．容量充電モデルとオフチップの電源ネットワークインピーダンスを合わせた等価回路は SPICE シミュレータで計算される．容量充電モデルによる電源ノイズ波形をすべての AES モジュールに対して 10000 個の平文入力を用いてそれぞれ生成する．

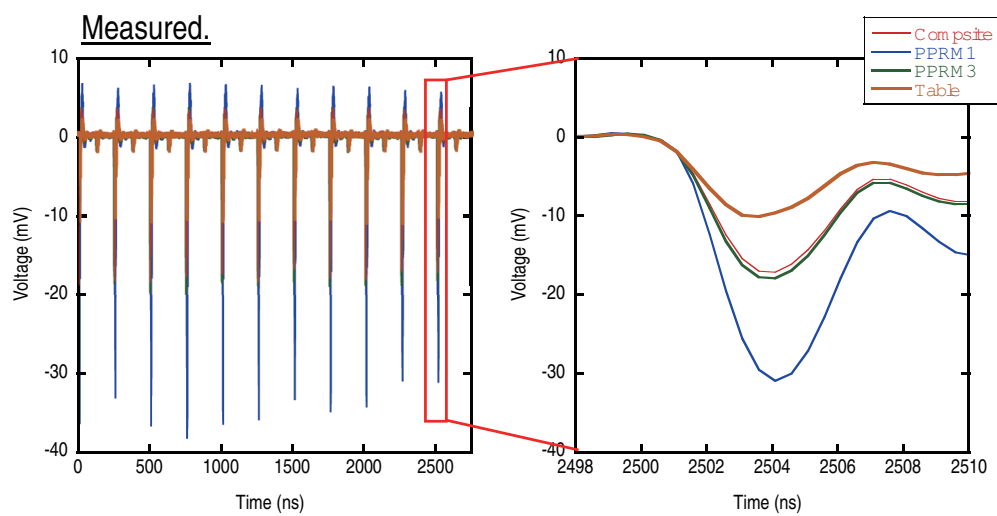
図 2.10 に容量充電モデルを用いたシミュレーションと SASEBO を用いて実測した消費電流波形の比較を示す．この波形には平文のラッチの 1 クロックサイクルとそれに続く 10 クロックサイクルの AES 暗号化処理を表している．AES 暗号化処理の 11 クロックサイクル目の最終ラウンドが終わると、すぐに暗号文が出力される．最終ラウンドの消費電流波形を拡大し並べて示す．

両方の波形において、クロックサイクルの始まりに明白に電流ドロップのピークが発生している．この電流ドロップは AES モジュール内のロジックゲートの動作による消費であり、クロック信号 F_{clk} の立ち上がりエッジに集中している．シミュレーションと実測で波形の形状が異なっているが、これはオフチップの電源ネットワークのフィルタリング効果が原因である．図 2.1 に示すシミュレーションモデルは単純化した集中定数的なインダクタンス、レジスタンス、キャパシタンスで構成された電源ネットワークを含んでいる．一方で、実測ではチップやパッケージ内の複数のボンディングワイヤ、リードフレーム、SASEBO ボード上のデカップリングの要素を含んだ分散定数的なインピーダンスが存在する．CPA においては消費電流のピークとハミング距離の相関値が重要であり、明らかな違いが波形に見られても CPA の結果に影響を与えないと考えられる．また、オフチップのインピーダンスによりサイドチャネル情報はフィルタリングされるため、インピーダンスを含まないシミュレーションをすることでより強度の高い評価となると考えられる．一方で、容量充電モデルはスイッチとキャパシタで構成される電流モデルとして容易に他の解析ツールに取り込むことが可能である．よって、チップ内でのオンチップデカップリングコンデンサやパッケージ、ボードでの対策にも応用が可能であると考えられる．

容量充電モデルを用いることで暗号化回路のサブブロックごとに電源ノイズ波形を取得することも可能である．図 2.11 に Table S-box 実装において、暗号化回路全体、S-box (SubBytes), MixColumn における電源ノイズ



(a)



(b)

図 2.10: AES 全ラウンドと最終ラウンドでの電源ノイズ波形 (a) シミュレーション結果 (b) 実測結果

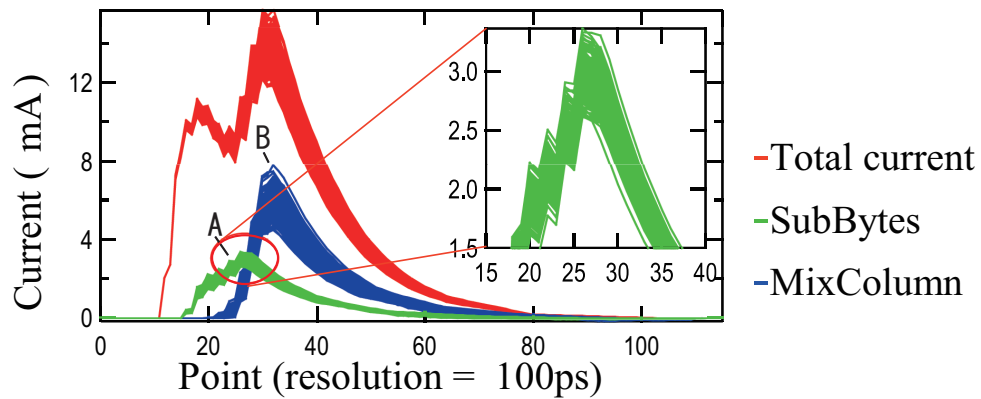


図 2.11: 最終ラウンドでの Table S-box 実装での回路ブロックごとの消費電流シミュレーション

をそれぞれプロットしたものを示す。SubBytes(図中 A), MixColumn(図中 B) の順に演算が行われている仕様通りのタイミング分布で消費電流が発生していることが見て取れる。回路ブロックごとに消費電流を求めることによりどの回路ブロックがサイドチャネル情報を漏洩しているかを評価することができ、設計者に有意な情報が得られると考えられる。

シミュレーションのコストを表 2.3 に示す。これらのシミュレーションは AES 暗号化処理 1 回分、20 MHz クロックによる暗号化 10 サイクルを含む、20 サイクル分のシミュレーションである。消費電流シミュレーションは容量充電モデルを使うことで、高速化された SPICE シミュレータを用いたフルランジスタレベルの AES モジュールのネットリストに比べて 200 倍高速化されている。この比較から 10000 波形以上必要となる CPA のシミュレーションにフルランジスタネットリストを使うことは現実的ではないと言える。

フルランジスタネットリストを用いて寄生容量を含んだシミュレーションを行う場合、この差は更に広がる。容量充電モデルはスタンダードディレイフォーマット (SDF) を用いてゲートレベルシミュレーションにバックアノテートを行っているため、モデル生成の段階で寄生成分による遅延や消費電力の影響を含んでいる。

表 2.3: シミュレーションのコスト

Sim. model	S-box 実装			
	Comp	PPRM3	Table	PPRM1
Full Tr. netlist*	1288 s	1076 s	938 s	5734 s
容量充電モデル**	4.2 s	4.4 s	4.0 s	26 s
高速化比率	306 倍	244 倍	234 倍	220 倍

Simulated by *HSIM, **HSPICE.

2.4.1 サイドチャネル攻撃評価

CPA では, 16 バイト (=128 ビット) ある鍵を 1 バイト 毎に分割し, 1 バイトの部分鍵に対して考えられる 256 通りの値に対して式 1.1 に基づいて消費電流とハミング距離の相関値を計算し, 消費電流波形の数による相関値の変化を評価する. 図 2.13 で”Composite S-box”実装の AES モジュールについてシミュレーションと実測の相関値を比較する. 0 バイト目の部分鍵に対する相関値の計算結果で, 黒の太線が正解鍵に対する相関値である. 相関値を求めるのに使用する波形数が実測において 2000 を超えた付近で正解鍵の相関値が他の候補の相関値から分離し鍵が特定できることがわかる.

他の Sbox 実装における同様の解析結果を図 2.12, 図 2.14, 図 2.15 で示す. すべての AES モジュールで正解鍵の相関値が他の候補から分離している様子がわかる. ”PPRM1 S-box”と”Table S-box”において他の実装よりも正解鍵が早く見つかっていることがわかる.

これらの結果より, AES 暗号化回路の秘密鍵は電力解析攻撃に対策を施さない場合, 実行可能な消費電流の波形数で特定できる可能性があると言える. シミュレーションと実測において相関値の傾向がよく一致するので, 容量充電モデルのアプローチは標準的な CMOS デジタル回路実装の暗号化回路において, レイアウト後のシミュレーションベースのサイドチャネル攻撃耐性評価に非常に有効であると考えられる.

図 2.16 に 16 ブロックある部分鍵に対しての CPA の結果を示す. 実測に比べて容量充電モデルでは少ない波形数で鍵が検出されていることがわかる. このことからシミュレーションによるサイドチャネル攻撃評価はオフチップインピーダンスによるフィルタリング効果を持たないためにより強度の高い評価であることが言える. 暗号回路の安全性評価においては強度の高い評価を行い安全性のマージンを持つことが重要である. その点からも容量充電モデルを用いた評価が有用であることが言える. 4

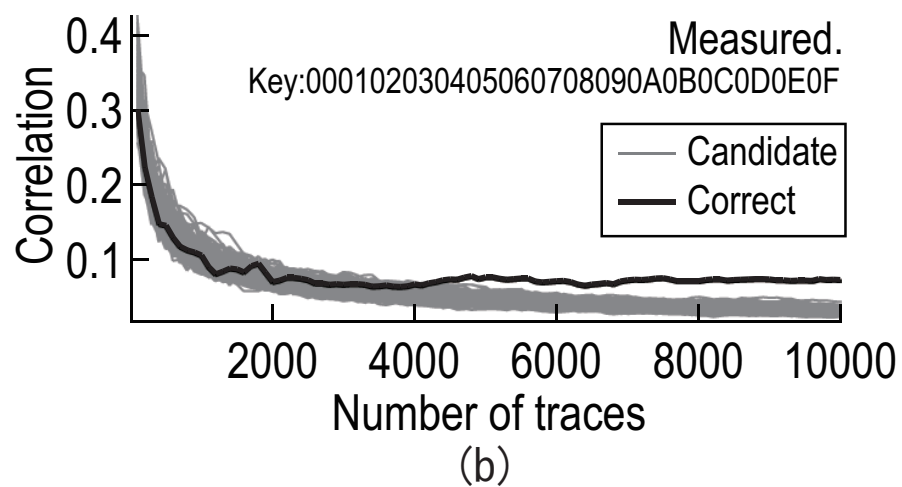
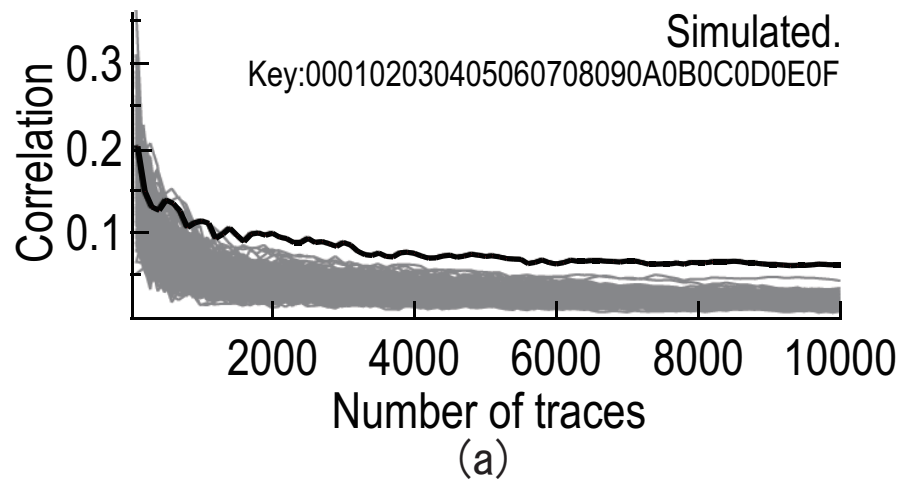


図 2.12: 各鍵候補の波形数に対する相関の最大値 (Composite S-box) (a) シミュレーション結果 (b) 実測結果

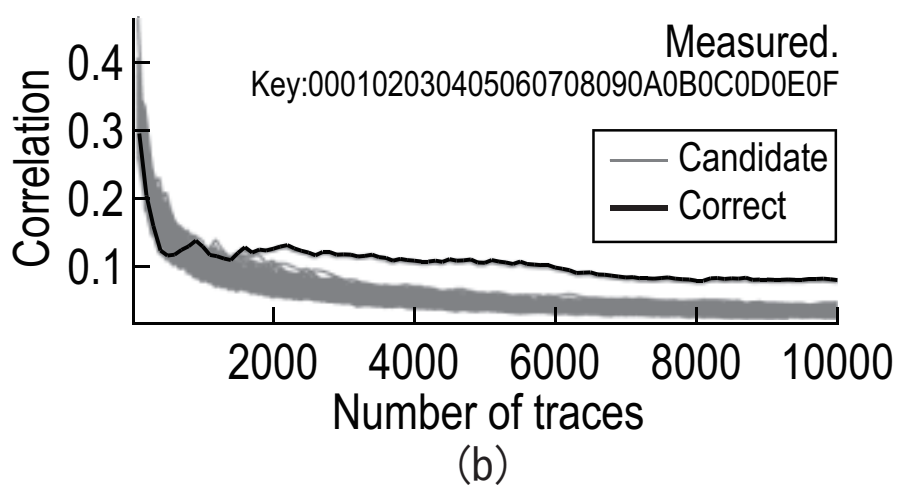
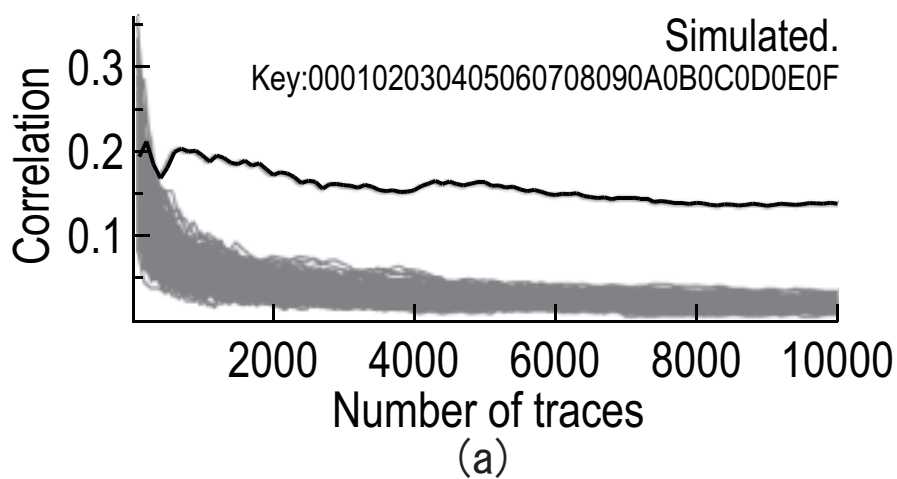


図 2.13: 各鍵候補の波形数に対する相関の最大値 (Table S-box) (a) シミュレーション結果 (b) 実測結果

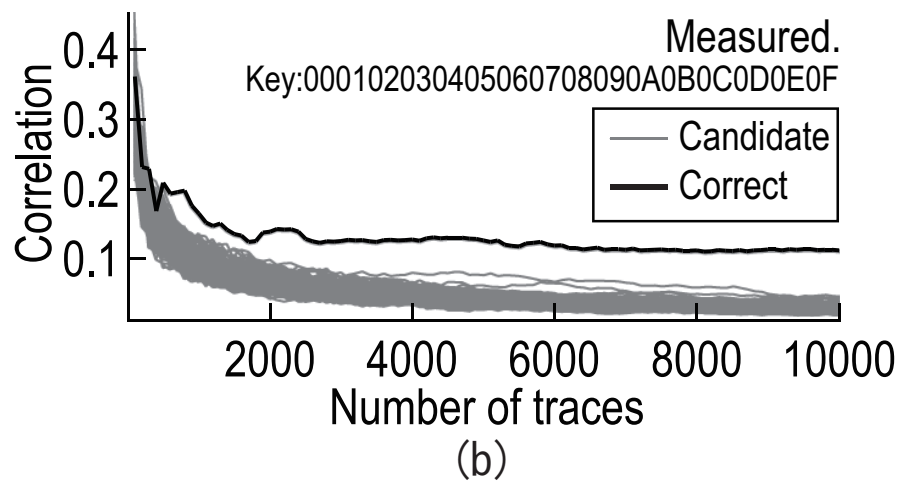
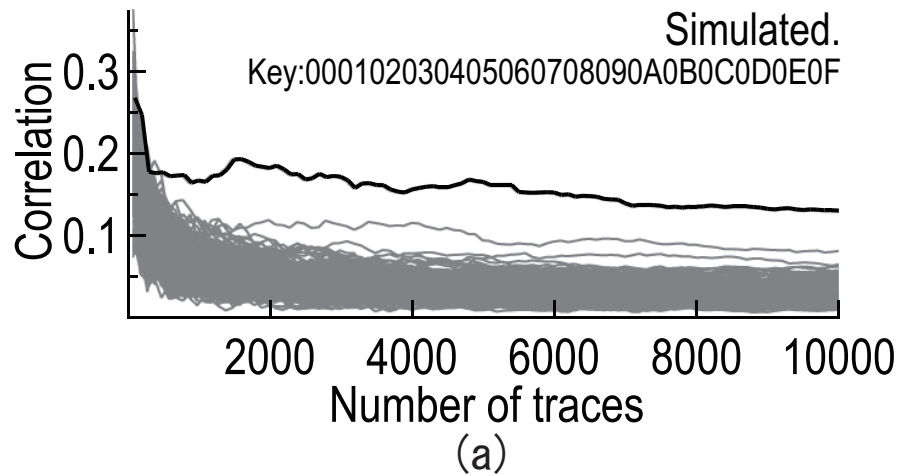


図 2.14: 各鍵候補の波形数に対する相関の最大値 (PPRM 1 stage S-box)
(a) シミュレーション結果 (b) 実測結果

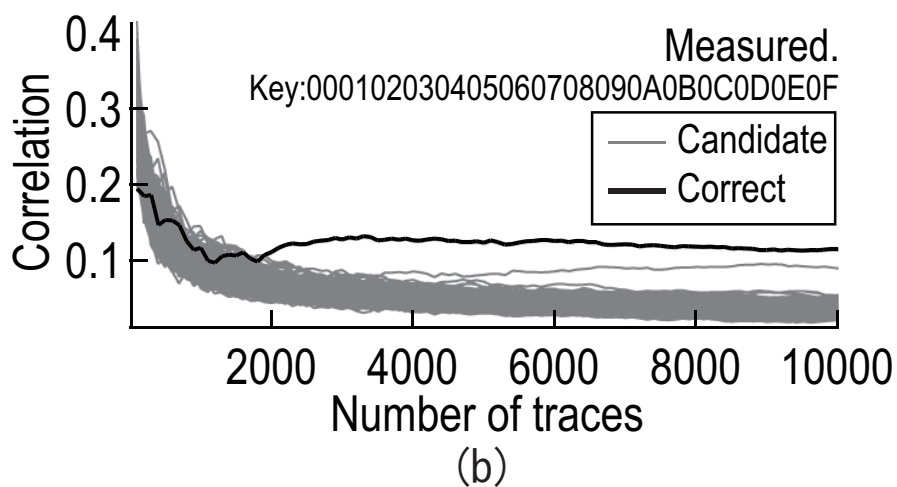
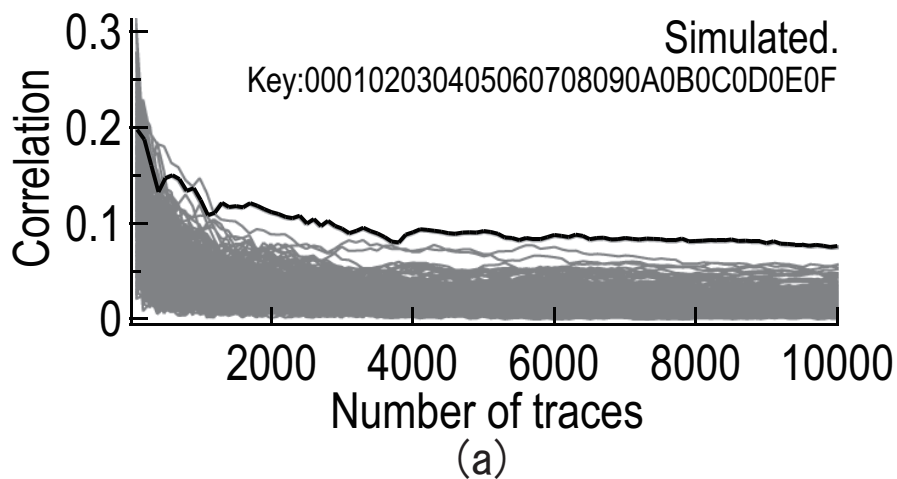


