



電子 1238

修士論文

微細素子のパラメータばらつきによる
耐タンパーLSIの劣化と対策

山内 裕史

東京大学大学院 工学系研究科 電子工学専攻
学籍番号 46413

指導教官 浅田 邦博 教授

提出日 平成18年2月3日

目次

第1章 序論	1
1.1 研究の背景	1
1.2 研究の目的	3
1.3 本論文の構成	4
第2章 標準1線式 CMOS 回路に対しての差分電磁界解析シミュレーション	5
2.1 電力解析・電磁界解析の原理・概要	5
2.1.1 電力解析	5
2.1.2 単純電力解析	6
2.1.3 差分電力解析	7
2.1.4 電磁界解析	9
2.2 差分電力解析・差分電磁界解析の手順	9
2.3 標準1線式 CMOS 回路に対しての差分電磁界解析シミュレーション	13
2.3.1 差分電磁界解析シミュレータの目的・利点	13
2.3.2 差分電磁界解析シミュレーション手順の流れ	14
2.3.3 DES の LSI レイアウト生成	16
2.3.4 攻撃対象となる注目配線の抽出	17
2.3.5 配線論理の設定	19
2.3.6 内部配線からの配線電流の見積もり	19
2.3.7 配線から発生する電磁波の見積もり	19
2.3.8 観測アンテナの配置と空間電位差の計算	21
2.3.9 アンテナ空間電位差の値を用いた差分解析	26
2.4 シミュレーション結果	26
2.4.1 DES の LSI レイアウトへの解析結果	26
2.4.2 観測アンテナの高さを変化させた場合の解析必要サンプル数の変化	28
2.4.3 空中雑音の影響を考慮した解析シミュレーション	29
2.5 注目配線からの放射電磁波削減による差分電磁界解析対策手法	31
2.5.1 注目配線の配線長縮小による対策手法	31
2.5.2 注目配線のインバータ分割による対策手法	33

第3章	微細素子のパラメータばらつきによる耐タンパーLSIの劣化	36
3.1	固有電力消費アーキテクチャによる耐タンパーLSI	36
3.1.1	Wave Dynamic Differential Logic	38
3.1.2	Sense Amplifier Based Logic	39
3.1.3	キャパシタを用いて消費電力波形の固有化を図る回路方式	40
3.2	微細素子のパラメータばらつきが耐タンパーLSIに与える影響	42
3.3	微細素子のパラメータばらつきを利用した耐タンパーLSIへの解析手法	43
3.4	WDDL回路に対しての解析シミュレーション	45
3.4.1	WDDL相当のDES暗号のLSIレイアウトの生成	46
3.4.2	2線式相補配線における内部配線からの配線電流の見積もり	48
3.4.3	注目周波数の決定と観測アンテナ位置の最適化	48
3.5	シミュレーション結果	55
3.5.1	DESのLSIレイアウトへの解析結果+ばらつき環境	55
3.5.2	観測アンテナの高さを変化させた場合の解析必要サンプル数の変化	57
3.5.3	空中雑音の影響を考慮した解析シミュレーション	58
3.5.4	全体のDES暗号鍵解析	59
第4章	素子ばらつきを考慮した電磁界解析への耐性を持った耐タンパーLSIの設計手法の提案	63
4.1	注目配線の配線長の縮小による対策手法	63
4.2	注目配線に対してのインバータ分割による対策手法	66
4.3	乱数を利用した相補配線にアンバランスがあっても解析不能なデータバス	67
4.4	3線式データエンコード方式を利用した対策手法	70
第5章	デバイスのスケージングにおける、素子ばらつきを考慮した電磁界解析への脆弱性の変化	74
5.1	製造プロセスをスケージングにより変化させた解析結果	74
5.2	しきい値ばらつきの分散モデルを適応させたスケージング結果	77
第6章	結論	81

参考文献	83
本研究に関する発表	86
謝辞	87

目次

1.1	スマートカード内のチップの概要	1
1.2	スマートカードの例	2
1.3	耐タンパー性についての攻撃	3
2.1	DES オペレーションの電流波形	7
2.2	DES オペレーションの第 2・3 ラウンドの電流波形	7
2.3	DES 暗号処理における消費電力の測定	10
2.4	DES の第 16 段から暗号文出力まで	11
2.5	相関波形の比較	12
2.6	予測鍵と相関波形のピークの比較	12
2.7	測定波形数と相関関数のピークの関係	13
2.8	標準 1 線式 CMOS 回路に対しての差分電磁界解析シミュレーションの手順	15
2.9	DES 暗号回路の入出力図	16
2.10	DES 暗号回路のタイミング図	17
2.11	自動合成された DES の LSI レイアウト(600um×600um)	17
2.12	注目配線の設定	18
2.13	注目配線の長さの比較	18
2.14	攻撃対象とした第 24bit 配線(821.68um)	18
2.15	微小ダイポールアンテナモデル	20
2.16	仮想配線からのリターン電流の考慮	20
2.17	配線分割による精度向上	20
2.18	チップ上のアンテナ配置	21
2.19	x 軸平行にアンテナを配置した場合のアンテナ空間電位差マップ	22
2.20	y 軸平行にアンテナを配置した場合のアンテナ空間電位差マップ	23
2.21	注目配線からの電界強度マップ	24
2.22	注目配線からの磁界強度マップ	25
2.23	サンプル数 1000 の場合の予測鍵と相関値	27
2.24	サンプル数 50000 の場合の予測鍵と相関値	28
2.25	サンプル数の変化と相関値の推移	28
2.26	観測アンテナの高さと解析必要サンプル数	29
2.27	測定距離 10m での情報技術装置の放射