図 2.15: 各鍵候補の波形数に対する相関の最大値 (PPRM 3 stage S-box)
 (a) シミュレーション結果 (b) 実測結果

種類の異なる S-box 実装において Composite S-box 実装が一番攻撃にかかる波形数が多く、いくつかのバイトにおいては攻撃が終了しなかったが、Table S-box 実装ではすべての鍵がもっとも早く検出される結果となった。これらの結果から今回対象とした 4 つの S-box 実装のうち Composite S-box がもっともサイドチャネル攻撃耐性が高く、Table S-box がもっとも脆弱であると言える。実装間のサイドチャネル攻撃への耐性もおおむねシミュレーションと実測で一致しているため容量充電モデルにより実装の違いによるサイドチャネル漏洩情報の違いが表現できていると言える。

次に鍵を変更した場合の CPA 攻撃結果について述べる。図 2.17 に鍵を変更した場合の Table S-box 実装の AES への CPA 結果を示す。鍵を変更した場合、入力平文が同じでも回路の内部遷移が変わるため攻撃結果が変化する。鍵を変更した場合でも容量充電モデルによるシミュレーションの結果は測定と傾向が一致していることが分かる。

2.4.2 他プロセスでのサイドチャネル漏洩評価

容量充電モデルによるシミュレーションがプロセスの変化にも追従できるかを評価するために 130 nm プロセスで製造された暗号化 LSI についても同様の評価を行う。このチップは SASEBO プロジェクトで製造されたものである [39]。CPA を行った結果を図 2.18 に示す。130 nm プロセスにおいても容量充電モデルによるシミュレーション結果は測定とよく一致しており、プロセスが変わっても汎用的に使用できる技術であると言える。

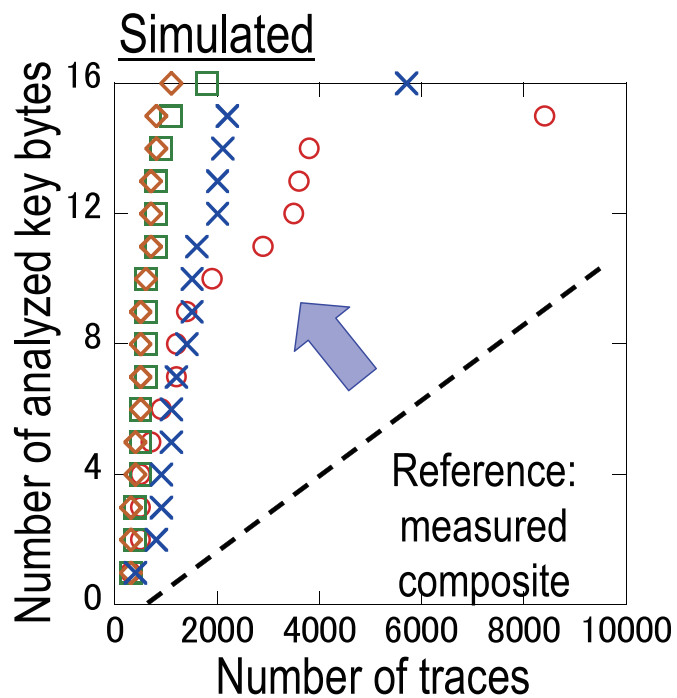
そのため、容量充電モデルを用いたシミュレーションベースの CPA は、対象回路の物理的なサイドチャネル攻撃への耐性が評価でき、よりサイドチャネル攻撃に対して耐性の高い暗号化モジュールを設計するのに有用であるといえる。

2.5 まとめ

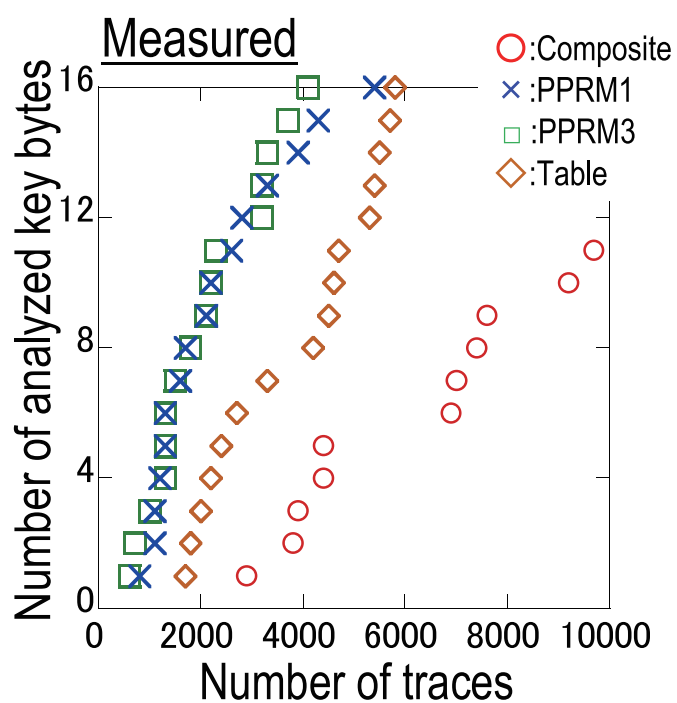
本章では、デジタル回路が動作した際のトランジスタの寄生容量への充電過程に着目した容量充電モデルを用いた高速な電源ノイズ解析手法を暗号化回路のサイドチャネル漏洩評価に応用することを提案した。

本研究で提案する手法により、CPA などのサイドチャネル攻撃のシミュレーションが実現可能となる。消費電流波形の導出にかかる時間は従来の

Key:000102030405060708090A0B0C0D0E0F



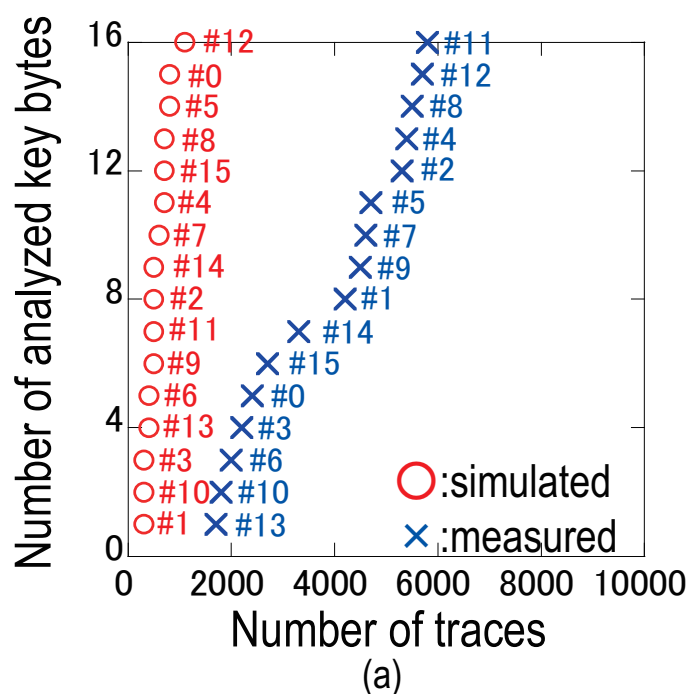
(a)



(b)

図 2.16: 4 種類の S-box 実装を行った AES 回路へ対する CPA 結果
(a) シミュレーション (b) 1 オーム法による実測

Key:000102030405060708090A0B0C0D0E0F



Key:000102030405060708F7158809CF4F3C

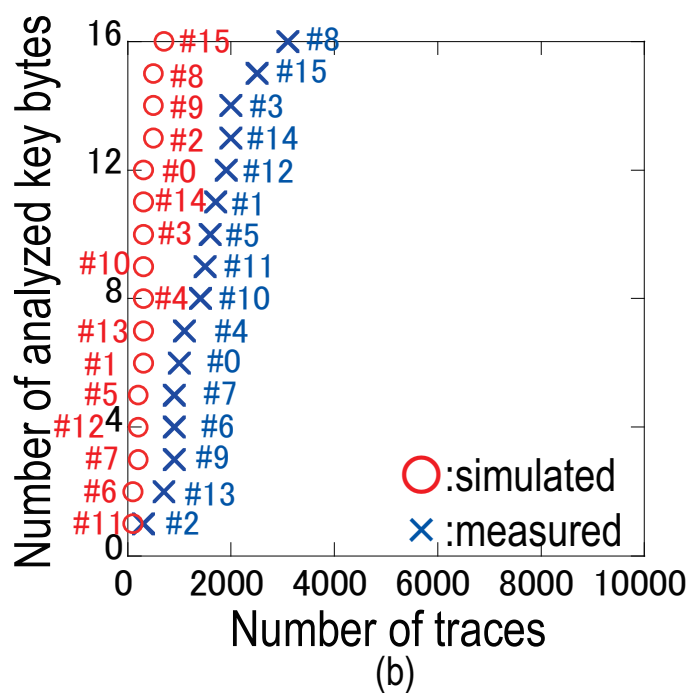


図 2.17: 二つの異なる鍵を用いた場合の Table S-box AES に対する CPA 結果

Key:000102030405060708090A0B0C0D0E0F

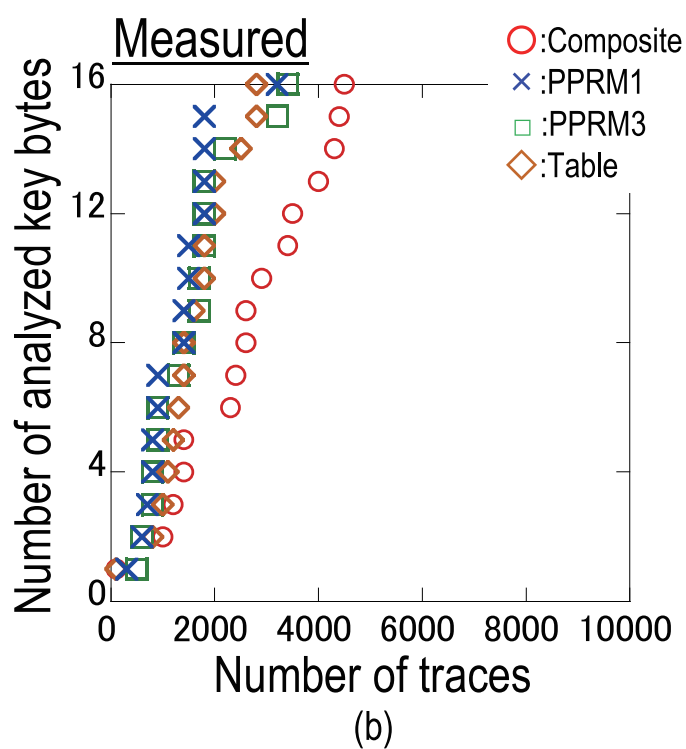
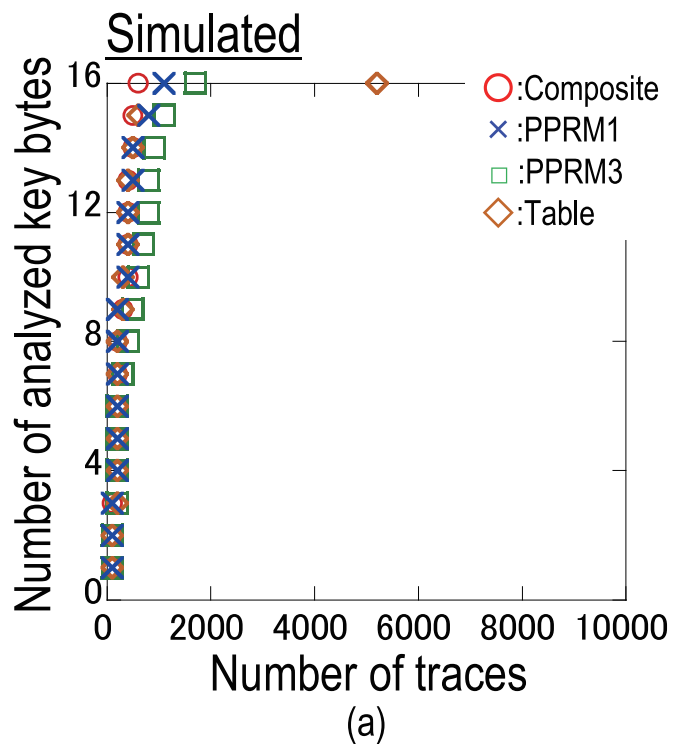


図 2.18: 130 nm CMOS で試作したチップでの CPA 結果 (a) シミュレーション (b) 1 オーム法による実測

フルトランジスタレベルの解析に比べて 200 倍の高速化を達成した。これにより CPA に必要な数万波形以上のシミュレーションが可能となった。この成果により暗号回路の設計段階においてサイドチャネル漏洩評価が可能になり、チップ試作などによる手戻り設計コストなどを下げる上で非常に重要な技術であると言える。本研究では攻撃手法を CPA に限定したが、容量充電モデルはデジタル回路において汎用的な消費電流モデルであるため、消費電流を対象とする他の攻撃においても使用できると予想される。

また、容量充電モデルがスイッチとキャパシタのみで構成できるため容易に他の解析ツールに取り込むことが可能である。そのため、磁界シミュレーションツールと組み合わせることで、EMプローブによる回路内局所攻撃などのより高度な攻撃への評価も可能となる可能性がある。

第3章

VLSI暗号回路における回路近傍での電源ノイズ測定

3.1 はじめに

暗号化回路においてチップ外部に漏れ出す消費電流を観測することで、回路動作を導出し暗号化回路内の秘密情報を抜き出す攻撃が脅威となっている。攻撃の脅威モデルとしてチップ外部での測定手法は数多く提案されているが、チップの内部電圧を測定したような例は無い。しかしながら、チップの外側で観測した波形は図 3.1 のように電源ネットワークのインピーダンスにより波形が変化する。この変化は実装方法によって大きく変わるために実際の製品で実装が変わる場合や攻撃者が暗号化回路の実装を変更した場合、チップ外部で行った測定での評価では不十分であると言える。そのため、暗号化回路の安全対策においてはチップ内部での電圧変動を正確に観測し、サイドチャネル情報の漏洩メカニズムを解明することが重要だと考えられる。

本章では、従来チップ内の電源ノイズ観測に用いられていたオンチップ電圧モニタリング技術を暗号回路を搭載したチップ上に実装し、暗号コアの電源ノイズを精度良く観測し、チップ外部での観測波形との違いについて考察を行う。

3.2 オンチップ波形モニタリング技術

チップ内部の電圧変動をモニタリングする技術としてオンチップモニタリング技術が提案されている [56],[57]。オンチップモニタの回路図を図 3.2(a) に示す。レベルシフタとなる SF(Source Follower) 段により対象回路へプロービングを行う。SF は MOS のゲートで入力を受けるために対象回路からはハイインピーダンスに見え、影響を与えにくい。次の段では SF でシフトされた対象回路の電源電圧 V_{sfo} をラッチコンパレータに

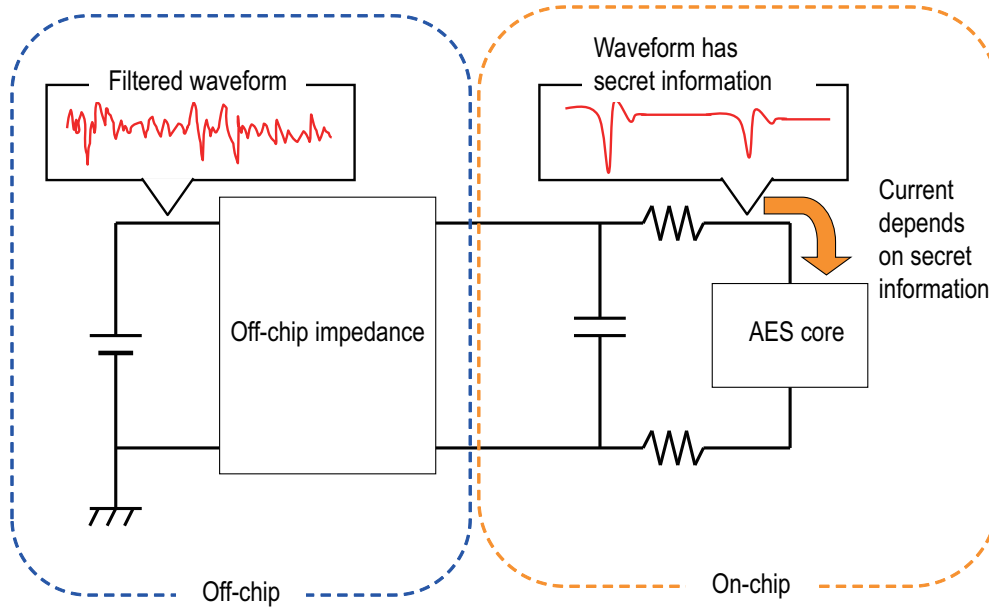


図 3.1: チップ内外での波形の変化イメージ

より参照電圧 V_{ref} と比較を行う．複数回比較を行い V_{ref} をスweepした場合の出力に”1”が出る確率は図 3.2(b) の様になる．ラッチコンパレータの出力が”1”である確率が 50%に近いとき V_{sfo} と V_{ref} が等しいと判断し電圧を特定する．ラッチコンパレータの比較タイミングはサンプリングクロック T_{clk} により制御される． T_{clk} をずらしていくことにより，連続した電源ノイズ波形が得られる (図 3.3)．

これまで，オンチップモニタリング技術はインバータチェイン [58] の様な基本的な回路や DFF を直列に接続したループシフトレジスタ [59]，32bit 汎用マイクロプロセッサ [60] などの多様な回路においてチップ内電圧測定に用いられた実績がある．

3.3 回路近傍での電源ノイズによる電力解析攻撃

オンチップモニタ回路により暗号化回路の電源ノイズ波形を取得するためには，一枚のチップ上に暗号回路およびその制御回路，オンチップモニタ回路を搭載したテストチップを設計する必要がある．本節では，暗号化回路とオンチップモニタを搭載したチップの概要を述べ，制御するためのシステムについて述べる．

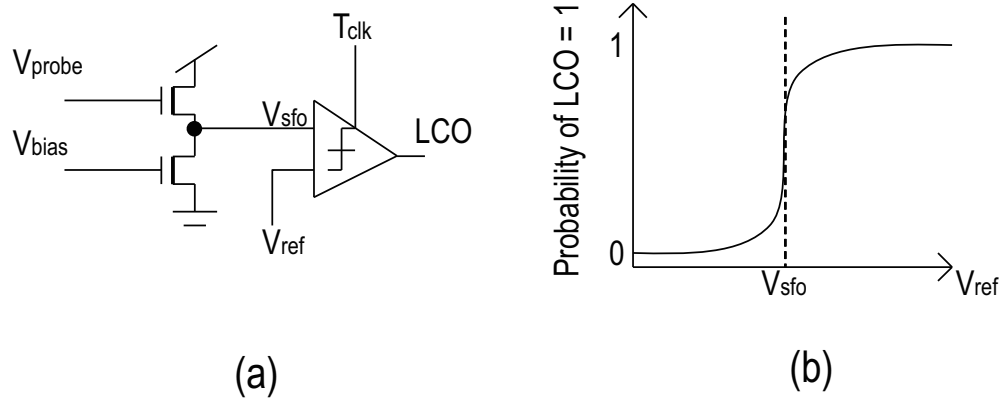


図 3.2: オンチップモニタフロントエンド (a) 回路図 (b) ラッチコンパレータによる比較

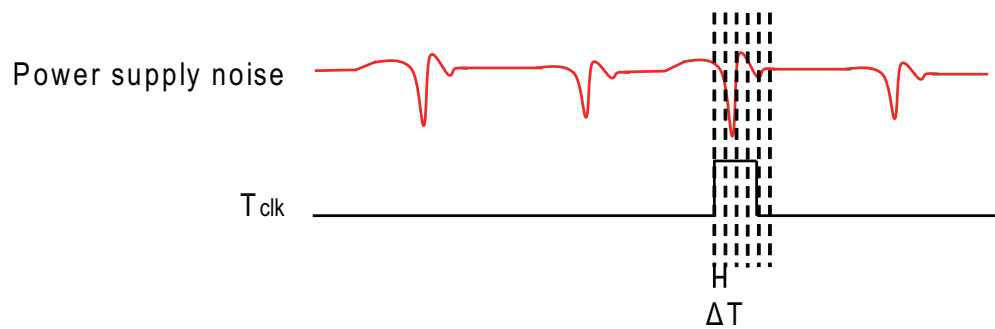


図 3.3: オンチップモニタによる連続波形取得イメージ

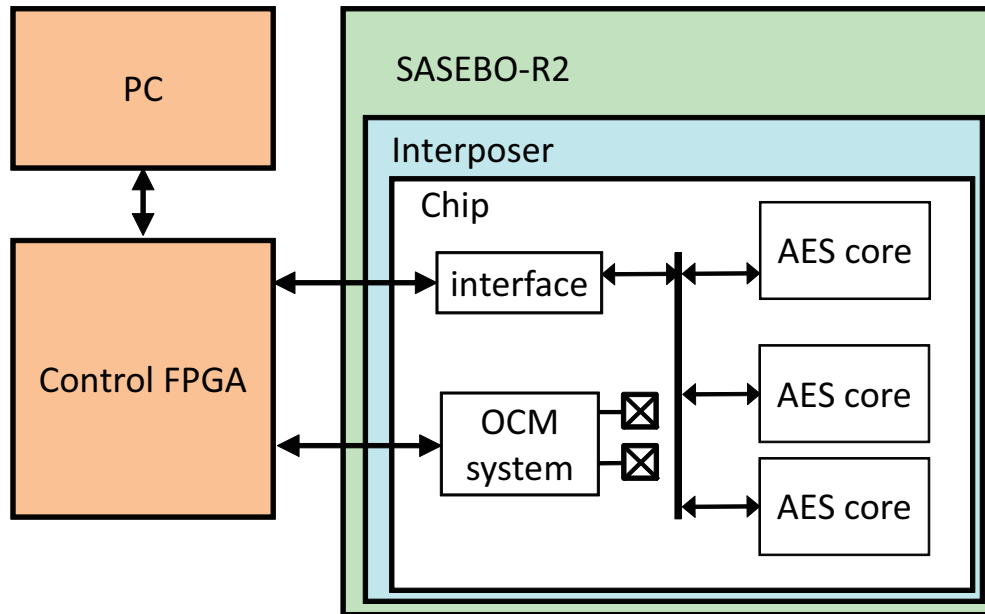


図 3.4: オンチップモニタ搭載暗号化チップのブロック図

3.3.1 テストチップ

図 3.4 にオンチップモニタ搭載暗号化チップのブロック図を示す。標準的な $1\ \Omega$ 法による測定を比較として行うために、SASEBO-R2 ボードに接続できるようなインタポーザ基板を用いた。SASEBO-R2 基板には $1\ \Omega$ 法を行うためのポートがインタポーザ基板との接続端子近傍に設けられている。複数の AES を制御するための制御インターフェース回路、オンチップモニタを外部の FPGA で同期しながら制御するシステムとなっている。

図 3.5 にテストチップのレイアウト図を示す。テストチップには複数の AES を実装しているが、標準的で電力解析攻撃に対して対策を施していない Composite S-box 実装を評価対象として選択する。

3.3.2 測定評価環境

次に測定評価環境について述べる。実際の評価系の写真を図 3.6 に示す。

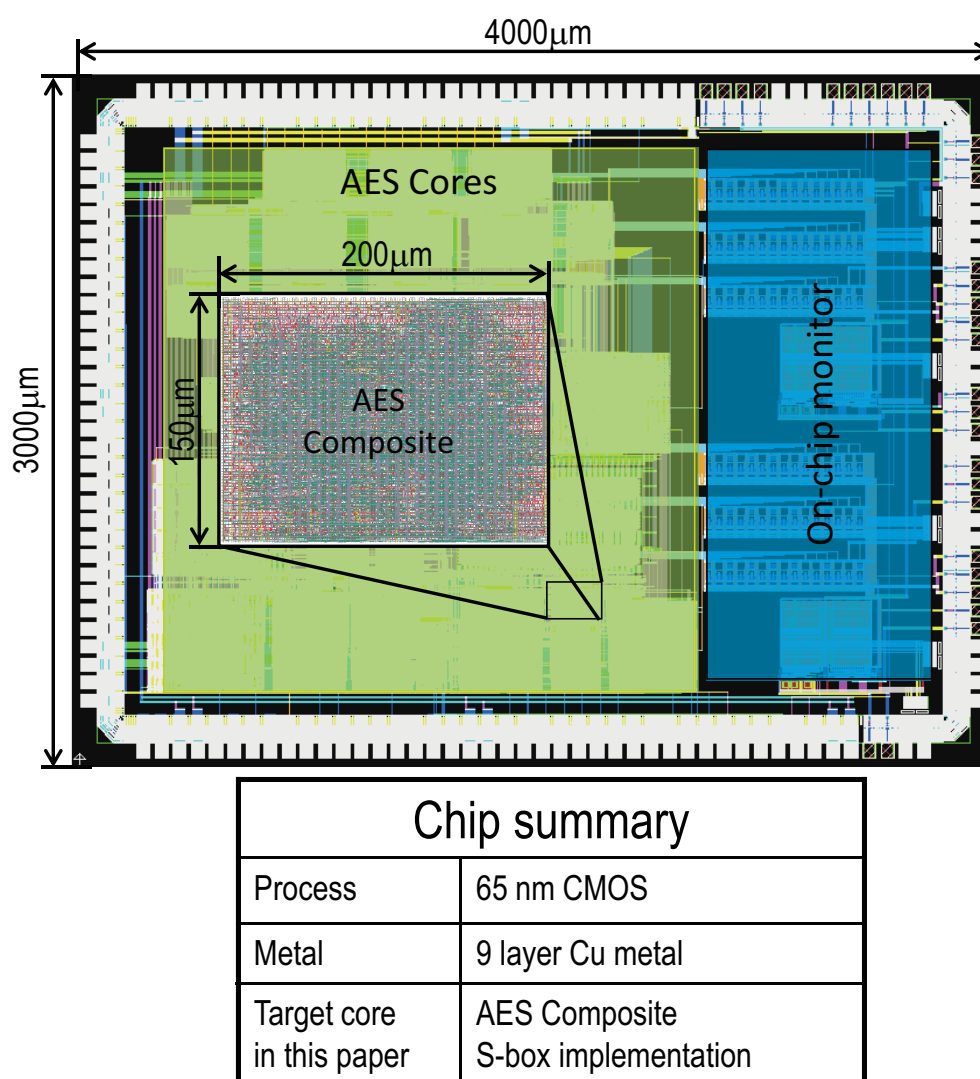


図 3.5: テストチップレイアウトとデザインサマリ

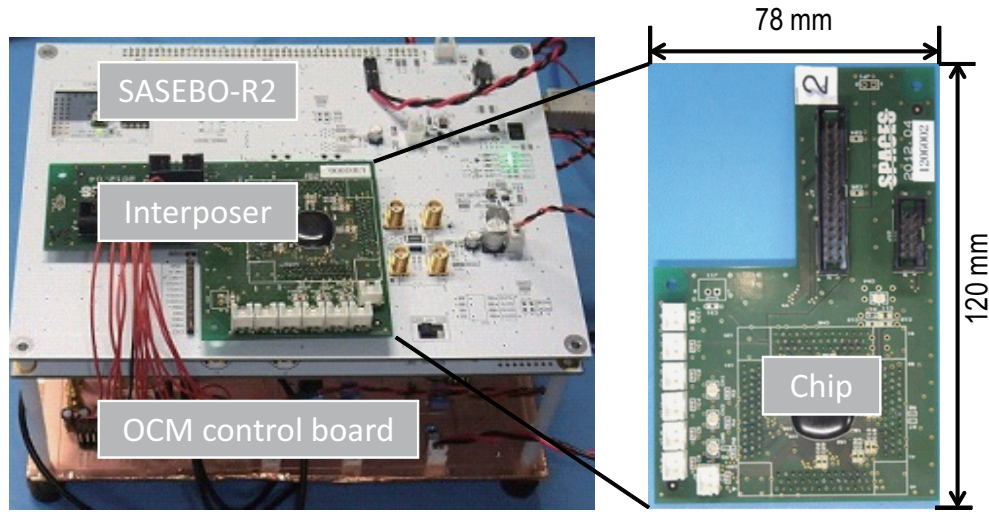


図 3.6: 測定評価環境

3.3.2.1 1 Ω 法による測定環境

従来手法である 1 Ω 法による測定のブロック図を図 3.7 に示す. SASEBO-R2 上の観測端子とオシロスコープを接続し, チップからの AES 暗号化回路の動作トリガ信号を用いて測定を行う. 電源電圧をオシロスコープで観測するため, 直接接続すると電源電圧の DC 成分のオフセットがあり, 測定の電圧分解能を下げてしまう. そこで, DC 成分を除去するためのキャパシタを直列に挿入している.

3.3.2.2 オンチップモニタによる測定環境

オンチップモニタで波形を取得するためには, ラッチコンパレータの出力を観測し, 参照電圧 V_{ref} と測定対象の電圧の高低を判断し, V_{ref} の設定, 電圧値の導定, サンプルングタイミング T_{clk} の設定を行う機構が必要となる. このときに PC との通信は数 100ms と長く測定時間のボトルネックとなる. そのため, FPGA による制御ロジックを構築し, 測定系の高速化を行った (図 3.8). サンプルングタイミングは AES 暗号化回路の動作と同期する必要があるため, AES の実行時のトリガ信号を元に生成する. AES 動作中の任意のタイミングでサンプルングクロックを生成するには長周期の遅延をつける必要がある. 外部測定器を用いると同期ずれ, ジッタが大きくなってしまう. そこで 240 MHz のクロックを基準と

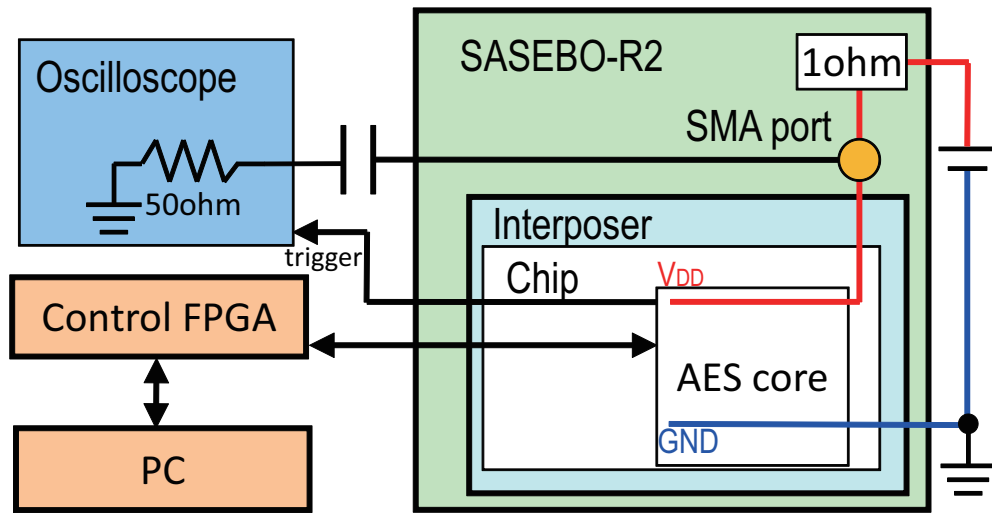


図 3.7: 1 Ω法による測定環境ブロック図

し、AESのクロックを分周し作成した。これにより 240 MHz のクロックを用いて遅延を行えば同期ずれは発生しない。AESトリガ動作信号の立ち上がり信号を元に基準となる 240 MHz のクロックを使用して 4.166 ns 単位の遅延をつけたトリガ信号を生成する。さらにそのトリガ信号からプログラマブル遅延 IC を用いて最小 10ps 単位の遅延を生成 (図 3.9) し、最大 10ps 時間分解能を持ち任意の長さの遅延を実現可能な測定系を構築した。

3.3.2.3 測定条件

オンチップモニタと 1 Ω法の比較のための測定条件を示す。1 Ω法に用いたオシロスコプの分解能は電圧方向で 100 μV 、時間方向で 500 ps である。オンチップモニタによる測定はサンプリング方式であるがゆえに、電圧、時間分解能と測定時間のトレードオフとなるため、電圧方向で 200 μV 、時間方向で 640 ps とした。測定対象の AES は 2 MHz で動作させる。

3.3.3 実験結果と考察

本節ではオンチップモニタと 1 Ω法による測定結果を示し、考察を行う。図 3.10 に測定した波形を示す。AES の動作周波数は 2 MHz であり 500 ns 周期で AES の動作による 10 クロックサイクルの電圧変動ピークが

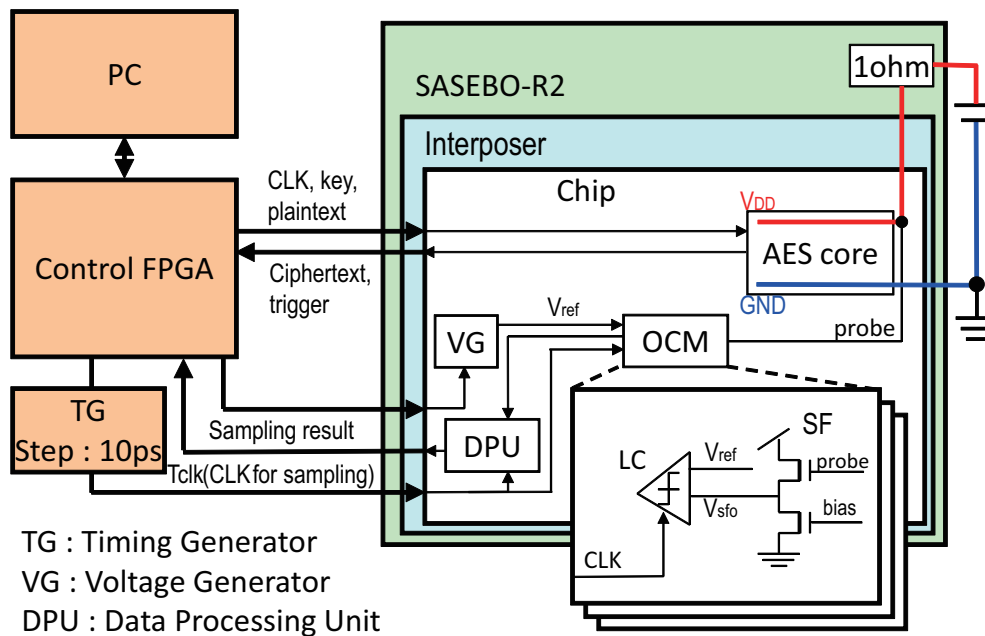


図 3.8: オンチップモニタによる測定環境ブロック図

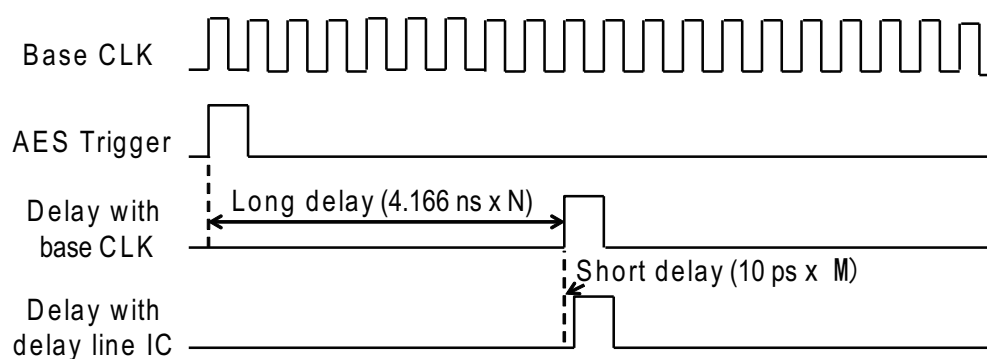


図 3.9: サンプリングタイミング生成フロー

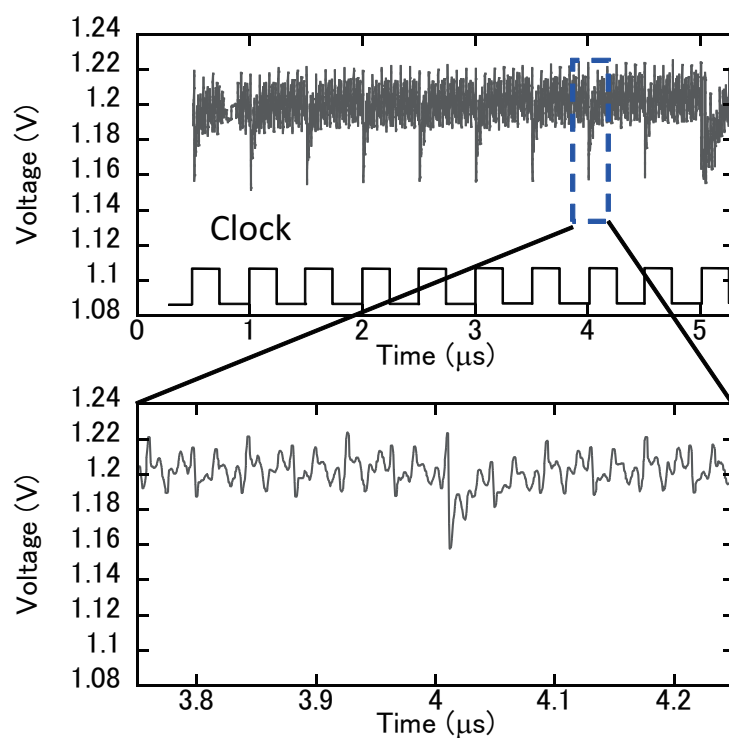
観測できる。オンチップモニタと $1\ \Omega$ 法による波形を比較すると電圧変動ピーク部分ではオンチップモニタの波形が急峻に変動を起こしている事がわかる。このことはチップ外部には高周波成分は PDN のインピーダンスによりフィルタがかかって出力されないことを示唆する。またピークの振幅においてもチップ内部ではチップ外部より 10 倍程度のドロップを起こしている事が見て取れる。これはチップ内外に寄生する静電容量により電荷の再分配が行われ外部まで消費電流が伝播しないからであると考えられる。

次に、これらの測定波形を用いて CPA を行った結果を図 3.11 に示す。オンチップモニタと $1\ \Omega$ 法でほぼ攻撃に必要な波形数が変わらない結果を得た。すなわち、電力解析攻撃に対して未対策な AES では高周波成分がフィルタリングされる状況であっても低周波成分にサイドチャネル情報が載っていると考えられる。また、CPA の結果は電源ノイズ振幅自体には依存せずあくまで入力データが異なる場合の暗号化コアの消費電力の変化のみをとらえていることがわかる。

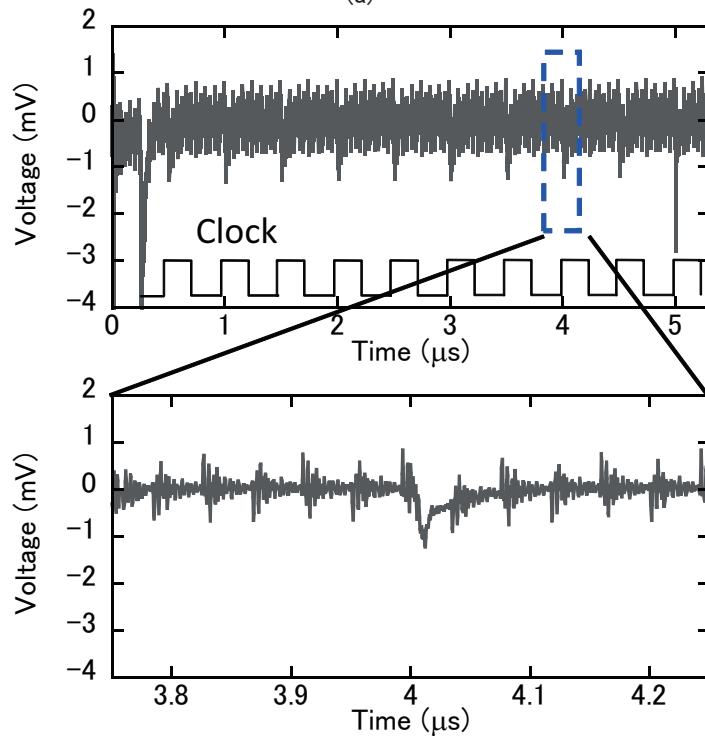
サイドチャネル情報が低周波成分に載って外部に漏れだしているかを確かめるために測定波形に 100 MHz 10 MHz 3 MHz のローパスフィルタ処理を掛けた波形が図 3.12 になる。周波数成分の分布を見るために FFT を行った結果が図 3.13 である。元波形では高周波側に高いピーク (spurs) があることがわかる。これは、制御 FPGA 内の 12 MHz クロックの 3 次、7 次高調波であり背景ノイズである。3 MHz のローパスフィルタを掛けた後は、背景ノイズは消え、ほぼ クロック周波数の 2 MHz とその 2 次高調波の 4 MHz にのみピークがあることがわかる。

ローパスフィルタを用いて CPA を行った結果を図 3.14 に示す。ローパスフィルタを掛けた場合でもオンチップモニタと $1\ \Omega$ 法で攻撃に必要な波形数に差は見られなかった。またフィルタを掛ける前と比べて鍵の検出に必要な波形数にほぼ差はない。このことから、電力解析攻撃に未対策な実装の AES の場合低周波成分にサイドチャネル情報が重畳していることが確認できる。

オンチップモニタと $1\ \Omega$ 法の測定波形の差が電力解析攻撃にどのように影響を与えるかを調べるために、電力解析攻撃の結果を詳しく評価する。電力解析攻撃では電源ノイズ波形に対して時間方向にスイープし、各測定点での相関値を評価する。時間方向の相関値の推移を図 3.15 にプロットする。黒い太線が正解鍵で内部動作を予測した場合の相関値である。相関値が上にあるほど正解鍵である可能性が高いと予想され、正解鍵が他の



(a)



(b)

図 3.10: 測定波形 (a) オンチップモニタ (b) 1 Ω 法

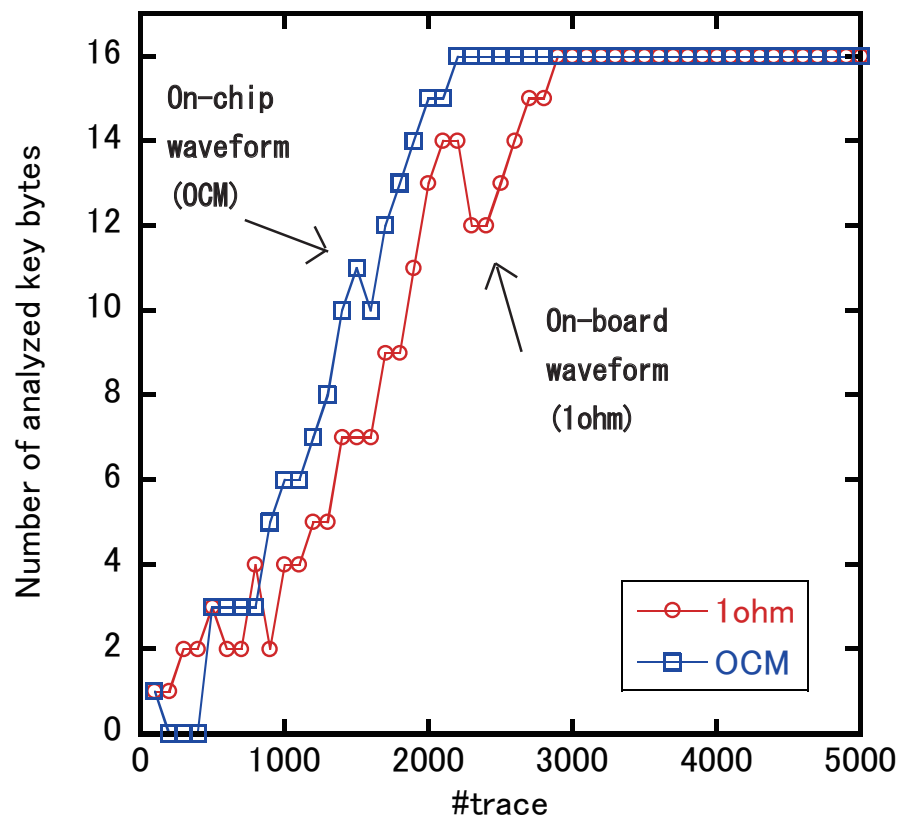
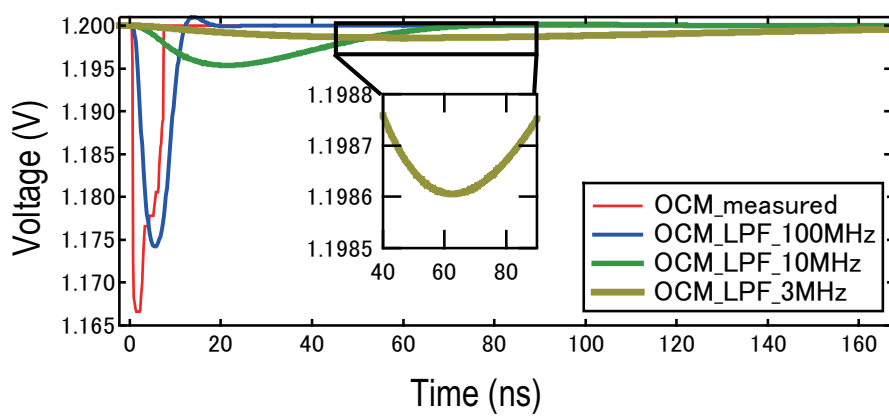
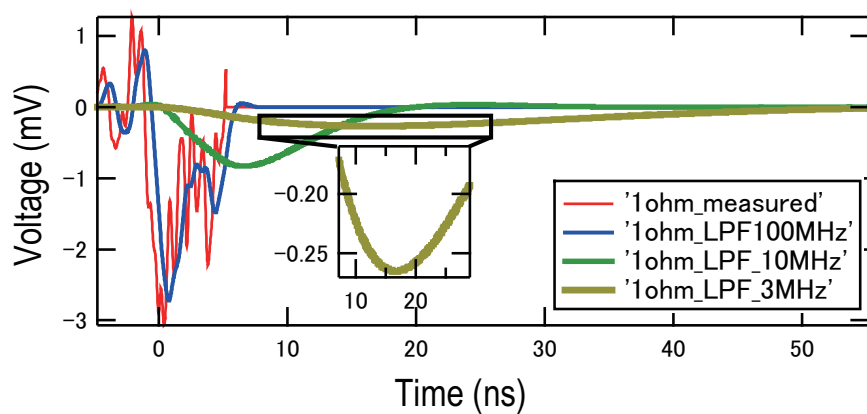


図 3.11: 測定による CPA 結果 (a) オンチップモニタ (b) 1 Ω 法

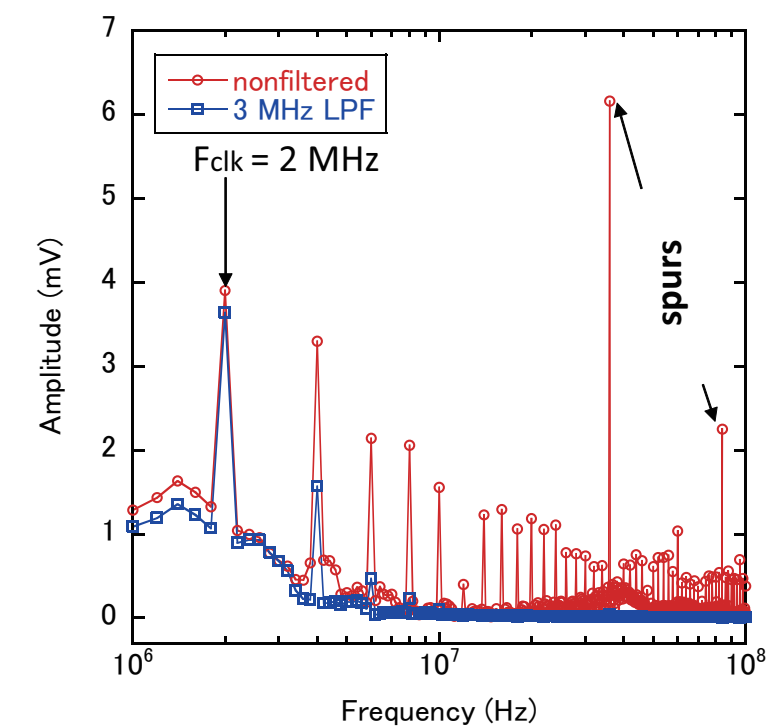


(a)

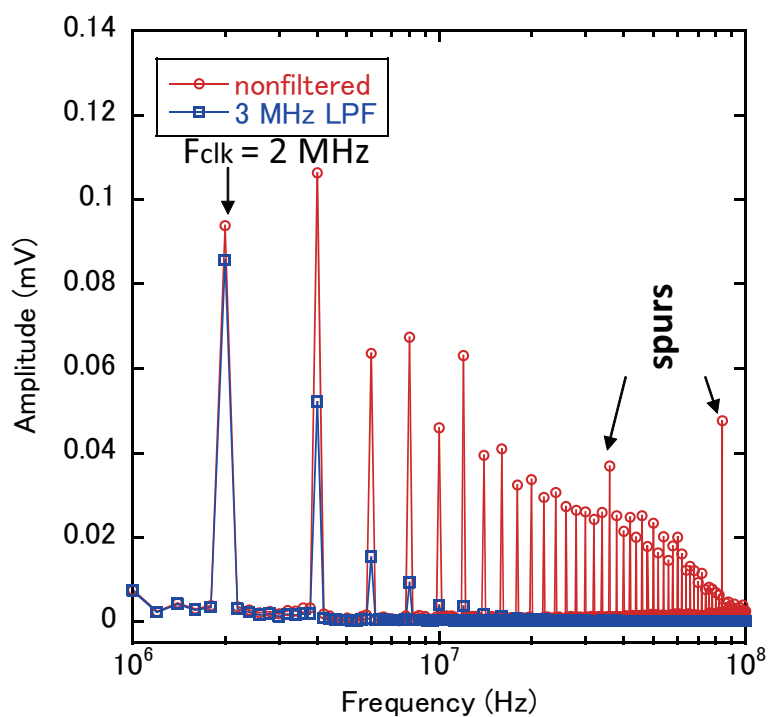


(b)

図 3.12: 100MHz 10MHz 3MHz のローパスフィルタ処理を行った波形 (a) オンチップモニタ (b) 1 Ω 法



(a)



(b)

図 3.13: FFT 波形 (a) オンチップモニタ (b) 1 Ω 法

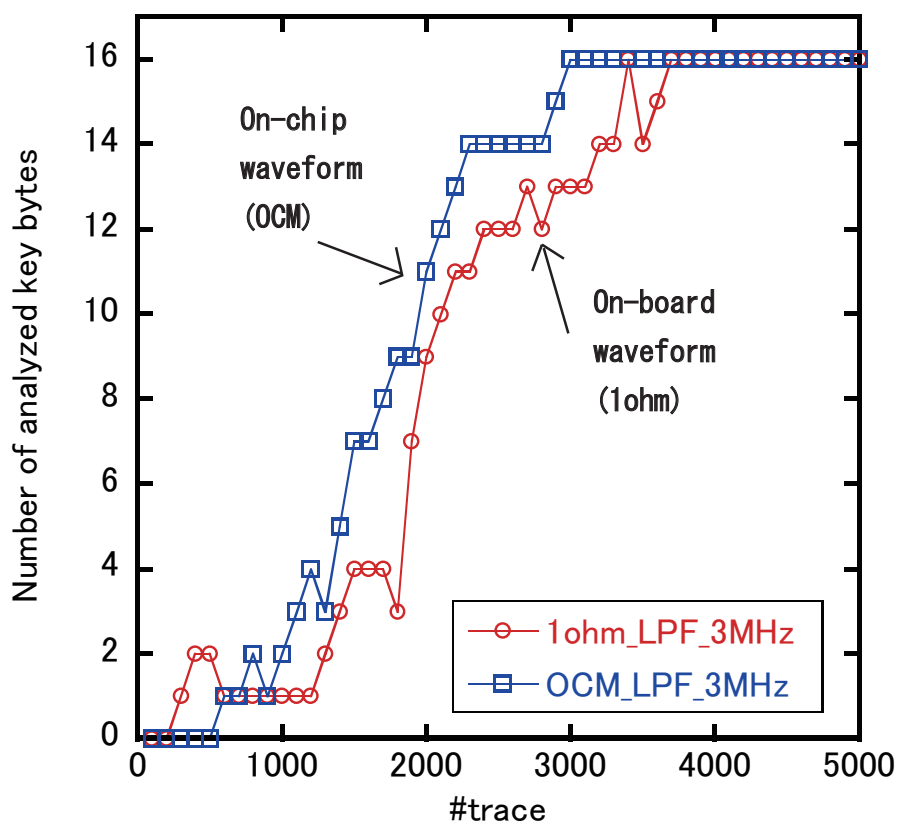


図 3.14: ローパスフィルタ後の CPA 結果 (a) オンチップモニタ (b) $1\ \Omega$ 法

候補鍵 [0:255] よりも高い場合は攻撃者に正解鍵が特定されてしまう。図 3.15を見るとオンチップモニタ、1 Ω 法どちらにおいても正解鍵の相関値が全区間の相関値の中で一番高くなっているため正解鍵が特定されている。オンチップモニタに対して1 Ω 法では外部のノイズが重畳しているため相関値が高い区間が狭くなっている。よって、オンチップモニタによる測定の方がより正確にサイドチャンネル情報を検出できていると言える。

最後に、ハミング距離に対してどの程度電源電圧ドロップが依存するかを評価する。個々での電源電圧ドロップは回路が動作していない時の電源電圧からの電圧変動ピークの差と定義する。図 3.16に通常電源電圧の場合の結果を示す。全てのS-boxでハミング距離を統一するために4章で説明するハミング距離統一平文を用いている。オンチップモニタ、1 Ω 法ともにハミング距離に依存して電源電圧ドロップが変化していることが見て取れる。この依存性があるために電力解析攻撃が成功してしまう。低電圧動作を行うことで電源電圧ドロップに変化があるかを評価した結果を図 3.17に示す。低電圧動作をさせることにより消費電流が低減されハミング距離に対する依存性が減る事が期待されるが、電源電圧ドロップの絶対値の変化のみにとどまり、ハミング距離に線形に依存している傾向は変わらなかった。よって単に電源電圧を下げるだけでは、サイドチャンネル情報漏洩を防ぐことはできない。

3.4 まとめ

本章では高精度なチップ内での電源変動波形取得機構であるオンチップモニタを暗号化LSIの電圧変動取得に使用することを提案した。

提案手法の有用性を実証するために従来手法である1 Ω 法と測定結果を比較した。比較結果より、電力解析攻撃対策を施していないAESにおいて低周波成分のみで攻撃が可能であることを示した。また、相関値の時間方向の推移を調べることにより、オンチップモニタによる攻撃がオフチップで測る手法に比べてノイズの影響が少ないことを示した。このことから、オンチップモニタは暗号化回路の電力解析攻撃の測定をするうえでより高性能な測定手法だといえる。

今後の展望としては、対策を施して安全だと考えられているAESに対してもチップ内部で取得した波形の高周波成分で攻撃できるかを評価することである。現在想定されている攻撃者の測定方法では安全であっても、将来的に攻撃者の測定技術は進歩すると考えられ、チップ内でのコ

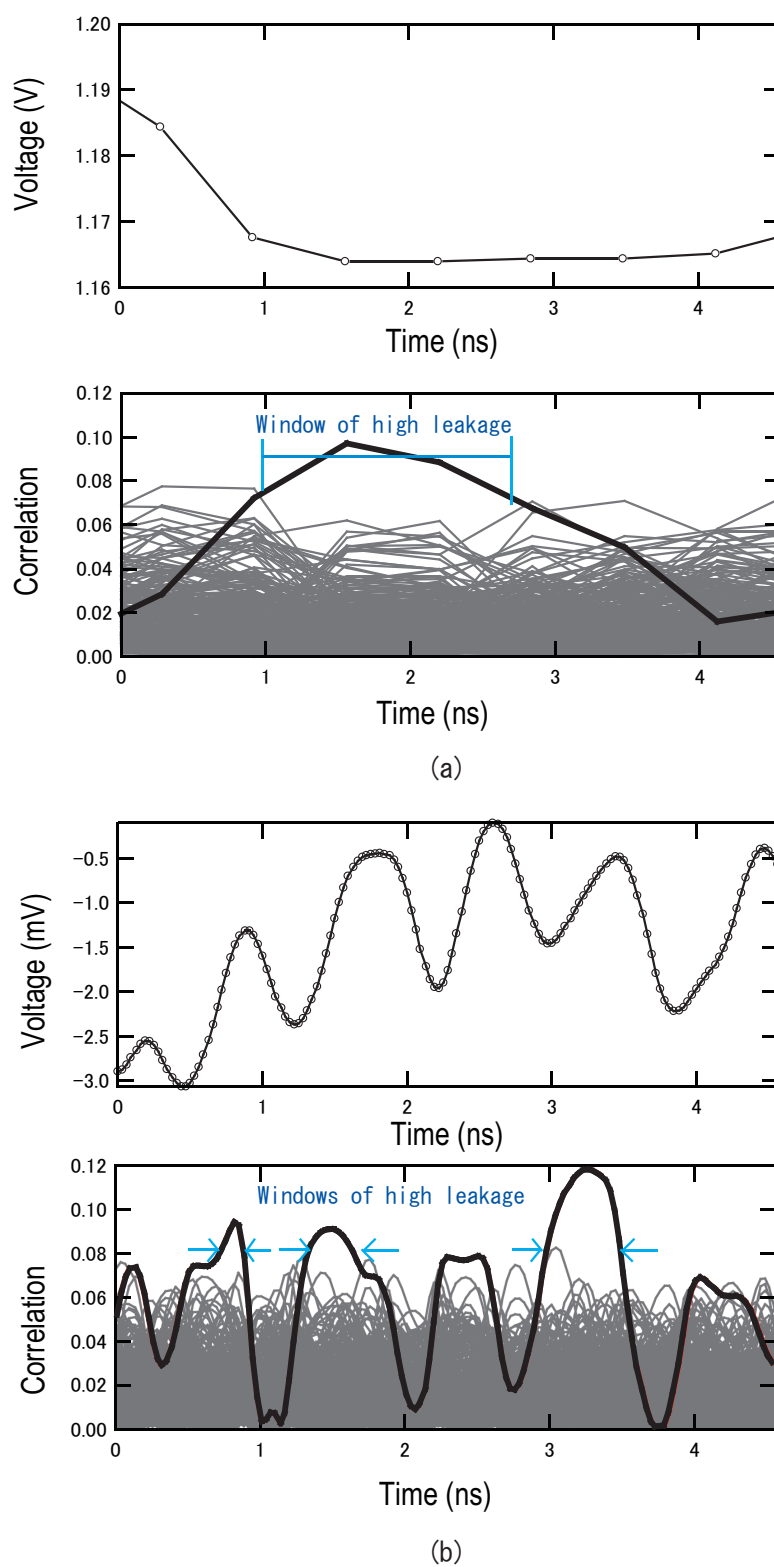


図 3.15: CPA に用いた波形と時間方向における相関値推移 (a) オンチップモニタ (b) 1 Ω 法

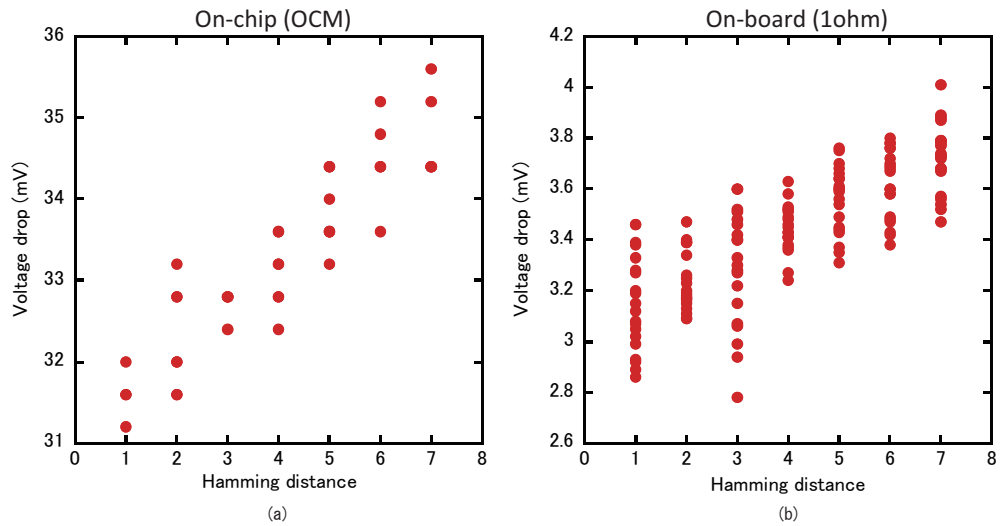


図 3.16: ハミング距離と電源電圧ドロップ 通常電源電圧 (1.2V) 時 (a) オンチップモニタ (b)1 Ω 法

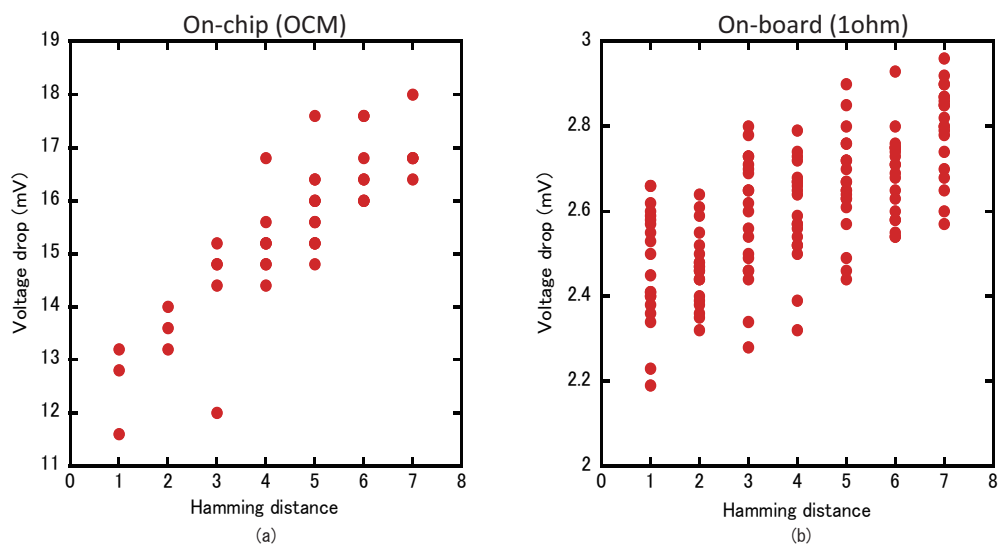


図 3.17: ハミング距離と電源電圧ドロップ 低電源電圧 (0.75V) 時 (a) オンチップモニタ (b)1 Ω 法

ア近傍での電力解析攻撃耐性の評価が重要になると考えられる.

第4章

VLSI暗号回路における電力解析攻撃への耐性評価

4.1 はじめに

暗号化デバイスの電力解析攻撃に対する安全性を設計、製造後の段階で評価することは暗号の信頼性において不可欠である。製造後の実装だけでサイドチャネル情報漏洩を防ぐことは困難であり、設計時においてハミング距離、ハミング重みによる評価を行い安全であると判断しても製造後にサイドチャネル情報が漏洩している可能性は否めない。そこで、シミュレーションによる電源ノイズ波形や実装後の波形を用いてサイドチャネル情報漏洩が無いかを実際にサイドチャネル攻撃を行うことで評価する必要がある。しかし、対策を行った暗号化回路に対してサイドチャネル攻撃を行うには数十～百万波形もの膨大な電源ノイズ波形を用いる必要があり [49] 評価コストが高く問題となる。本章では、サイドチャネル情報漏洩の評価コストを削減するために、回路の漏洩を最大化する入力ベクタ生成手法を提案し、サイドチャネル攻撃評価に必要な波形数削減を目標とする。

4.2 電力解析攻撃耐性評価手法

電力解析攻撃において最終ラウンドがターゲットになることが多い。図 4.1 に AES 暗号化の最終ラウンドでのデータフローを示す。最終ラウンドでは MixColumns 処理がスキップされるため、各データレジスタの依存が少なくなり鍵を推定した場合の逆算が容易になる。AES では入力 of 128 bit を 8 bit 毎に分割しマトリクスとして扱う (図 4.2)。MixColumns では以下の様な式 4.1 に基づいてデータ変換が行われる。マトリクスでの列毎に演算が行われるので MixColumns への入力を a_i 、出力を b_i とする。式 4.1 より、MixColumns では全てのデータレジスタのデータが相互

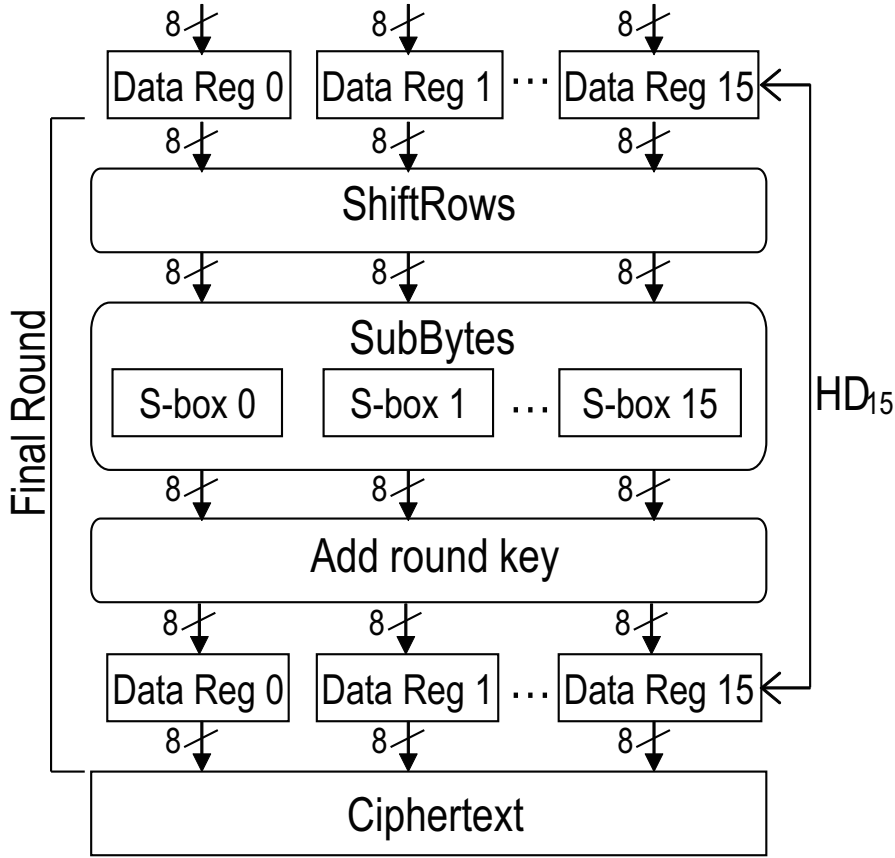


図 4.1: AES の最終ラウンドでのデータフロー

に加算されることが分かる．そのため攻撃者にとっては予想が困難である．攻撃者は図 4.1 で示すように最終ラウンド前後でのデータレジスタのハミング距離 $H_i (0 \leq i \leq 15)$ を各マトリクス位置毎に存在する候補鍵 $k (0 \leq k \leq 255)$ で逆算し求め，電源ノイズと相関があるかを判断し，どの候補鍵 k が正解であるかを特定する．

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} \quad (4.1)$$

提案する図 4.3 にサイドチャネル攻撃に対する評価フローを示す．入力 は実際に使用する秘密鍵と入力平文である．本論文では測定手法を 1 Ω

S_{00}	S_{01}	S_{02}	S_{03}
S_{10}	S_{11}	S_{12}	S_{13}
S_{20}	S_{21}	S_{22}	S_{23}
S_{30}	S_{31}	S_{32}	S_{33}

図 4.2: AES でのデータマトリクス

法, シミュレーション手法を TSDPC モデルとしたが, 他のシミュレーション手法を用いてもフローは変わらない. それぞれの電源ノイズ取得手法をつかい波形を集め, サイドチャネル攻撃を行う. サイドチャネル攻撃によって得られた仮定鍵 (Guessed key) が実際の秘密鍵と合っているかで評価を行う. 鍵が 1 バイトでも得られている場合, 評価に使用する平文の数を増やせば全ての鍵が特定される可能性が高い. 使用する平文は過去の事例では 1 万~100 万程度である. しかし, 100 万波形もの測定を設計時に行い暗号化コアの安全性を評価し再設計を行うことは現実的ではない.

そこで, 攻撃時に攻撃者が想定している CPA 攻撃において電力モデルとして用いられるハミング距離に着目し暗号回路にとって厳しい条件での評価について考える.

4.2.1 ハミング距離統一平文

暗号回路にとってサイドチャネル情報の漏洩が最大になるのは, 漏洩情報に対してのノイズが最小となる場合である. ここでノイズとして考えられるのは測定系からの熱雑音, 電磁ノイズだけで無く, サイドチャネル攻撃時に対象にしているマトリクス位置以外の部分の暗号化回路の動作による電源ノイズも含まれる. 図 4.4(a) にランダムな入力平文の場合の

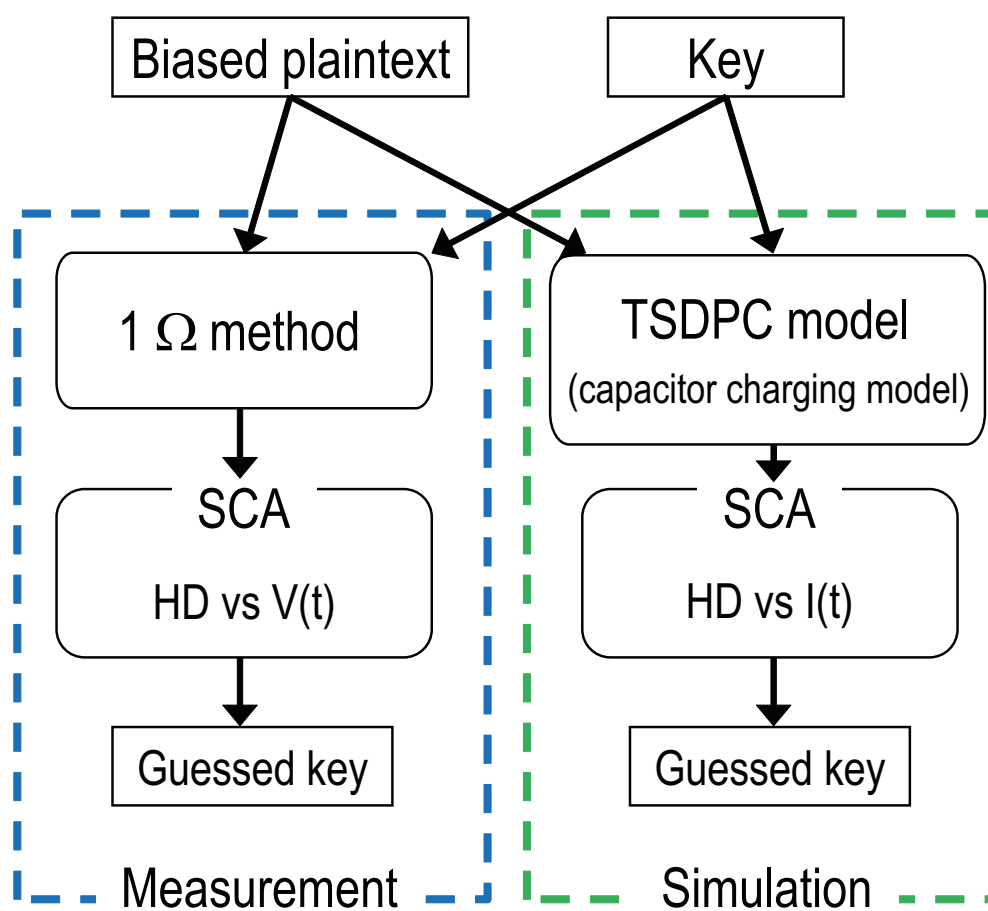


図 4.3: CPA を用いたサイドチャネル攻撃評価フロー

	target D Reg0	D Reg1	D Reg2	...	D Reg14	D Reg15	
HD	1	3	4	...	7	2	Avg.HD $\neq$ 1
Power	PHD=1	PHD=3	PHD=4	...	PHD=7	PHD=2	Avg.P = PHD=1 + P _{error}

Error for CPA

(a)

	target D Reg0	D Reg1	D Reg2	...	D Reg14	D Reg15	
HD	1	1	1	...	1	1	Avg.HD = 1
Power	PHD=1	PHD=1	PHD=1	...	PHD=1	PHD=1	Avg.P = PHD=1

Similar power to target byte

(b)

図 4.4: CPA のイメージ (a) ランダムな平文 (b) ハミング距離統一平文

CPA のイメージを示す。今、0 バイト目のマトリクスの消費電力 $P_{HD=1}$ に着目して攻撃を行っているとする。他の 1～15 バイト目の動作による消費電力は攻撃にとってノイズとして観測される。暗号化回路の設計者の立場に立って考えると、使用する鍵は既知のものであり、鍵を使用して暗号化回路の動作を制御することは可能である。そこで図 4.4(b) に示すように全てのマトリクス位置でハミング距離が同じような平文を入力した場合に攻撃を行う場合のイメージを示す。ハミング距離が全てのマトリクス位置で同じため回路全体の平均消費電力も対象のマトリクス位置の消費電力に近いものとなる。なぜならハミング距離が同じ場合、各 SubBytes では同じビット数の遷移が発生し、異なる部分は AddRoundKey のみとなるからである。

次にこのようなハミング距離が統一された平文を作る手法について説明する。単純にハミング距離が統一されたパターンを探索する場合探索空間は 2^{128} パターンとなり現実的ではない。そこで、攻撃に使用する最

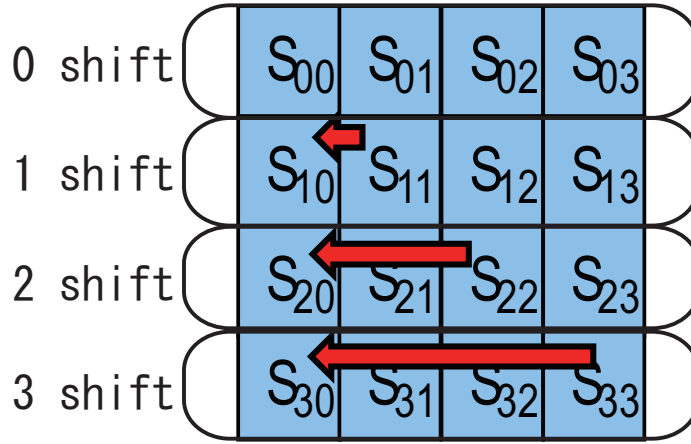


図 4.5: Shiftrows 演算でのマトリクス内のデータ移動

表 4.1: Shiftrow 演算における各マトリクス位置の関連

関連数	マトリクス位置のグループ
0	$S_{00}, S_{01}, S_{02}, S_{03}$
2	$(S_{20}, S_{22}), (S_{21}, S_{23})$
4	$(S_{10}, S_{11}, S_{12}, S_{13}), (S_{30}, S_{31}, S_{32}, S_{33})$

終ラウンドでのデータフローを考える．前述した MixColumns は最終ラウンドでスキップされるので，AddRoundKey, SubBytes, ShiftRows を逆算すれば 1 ラウンド前のデータが求められハミング距離を計算できる．AddRoundKey, SubBytes はデータの中身が変わるだけなので計算により簡単に逆算が可能である．図 4.5 に示すように ShiftRows ではデータの位置が変化するため，ハミング距離を求めるうえで他のマトリクス位置との関連性が発生する．表 4.1 に ShiftRows における各データマトリクス位置での関連する数，グループを示す．ハミング距離を統一した平文を生成するためには，これらの関連したデータ位置のデータを同時に生成する必要がある．最大探索範囲は 4 カ所のマトリクス位置で部分鍵が関連する場合であり，探索範囲は 1 バイト鍵の全候補の関連マトリクス乗で表せ， $(2^8)^4 = 2^{32}$ である．これは十分現実的な時間で探索が可能である．

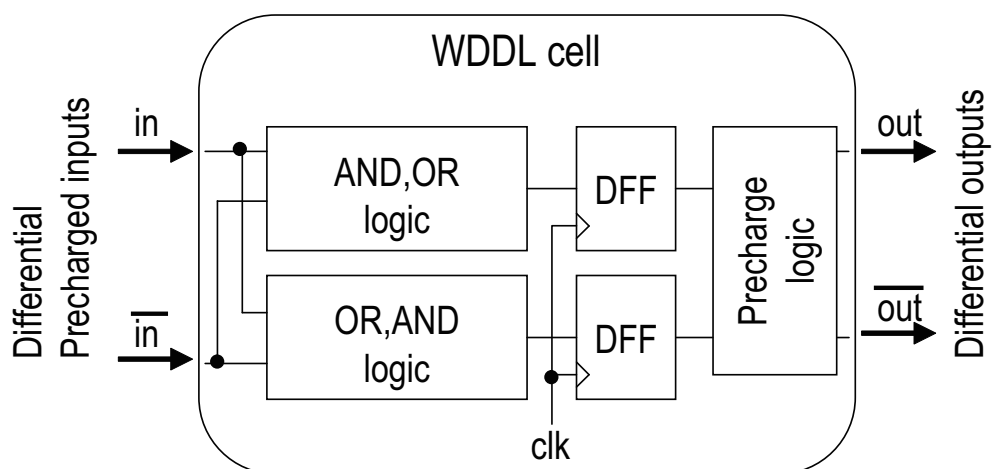


図 4.6: WDDL セルのイメージ

4.3 提案手法による評価結果

4.3.1 テストチップ

提案手法を評価するために実際に試作したチップにおける実測とシミュレーションの比較を行う。対象とした対策実装は Wave Dynamic Differential Logic(WDDL)[17]を選択した。WDDLは、正論理、負論理の2線式ロジックとなっており、データ遷移に依存しない電力消費を行う電力解析攻撃への対策手法となっている(図 4.6)。

図 4.7にチップのレイアウトを示す。未対策の Table(Look-up Table)実装に対して1.4倍ほどのゲート数である。

1 Ω 法による測定のブロック図と写真を図 4.8に示す。SASEBO-R2上の観測端子とオシロスコープを接続し、チップからのトリガ信号を用いて測定を行う。電力解析攻撃対策版での電源電圧変動差は微小であると考えられるため40 dBの信号増幅器を用いて増幅を行いオシロスコープへと入力している。

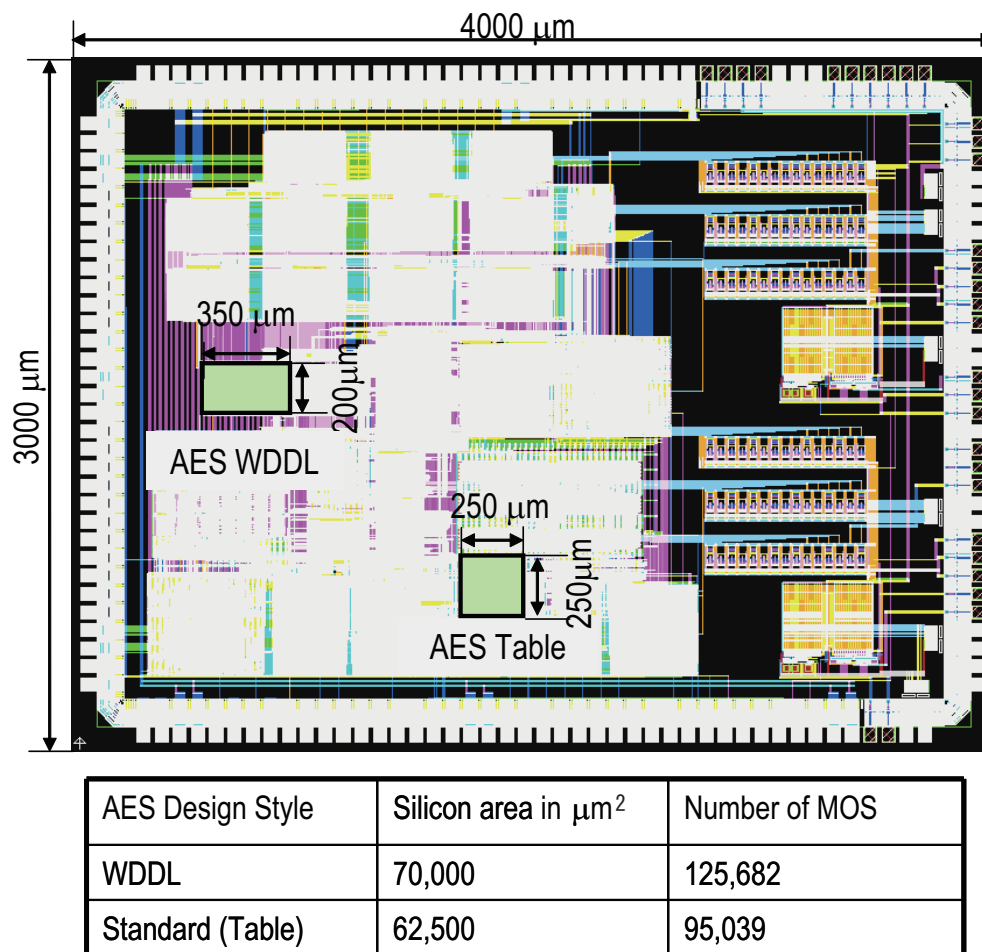


図 4.7: チップレイアウトとデザインサマリ

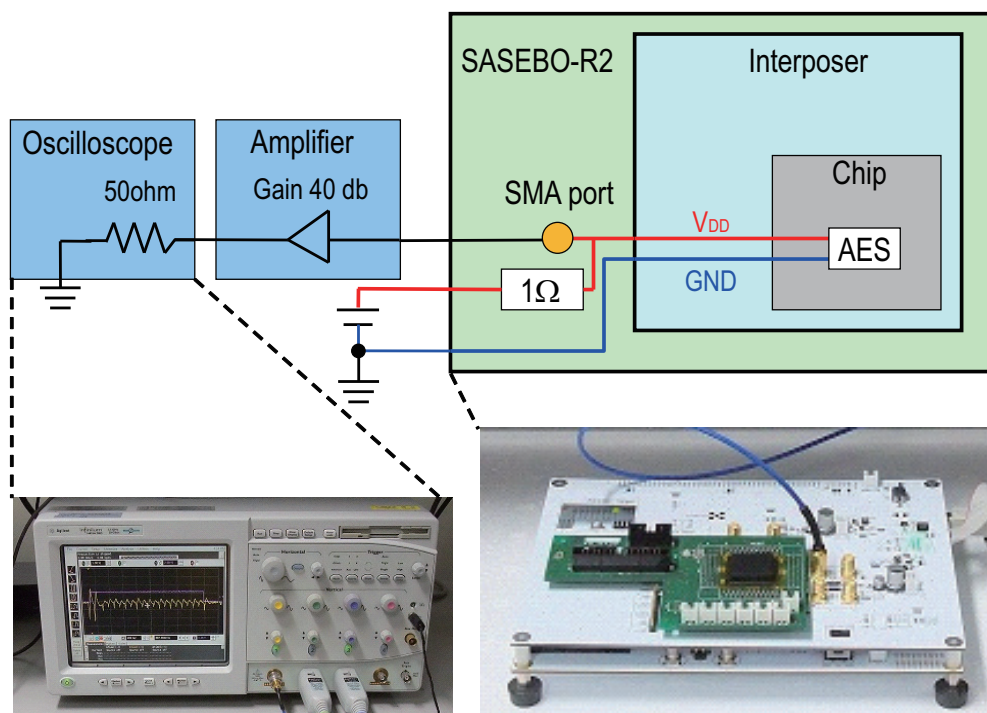


図 4.8: 測定環境

4.3.2 実験結果

4.3.2.1 ハミング距離統一平文の効果

ハミング距離統一平文の効果を確認するために電力解析攻撃に対して対策を施していないコアにおいて評価を行う。評価指標は3章で用いた電源電流ドロップである。2章で対象としたコアと同じ4種類の電力解析攻撃未対策実装に対して容量充電モデルによるシミュレーションを行い評価を行う。図4.9に Composite S-box におけるランダム入力と選択平文入力での電源電流ドロップの比較を示す。ランダム入力では、明確なハミング距離依存性は観測できない。しかし、CPAが成功することからハミング距離依存性が存在することがいえる。一方でハミング距離統一平文を用いた場合明確なハミング距離依存性が観測できる。実装によるハミング距離依存性の変化を調べるために他の S-box 実装に対してハミング距離依存性を求めた結果を図4.10に示す。どの実装においてもハミング距離依存性が明確に観測できる。ハミング距離に対する電源電流ドロップの傾きに注目すると Composite が高いハミング距離において緩やかになっている。このことは2章において Composite S-box で鍵が検出されにくい結果と一致している。

図4.11に選択平文で CPA を行った結果を示す。全ての実装において10～15波形程度で全ての鍵が検出されている。ハミング距離依存性評価から明らかなように全ての実装でハミング距離に依存した消費電流が得られるため実装間で攻撃に必要な波形数に大きな差は見られない。以上の結果からハミング距離統一平文は暗号化回路におけるハミング距離依存性を効率的に評価できるといえる。

4.3.2.2 電力解析攻撃対策コアの評価

前節で述べた測定環境にて測定した電源ノイズ波形と2章で述べた TS-DPC モデルによる電源ノイズシミュレーション結果を図4.12に示す。動作周波数は24MHzであり、WDDL 実装では Precharge と Evaluation の2サイクル1ラウンド処理なので、通常の実装の倍のクロックによるノイズが観測できる。サイドチャネル攻撃の対象となるのは最終ラウンドの Evaluation の位置である。

CPA による電力解析攻撃の結果を図4.13に示す。横軸は攻撃に使用した波形数であり、縦軸は16個あるマトリクス位置において正解鍵が256個の全候補鍵中で何番目に相関値が高かったという順位の平均値である。

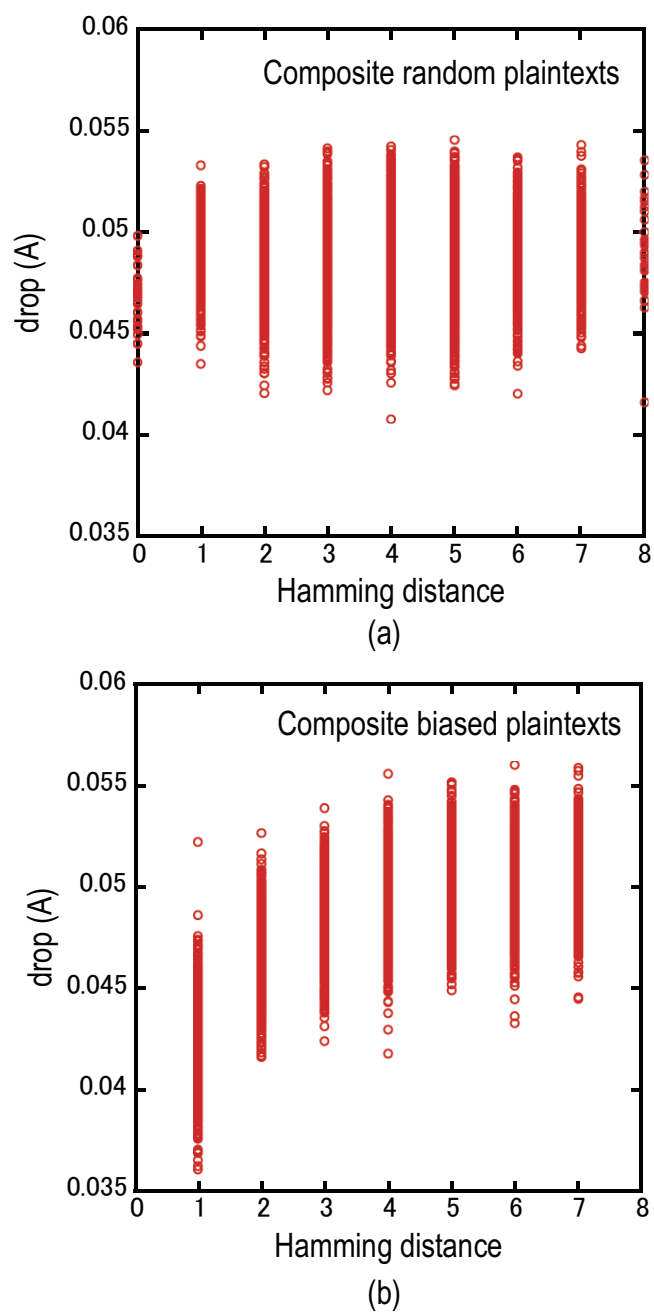


図 4.9: Composite S-box でのハミング距離依存性 (a) ランダムな入力平文 (b) 選択平文入力

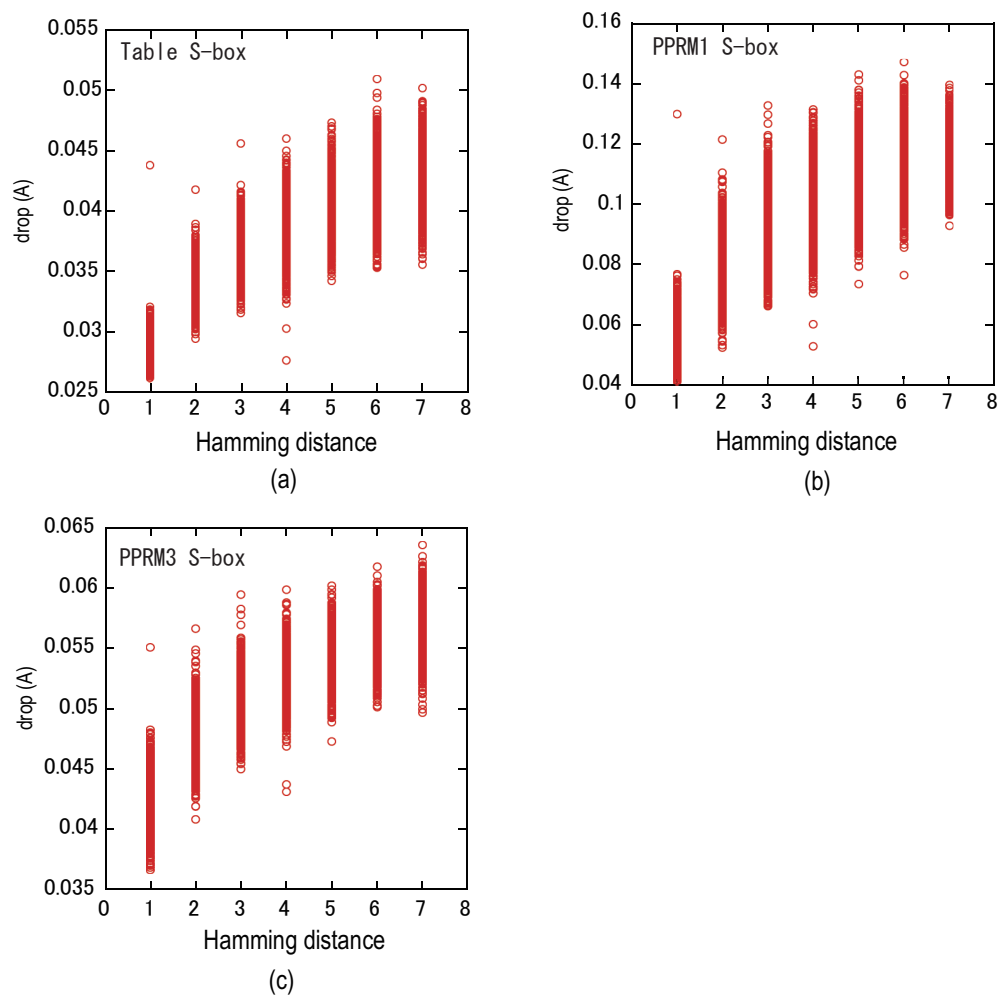


図 4.10: 異なる S-box 実装における選択平文を用いた場合のハミング距離依存性 (a) Table S-box (b) PPRM 1-stage S-box (c) PPRM 3-stage Sbox

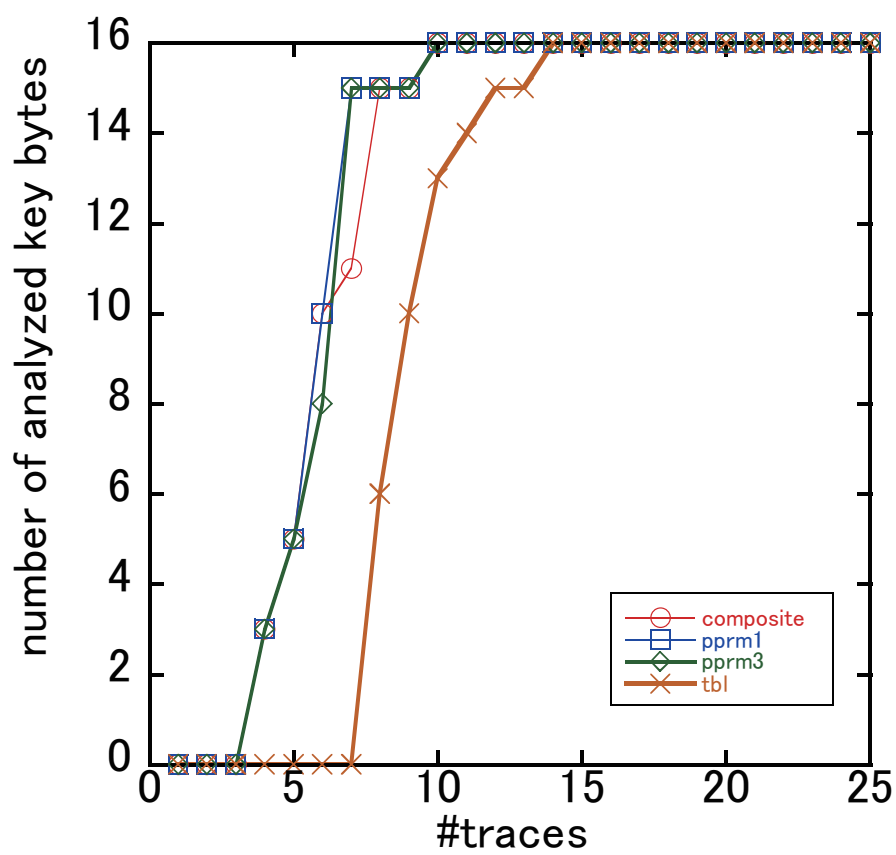
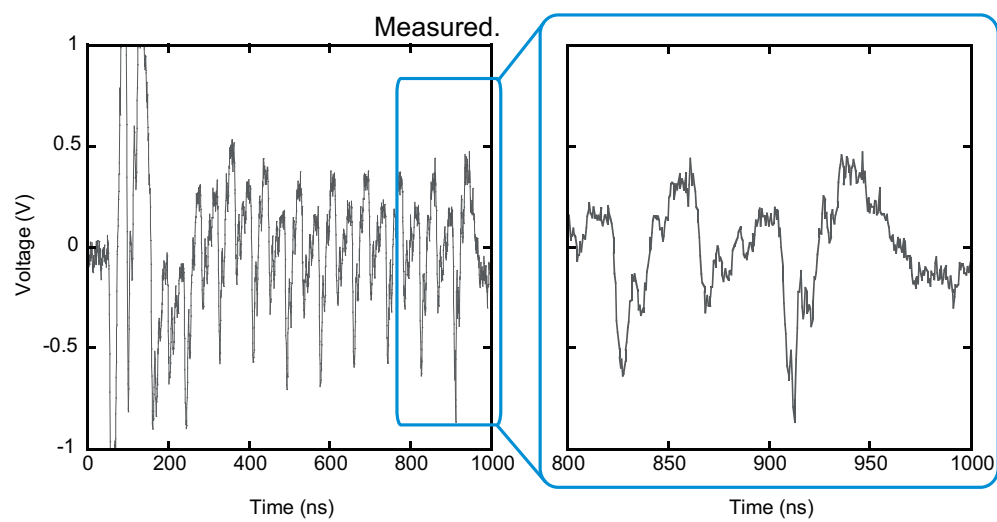
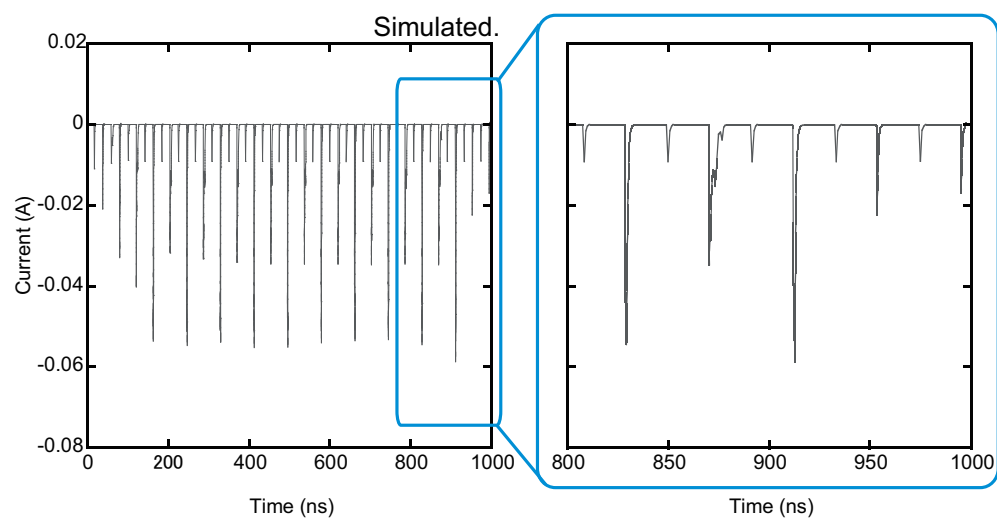


図 4.11: 選択平文での CPA 結果



(a)



(b)

図 4.12: WDDL 実装 AES の電源ノイズ波形 (a) 1 Ω 法による実測 (b) TSDPC モデルによるシミュレーション

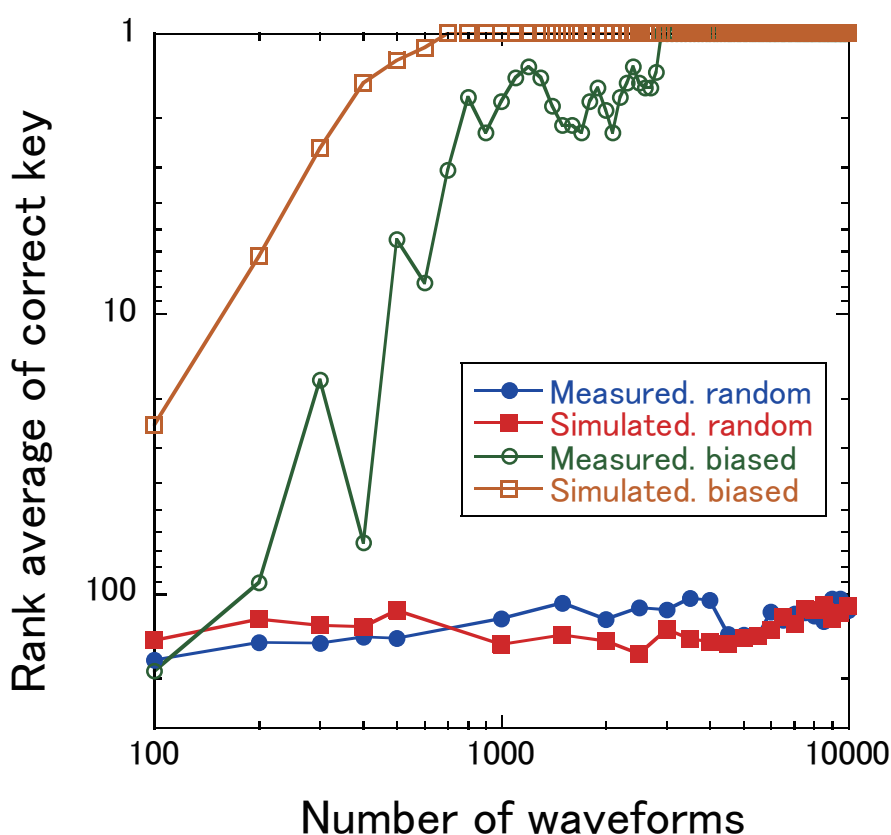


図 4.13: CPA 結果

ランダムな入力を使用した場合は測定、シミュレーション共に 140 位程度で横ばいであり、5000～10000 波形で右肩上がりで徐々に上昇している。この傾向が続くとなると 10 万波形程度で鍵が特定される可能性は高い。対してハミング距離を統一した場合は 4000 波形程度で全ての鍵が見つかるという結果になった。すなわち今回実装した WDDL 実装では鍵が取得する電源ノイズ波形数を増加させれば秘密鍵が特定される可能性があることになる。

4.4 まとめ

本章では電力解析攻撃の評価段階において少ない電源ノイズ波形数で耐性を評価することのできるハミング距離統一平文を提案した。

提案手法を実証するために電力解析攻撃に対して対策を施した実装に

において測定，シミュレーションによる電源ノイズ波形を用いた評価においてランダム入力平文とハミング距離統一平文において評価を行った．ハミング距離統一平文を用いることでランダム入力平文では1万波形以上でないと特定できない鍵が4000波形以内で特定できることを示した．

本研究ではハミング距離を統一することを考えたが攻撃モデルに併せて全 S-box での動作をそろえるという概念は他の攻撃モデルに対しても応用可能であると考えられる．また，評価手法フローに関して設計者独自の攻撃者よりも有利に評価する手法を考案することが必要であると考えられる．

第5章

結論

暗号化デバイスにおいて電力解析攻撃などのサイドチャネル攻撃が提案され脅威となっている。そのため、設計段階、製造段階での電力解析攻撃に対する耐性を評価する技術が重要となる。現在、物理デバイスレベルでのシミュレーションで電力解析攻撃に必要な膨大な波形数のシミュレーションに耐えうるシミュレータは提案されていない。製造後の評価においても、チップ外で測定を行うという攻撃者と同じレベルでの測定手法しか確立されておらず、攻撃者の測定技術が向上した場合に評価で安全であっても安全とは言い切れなくなる。また、電力解析攻撃への耐性評価全般においても実際の攻撃に用いられる手法を使用しており、効率的であるとは言い難い。本研究ではこれらの問題に対して、物理デバイスレベルでの高速なシミュレーションである容量充電モデルを用いたシミュレーションを提案した。また、オンチップモニタを用いたチップ内での電源ノイズ測定手法を提案した。評価において効率的な入力を生成するハミング距離統一平文を提案した。

1章では暗号化回路がスマートカードなどの携帯デバイスに搭載され普及していることを述べ、電力解析攻撃などのサイドチャネル攻撃の脅威にさらされていることを述べた。サイドチャネル攻撃において様々な新たな攻撃が提案されており、設計者が評価しなければならない漏洩項目が増加しており評価コストが増加していることについて述べ、電力解析攻撃評価において従来行われていたシミュレーション、測定、評価手法を挙げそれぞれの課題について述べた。

2章では容量充電モデルという高速な消費電流解析手法を電力解析攻撃評価に応用することを提案した。容量充電モデルを用いたレイアウト後の情報を含む消費電流波形の導出にかかる時間は従来のフルトランジスタレベルでのレイアウト情報を含まない解析に比べて200倍の高速化を達成した。これにより設計段階でレイアウト後のCPA評価に必要な数万波形以上のシミュレーションが可能となる。

容量充電モデルによる解析結果はS-boxの実装差による消費電流の変化をよく表現しており、65 nm CMOSテクノロジーで製造されたテストチッ

プとの実測結果と傾向が一致している。電力解析攻撃の一つである CPA の結果でも容量充電モデルと実測で実装間の攻撃結果の傾向が一致し、容量充電モデルによるサイドチャネル情報が表現できていることを示した。

今後の課題として、容量充電モデルがスイッチとキャパシタのみで構成できるため容易に他の解析ツールに取り込むことが可能な特性を生かし、磁界シミュレーションツールと組み合わせることで、EMプローブによる回路内局所攻撃などのより高度な攻撃への評価が挙げられる。

3章では高精度なチップ内での電源電圧変動波形取得機構であるオンチップモニタを暗号化 LSI の電圧変動取得に使用することを提案した。

提案手法の有用性を実証するために従来手法である 1 オーム法と測定結果を比較した。比較結果より、電力解析攻撃対策を施していない AES において低周波成分のみで攻撃が可能であることを示した。また、相関値の時間方向の推移を調べることにより、オンチップモニタによる攻撃がオフチップで測る手法に比べてノイズの影響が少ないことを示した。このことから、オンチップモニタは暗号化回路の電力解析攻撃の測定をするうえでより高性能な測定手法だといえる。

今後の展望としては、対策を施して安全だと考えられている AES に対してもチップ内部で取得した波形の高周波成分で攻撃できるかを評価することである。現在想定されている攻撃者の測定方法では安全であっても、将来的に攻撃者の測定技術は進歩すると考えられ、チップ内でのコア近傍での電力解析攻撃耐性の評価が重要になると考えられる。

4章では電力解析攻撃の評価段階において少ない電源ノイズ波形数で耐性を評価することのできるハミング距離統一平文を提案した。

提案手法を実証するために電力解析攻撃に対して対策を施した実装において測定、シミュレーションによる電源ノイズ波形を用いた評価においてランダム入力平文とハミング距離統一平文において評価を行った。ハミング距離統一平文を用いることでランダム入力平文では 1 万波形以上でないと特定できない鍵が 4000 波形以内で特定できることを示した。

今後の展望として、ハミング距離統一平文における攻撃モデルに併せて全 S-box での動作をそろえるという概念は他の攻撃モデルに対しても応用可能であると考えられる。また、評価手法フローに関して設計者独自の攻撃者よりも有利に評価する手法を考案することが必要であると考えられる。

以上の成果より、暗号化回路において問題となっている電力解析攻撃に対して設計段階でのシミュレーションによる耐性評価、製造後の測定

による評価，それら両方に共通する評価の効率化を提案した．提案手法を用いることで，暗号回路の電力解析攻撃への安全性を考慮した設計フローが開発できると考える．

今後，安全性評価においては設計者が攻撃者を上回るような評価手法が求められると考えられる．本研究で CPA に関しては設計者にしか知り得ない秘密鍵という情報を活用し評価に必要な時間を短縮する技術を提案したが，他の手法への応用も必須であると考える．またその過程で実際に攻撃を行わないで評価が可能な指標が重要となってくると考える．

謝辞

本研究の機会を賜り、熱心にご指導頂きました神戸大学大学院 システム情報学研究科・永田 真教授に心から感謝の意を表します。

貴重な時間を割き、本論文を査読して頂きました神戸大学大学院 システム情報学研究科・吉本 雅彦教授、鳩野 逸生教授、有木 康雄教授に御礼申し上げます。

適切なご指導、ご助言を頂きました神戸大学大学院 システム情報学研究科・三浦 典之特命助教、鎌田 十三郎講師に深く感謝いたします。

本研究は独立行政法人科学技術振興機構の戦略的国際科学技術協力事業（共同研究型）による成果である。日頃よりご議論頂いている産業技術総合研究所・片下 敏宏氏、堀 洋平氏、電気通信大学・佐藤 証教授、崎山 一男教授、李 陽特任助教、東北大学・本間 尚文准教授、林 優一准教授、遠藤 翔氏、森田テック株式会社・佐々木 明彦氏、Pierre-and-Marie-Curie 大学・Pirouz Bazargan-Sabet 助教、Telecom ParisTech・Shivam Bhasin 氏、Jean-Luc Danger 教授に心より感謝いたします。

本研究において、様々なご指導とご助言を頂きました神戸大学大学院 自然科学研究科 情報知能工学専攻・荒賀 佑樹氏、吉川 薫平氏に心より感謝いたします。

本研究において、熱心なご指導とご助言を頂きました株式会社エイアールテック・小坂 大輔氏に心より感謝いたします。

社会の場を通して、丁寧なご指導を頂きました株式会社エイアールテック (神戸大学共同研究員兼務)・益子耕一郎氏、パナソニック株式会社・道正 志郎氏に感謝いたします。

様々な御助言を頂きましたルネサスエレクトロニクス株式会社・深澤 光弥氏、松野 哲朗氏、株式会社富士通研究所・橋田 拓志氏、パナソニック株式会社・坂東 要志氏、株式会社メガチップス・澤田 卓也氏に感謝いたします。

日頃より様々な事務・会計処理をして頂きました坪井 彩氏に感謝いたします。

同じ研究室で共に学び、日頃よりお世話になりました東 直矢氏、高谷 聡氏に感謝いたします。

共に学び、日頃よりお世話になりました大阪大学大学院 情報科学研究科 コンピュータサイエンス専攻・田中 俊彰氏に感謝いたします

本研究室、情報知能学専攻第 26 講座の皆様に感謝いたします。

最後に、私をここまで育ててくださいました両親、また暖かく見守ってくださった家族に心よりの感謝をいたします。

参考文献

- [1] EUROS MART, “Growth trend for solutions combining convenience and security continues,” <http://www.eurosmart.com/index.php/publications/market-overview.html>, 2013.
- [2] “Data encryption standard (des),” <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>, 1999.
- [3] M. Matsui, “Linear cryptanalysis method for des cipher,” *Advances in Cryptology - EUROCRYPT ’93*, Lecture Notes in Computer Science, vol. 765, pp. 386-397, Springer Berlin Heidelberg, 1994.
- [4] “DES crack,” http://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_descracker_pressrel.html, 1998.
- [5] J. Daemen and V. Rijmen, “Aes algorithm specification,” <http://csrc.nist.gov/archive/aes/rijndael/wsdindex.html>, 2001.
- [6] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting, “Improved cryptanalysis of rijndael,” in *Fast Software Encryption*, Vol. 1978 of Lecture Notes in Computer Science, pp. 213–230, Springer Berlin Heidelberg, 2001.
- [7] A. Biryukov and D. Khovratovich, “Related-key cryptanalysis of the full aes-192 and aes-256,” *Cryptology ePrint Archive*, Report 2009/317, 2009.
- [8] A. Bogdanov, D. Khovratovich, and C. Rechberger, “Biclique cryptanalysis of the full aes,” in *Advances in Cryptology - ASIACRYPT 2011*, Vol. 7073 of Lecture Notes in Computer Science, pp. 344–371, Springer Berlin Heidelberg, 2011.
- [9] “Federal information processing standards,” <http://www.nist.gov/itl/fips.cfm>.

-
- [10] “Cryptography research and evaluation committees,” <http://www.cryptrec.go.jp/>.
- [11] “Cryptrec 暗号リスト,” <http://www.cryptrec.go.jp/list.html>.
- [12] P.C. Kocher, “Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems,” in *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO ’96, pp. 104–113, London, UK, UK, 1996, Springer-Verlag.
- [13] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in *Proceedings of the International Cryptology Conference*, pp. 388–397, 1999.
- [14] E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model,” in *Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems*, pp. 16–29, 2004.
- [15] S. Ors, F. Gurkaynak, E. Oswald, and B. Preneel, “Power-analysis attack on an asic aes implementation,” in *Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on*, Vol. 2, pp. 546–552 Vol.2, 2004.
- [16] K. Tiri and I. Verbauwhede, “Charge recycling sense amplifier based logic: securing low power security ics against dpa [differential power analysis],” in *Solid-State Circuits Conference, 2004. ESSCIRC 2004. Proceeding of the 30th European*, pp. 179–182, 2004.
- [17] K. Tiri and I. Verbauwhede, “A logic level design methodology for a secure dpa resistant asic or fpga implementation,” in *Design, Automation and Test in Europe Conference and Exhibition, 2004. Proceedings*, Vol. 1, pp. 246–251 Vol.1, 2004.
- [18] C. Tokunaga and D. Blaauw, “Secure aes engine with a local switched-capacitor current equalizer,” in *ISSCC*, pp. 64–65, 2009.
- [19] E. Trichina, “Combinational logic design for aes subbyte transformation on masked data,” 2003, 11 Nov 2003.

-
- [20] T. Popp and S. Mangard, “Masked dual-rail pre-charge logic: Dpa-resistance without routing constraints,” in *Cryptographic Hardware and Embedded Systems - CHES 2005*, Vol. 3659 of Lecture Notes in Computer Science, pp. 172–186, Springer Berlin Heidelberg, 2005.
 - [21] S. Nikova, C. Rechberger, and V. Rijmen, “Threshold implementations against side-channel attacks and glitches,” in *Proceedings of Information and Communications Security, 8th International Conference, ICICS 2006, number 4307 in Lecture Notes in Computer Science*, pp. 529–545, Springer-Verlag, 2006.
 - [22] K. Tiri and I. Verbauwhede, “Simulation models for side-channel information leaks,” in *Proceedings of the 42Nd Annual Design Automation Conference, DAC '05*, pp. 228–233, New York, NY, USA, 2005, ACM.
 - [23] D. Suzuki, M. Saeki, and T. Ichikawa, “Dpa leakage models for cmos logic circuits,” in *Cryptographic Hardware and Embedded Systems - CHES 2005, 7th International Workshop, Edinburgh, UK, August 29 - September 1, 2005, Proceedings*, Vol. 3659 of Lecture Notes in Computer Science, pp. 366–382, Springer, 2005.
 - [24] D. Agrawal, J. Rao, P. Rohatgi, and K. Schramm, “Templates as master keys,” in *Cryptographic Hardware and Embedded Systems - CHES 2005*, Vol. 3659 of Lecture Notes in Computer Science, pp. 15–29, Springer Berlin Heidelberg, 2005.
 - [25] E. Oswald and S. Mangard, “Template attacks on masking - resistance is futile,” in *Topics in Cryptology, CT-RSA 2007*, Vol. 4377 of Lecture Notes in Computer Science, pp. 243–256, Springer Berlin Heidelberg, 2006.
 - [26] M. Medwed and E. Oswald, “Template attacks on ecdsa,” in *Information Security Applications*, Vol. 5379 of Lecture Notes in Computer Science, pp. 14–27, Springer Berlin Heidelberg, 2009.
 - [27] A. Moradi, O. Mischke, and T. Eisenbarth, “Correlation-enhanced power analysis collision attack,” in *Cryptographic Hardware and Em-*

- bedded Systems, CHES 2010*, Vol. 6225 of Lecture Notes in Computer Science, pp. 125–139, Springer Berlin Heidelberg, 2010.
- [28] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, “Mutual information analysis,” in *Cryptographic Hardware and Embedded Systems - CHES 2008*, Vol. 5154 of Lecture Notes in Computer Science, pp. 426–442, Springer Berlin Heidelberg, 2008.
- [29] Y. Li, D. Nakatsu, Q. Li, K. Ohta, and K. Sakiyama, “Clockwise collision analysis – overlooked side-channel leakage inside your measurements,” Cryptology ePrint Archive, Report 2011/579, 2011.
- [30] T. Nakasone, Y. Li, Y. Sasaki, M. Iwamoto, K. Ohta, and K. Sakiyama, “Key-dependent weakness of aes-based ciphers under clockwise collision distinguisher,” in *Information Security and Cryptology - ICISC 2012*, Vol. 7839 of Lecture Notes in Computer Science, pp. 395–409, Springer Berlin Heidelberg, 2013.
- [31] L. Lerman, G. Bontempi, and O. Markowitch, “Side channel attack: an approach based on machine learning,” in *Second International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE)*, 2011.
- [32] G. Hospodar, E.D. Mulder, B. Gierlichs, I. Verbauwhede, and J. Vandewalle, “Least squares support vector machines for side-channel analysis,” in *Second International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE)*, 2011.
- [33] J. den Hartog, J. Verschuren, E. de Vink, J. Vos, and W. Wiersma, “Pinpas: A tool for power analysis of smartcards,” in *Security and privacy in the age of uncertainty : IFIP TC11 18th international conference on information security (SEC2003), May 26-28, 2003, Athens, Greece*, IFIP series ; no. 122, pp. 453–457, Kluwer Academic Publishers, 2003.
- [34] M. Aigner, S. Mangard, F. Menichelli, R. Menicocci, M. Olivieri, T. Popp, G. Scotti, and A. Trifiletti, “Side channel analysis resistant design flow,” in *IEEE International Symposium on Circuits and Systems (ISCAS 2006)*, 2006.

-
- [35] M. Kirschbaum and T. Popp, “Evaluation of power estimation methods based on logic simulations,” in *Proceedings of the 15th Austrian Workshop on Microelectronics*, pp. 45 – 51, Verlag der Technischen Universität Graz, 2007.
- [36] Z. Chen and P. Schaumont, “Early feedback on side-channel risks with accelerated toggle-counting,” in *Hardware-Oriented Security and Trust, 2009. HOST '09. IEEE International Workshop on*, pp. 90–95, 2009.
- [37] S. Mangard and K. Schramm, “Pinpointing the side-channel leakage of masked aes hardware implementations,” in *Cryptographic Hardware and Embedded Systems - CHES 2006*, Vol. 4249 of Lecture Notes in Computer Science, pp. 76–90, Springer Berlin Heidelberg, 2006.
- [38] F. Regazzoni, S. Badel, T. Eisenbarth, J. Grotschadl, A. Poschmann, Z. Toprak, M. Macchetti, L. Pozzi, C. Paar, Y. Leblebici, and P. Ienne, “A simulation-based methodology for evaluating the dpa-resistance of cryptographic functional units with application to cmos and mcml technologies,” in *International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation, 2007. IC-SAMOS 2007.*, pp. 209–214, 2007.
- [39] RISEC, AIST, “Side-channel attck standard evaluation board,” <http://www.risec.aist.go.jp/project/sasebo/>.
- [40] M. Stefan, O. Elisabeth, and P. Thomas, “*Power Analysis Attacks - Revealing the Secrets of Smart Cards*,” pp. 43–53, Springer, 2005.
- [41] RISEC, AIST, “Sasebo-giii quick start guide,” <http://www.risec.aist.go.jp/project/sasebo/>.
- [42] T. Katashita., A. Satoh, K. Kikuchi, H. Nakagawa, and M. Aoyagi, “Evaluation of dpa characteristics of sasebo for board level simulations,” in *Constructive Side-Channel Analysis and Secure Design ,International Workshop on*, pp. 36–39, 2010.

- [43] J.J. Quisquater and D. Samyde, “Electromagnetic analysis (ema): Measures and counter-measures for smart cards,” in *Smart Card Programming and Security*, Vol. 2140 of Lecture Notes in Computer Science, pp. 200–210, Springer Berlin Heidelberg, 2001.
- [44] D. Agrawal, B. Archambeault, J. Rao, and P. Rohatgi, “The em side-channel(s),” in *Cryptographic Hardware and Embedded Systems - CHES 2002*, Vol. 2523 of Lecture Notes in Computer Science, pp. 29–45, Springer Berlin Heidelberg, 2003.
- [45] C. Gebotys, S. Ho, and C. Tiu, “Em analysis of rijndael and ecc on a wireless java-based pda,” in *Cryptographic Hardware and Embedded Systems - CHES 2005*, Vol. 3659 of Lecture Notes in Computer Science, pp. 250–264, Springer Berlin Heidelberg, 2005.
- [46] T. Sugawara, D. Suzuki, M. Saeki, M. Shiozaki, and T. Fujino, “On measurable side-channel leaks inside asic design primitives,” in *Cryptographic Hardware and Embedded Systems - CHES 2013*, Vol. 8086 of Lecture Notes in Computer Science, pp. 159–178, Springer Berlin Heidelberg, 2013.
- [47] Consortium, “Common criteria for information technology security evaluation(iso/iec 15408),” <http://www.commoncriteriaportal.org/>, 2013.
- [48] Consortium, “Text for iso/iec 1st wd 17825 - information technology - security techniques - non-invasive attack mitigation test metrics for cryptographic modules,” http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=60612, 2012.
- [49] “Power analysis attacks on sasebo,” http://www.rcis.aist.go.jp/files/special/SASEBO/CryptoLSI-ja/SASEBO_PA_Report_English.pdf, RCIS ,AIST, 2010.
- [50] S. Guilley, L. Sauvage, P. Hoogvorst, R. Pacalet, G. Bertoni, and S. Chaudhuri, “Security evaluation of wddl and seclib countermeasures against power attacks,” *IEEE Transactions on Computers*, Vol. 57, No. 11, pp. 1482–1497, 2008.

-
- [51] T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard, “Evaluation of the masked logic style mdpl on a prototype chip,” in *Cryptographic Hardware and Embedded Systems - CHES 2007*, Vol. 4727 of Lecture Notes in Computer Science, pp. 81–94, Springer Berlin Heidelberg, 2007.
 - [52] “Primetime px,” <http://www.synopsys.com/Tools/Implementation/SignOff/Pages/PrimeTime.aspx>.
 - [53] T. Asai and M. Yoshikawa, “Efficient acquisition technique of side-channel information using event-model simulation,” in *International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE)*, 2013.
 - [54] H. Tsujikawa, K. Shimazaki, S. Hirano, M. Ohki, T. Yoneda, and H. Benno, “A design methodology for low emi-noise microprocessor with accurate estimation-reduction-verification,” in *Proceedings of the IEEE 2002 Custom Integrated Circuits Conference, 2002.*, pp. 299–302, 2002.
 - [55] M. Badaroglu, G. Van der Plas, P. Wambacq, S. Donnay, G. Gielen, and H. De Man, “Swan: high-level simulation methodology for digital substrate noise generation,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 14, No. 1, pp. 23–33, 2006.
 - [56] T. Hashida and M. Nagata, “On-chip waveform capture and diagnosis of power delivery in soc integration,” in *2010 IEEE Symposium on VLSI Circuits (VLSIC)*, pp. 121–122, 2010.
 - [57] Y. Araga, T. Hashida, and M. Nagata, “An on-chip waveform capturing technique pursuing minimum cost of integration,” in *Proceedings of 2010 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 3557–3560, 2010.
 - [58] M. Nagata, J. Nagai, T. Morie, and A. Iwata, “Measurements and analyses of substrate noise waveform in mixed-signal ic environment,” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 19, No. 6, pp. 671–678, 2000.

-
- [59] K. Yoshikawa, Y. Sasaki, K. Ichikawa, Y. Saito, and M. Nagata, “Co-simulation of on-chip and on-board ac power noise of cmos digital circuits,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. 95, No. 12, pp. 2284–2291, 2012.
- [60] M. Fukazawa, T. Matsuno, T. Uemura, R. Akiyama, T. Kagemoto, H. Makino, H. Takata, and M. Nagata, “Fine-grained in-circuit continuous-time probing technique of dynamic supply variations in socs,” in *IEEE International Solid-State Circuits Conference, 2007. ISSCC 2007. Digest of Technical Papers.*, pp. 288–603, 2007.

発表論文一覧

本研究に関する発表論文

学術雑誌

- [1] D. Fujimoto, T. Katashita, Y. Hori, A. Satoh, and M. Nagata, “A Fast Power Current Simulation of Cryptographic VLSI Circuits for Side Channel Attack Evaluation,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E96-A, No. 12, pp. 2533–2541, Dec. 2013.
- [2] D. Fujimoto, N. Miura, M. Nagata, Y. Hayashi, N. Homma, T. Aoki, Y. Hori, T. Katashita, K. Sakiyama, T-H. Le, J. Bringer, P. Bazargan-Sabet, S. Bhasin, and J-L. Danger, “Power Noise Measurements of Cryptographic VLSI Circuits Regarding Side-Channel Information Leakage,” *IEICE Transactions on Electronics*, Vol. E97-C, No. 4, to appear, 2014.

国際会議

- [3] D. Fujimoto, T. Katashita, Y. Hori, A. Satoh, and M. Nagata, “A Fast Power Current Analysis Methodology using Capacitor Charging Model for Side Channel Attack Evaluation,” *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, P35, pp. 87 - 92, 2011.
- [4] M. Nagata, D. Fujimoto, and D. Tanaka, “Power Current Modeling of Cryptographic VLSI Circuits for Analysis of Side Channel Attacks,” *Asia-Pacific International Symposium and Exhibition on Electromagnetic Compatibility (APEMC)*, No.103, 2013.
- [5] D. Fujimoto, N. Miura, M. Nagata, Y. Hayashi, N. Homma, Y. Hori, T. Katashita, K. Sakiyama, T-H. Le, J. Bringer,

- P. Bazargan-Sabet, and J-L. Danger, “On-Chip Power Noise Measurements of Cryptographic VLSI Circuits and Interpretation for Side-Channel Analysis,” *International Symposium on Electromagnetic Compatibility (EMC Europe 2013)*, pp. 405 - 410 , 2013.
- [6] D. Fujimoto, N. Miura, M. Nagata, Y. Hayashi, N. Homma, T. Aoki, Y. Hori, T. Katashita, K. Sakiyama, T-H. Le, J. Bringer, P. Bazargan-Sabet, S. Bhasin, and J-L. Danger, “Correlation Power Analysis using Bit-Level Biased Activity Plaintexts against AES Cores with Countermeasures,” *EMC Tokyo*, to appear , 2014.

学術講演

- [7] 片下 敏宏, 佐藤 証, 永田 真, 藤本 大介, 菊地 克弥, 仲川 博, 青柳 昌宏, “サイドチャネル標準シミュレーションモデル構築に向けた標準評価ボードのDPA特性測定,” *Symposium on Cryptography and Information Security (SCIS)*, 講演番号 4B2-1, 2010.
- [8] 片下 敏宏, 佐藤 証, 永田 真, 藤本 大介, “暗号 LSI の電源ノイズシミュレーションによるサイドチャネル解析,” **マルチメディア, 分散, 協調とモバイル (DICOMO) シンポジウム**, 講演番号 7F-2, pp. 1666-1672, 2010.
- [9] 藤本 大介, 片下 敏広, 佐々木 明彦, 堀 洋平, 佐藤 証, 永田 真, “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,” *Symposium on Cryptography and Information Security (SCIS)*, 講演番号 1C2-6, 2012.
- [10] 藤本 大介, 田中 大智, 永田 真, “容量充電モデルを用いたシミュレーションによるサイドチャネル情報漏洩探索手法,” *Symposium on Cryptography and Information Security (SCIS)*, 講演番号 1E1-2, 2013.
- [11] 田中 大智, 藤本大介, 永田 真, “容量充電モデルを用いたシミュレーションによる相関電力解析の考察,” *Symposium on Cryptography and Information Security (SCIS)*, 講演番号 1E2-2, 2013.
- [12] 遠藤 翔, 李 陽, 本間 尚文, 崎山 一男 藤本 大介, 永田 真, 太田 和夫, 青木 孝文 “故障感度隠蔽のための効率的な対策とその評価,”

Symposium on Cryptography and Information Security (SCIS), 講演番号 1E1-5, 2013.

- [13] 藤本 大介, 田中 大智, 三浦 典之, 永田 真, 林 優一, 本間 尚文, 青木 孝文, 堀 洋平, 片下 敏広, 崎山 一男, Thanh-Ha Le, Julien Bringer, Pirouz Bazargan-Sabet, Shivam Bhasin, Jean-Luc Danger “チップ内外での電源電圧取得によるサイドチャネル漏洩情報の一考察,” *Symposium on Cryptography and Information Security (SCIS)*, 講演番号 2A3-3, 2014.

口頭発表

- [14] D. Fujimoto, T. Katashita, Y. Hori, A. Satoh, and M. Nagata, “A Fast Power Current Simulation of Cryptographic VLSI Circuits for Side Channel Attack Evaluation,” *Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, Poster, 2011.
- [15] D. Fujimoto, D. Tanaka, and M. Nagata, “A simulation methodology searching side-channel leakage using capacitor charging model,” *International Workshop on Security (IWSEC)*, Poster, 2012.

技術報告

- [16] 藤本 大介, 三浦 典之, 永田 真, “サイドチャネル攻撃評価のための電源ノイズモデル,” *電磁環境工学情報 (EMC)*, No.306 pp 31 - 39 , 2013.

その他の発表論文

学術講演

- [17] 藤本 大介, 松野 哲郎, 小坂 大輔, 濱西 直之, 田邊 顕, 塩地 正純, 永田 真, “65nm CMOS テクノロジによる 6bit 任意デジタル雑音エミュレータの開発,” *電子情報通信学会 信学技報 ICD2009-34* ,pp. 7-10, 2009 年 10 月.

口頭発表

- [18] 藤本 大介, 松野 哲郎, 永田 真, “CMOS デジタル回路における雑音発生モデル化と実証,” 電子情報通信学会 若手研究会, ポスター, 2009 年 12 月.

図一覧

1.1	全世界でのスマートカード出荷数の推移	2
1.2	サイドチャネル攻撃イメージ	3
1.3	消費電力による内部状態推定イメージ	3
1.4	AES のブロック図	4
1.5	電力解析攻撃における測定手法	9
1.6	電力解析攻撃に対する耐性評価フロー	10
2.1	容量充電モデルの等価回路	14
2.2	容量充電モデルにおけるスタンダードセルの寄生容量値導出	15
2.3	2 入力 NAND ゲートの消費電流シミュレーション	15
2.4	DFF の消費電流シミュレーション	16
2.5	容量充電モデルモデリングフロー	17
2.6	容量充電モデルを用いた CPA フロー	19
2.7	65nmCMOS チップのレイアウト	20
2.8	測定環境	21
2.9	SASEBO-R ボード	22
2.10	AES 全ラウンドと最終ラウンドでの電源ノイズ波形 (a) シ ミュレーション結果 (b) 実測結果	24
2.11	最終ラウンドでの Table S-box 実装での回路ブロックごと の消費電流シミュレーション	25
2.12	各鍵候補の波形数に対する相関の最大値 (Composite S-box) (a) シミュレーション結果 (b) 実測結果	27
2.13	各鍵候補の波形数に対する相関の最大値 (Table S-box) (a) シミュレーション結果 (b) 実測結果	28
2.14	各鍵候補の波形数に対する相関の最大値 (PPRM 1 stage S-box) (a) シミュレーション結果 (b) 実測結果	29
2.15	各鍵候補の波形数に対する相関の最大値 (PPRM 3 stage S-box) (a) シミュレーション結果 (b) 実測結果	30
2.16	4 種類の S-box 実装を行った AES 回路へ対する CPA 結果 (a) シミュレーション (b) 1 オーム法による実測	32

2.17	二つの異なる鍵を用いた場合の Table S-box AES に対する CPA 結果	33
2.18	130 nm CMOS で試作したチップでの CPA 結果 (a) シミュレーション (b) 1 オーム法による実測	34
3.1	チップ内外での波形の変化イメージ	38
3.2	オンチップモニタフロントエンド (a) 回路図 (b) ラッチコンパレータによる比較	39
3.3	オンチップモニタによる連続波形取得イメージ	39
3.4	オンチップモニタ搭載暗号化チップのブロック図	40
3.5	テストチップレイアウトとデザインサマリ	41
3.6	測定評価環境	42
3.7	1 Ω 法による測定環境ブロック図	43
3.8	オンチップモニタによる測定環境ブロック図	44
3.9	サンプリングタイミング生成フロー	44
3.10	測定波形 (a) オンチップモニタ (b) 1 Ω 法	46
3.11	測定による CPA 結果 (a) オンチップモニタ (b) 1 Ω 法	47
3.12	100MHz 10MHz 3MHz のローパスフィルタ処理を行った波形 (a) オンチップモニタ (b) 1 Ω 法	48
3.13	FFT 波形 (a) オンチップモニタ (b) 1 Ω 法	49
3.14	ローパスフィルタ後の CPA 結果 (a) オンチップモニタ (b) 1 Ω 法	50
3.15	CPA に用いた波形と時間方向における相関値推移 (a) オンチップモニタ (b) 1 Ω 法	52
3.16	ハミング距離と電源電圧ドロップ 通常電源電圧 (1.2V) 時 (a) オンチップモニタ (b) 1 Ω 法	53
3.17	ハミング距離と電源電圧ドロップ 低電源電圧 (0.75V) 時 (a) オンチップモニタ (b) 1 Ω 法	53
4.1	AES の最終ラウンドでのデータフロー	56
4.2	AES でのデータマトリクス	57
4.3	CPA を用いたサイドチャネル攻撃評価フロー	58
4.4	CPA のイメージ (a) ランダムな平文 (b) ハミング距離統一平文	59
4.5	Shiftrows 演算でのマトリクス内のデータ移動	60
4.6	WDDL セルのイメージ	61

4.7	チップレイアウトとデザインサマリ	62
4.8	測定環境	63
4.9	Composite S-box でのハミング距離依存性 (a) ランダムな 入力平文 (b) 選択平文入力	65
4.10	異なる S-box 実装における選択平文を用いた場合のハミング 距離依存性 (a) Table S-box (b) PPRM 1-stage S-box (c) PPRM 3-stage Sbox	66
4.11	選択平文での CPA 結果	67
4.12	WDDL 実装 AES の電源ノイズ波形 (a) 1 Ω 法による実測 (b)TSDPC モデルによるシミュレーション	68
4.13	CPA 結果	69

表一覧

1.1	暗号化回路におけるサイドチャネル情報漏洩シミュレーション	8
2.1	2入力 NAND ゲートの全入力遷移	17
2.2	AES 暗号化回路における異なる S-box 実装間の規模差 . . .	20
2.3	シミュレーションのコスト	26
4.1	Shiftrow 演算における各マトリクス位置の関連	60

神戸大学博士論文「暗号モジュールの電源ノイズと情報漏洩に関する研究」全 102 頁

提出日 2014 年 1 月 21 日

本博士論文が神戸大学機関リポジトリ **Kernel** にて掲載される場合、掲載登録日(公開日)はリポジトリの該当ページ上に記載されます。

© 藤本 大介

本論文の内容の一部あるいは全部を無断で複製・転載・翻訳することを禁じます。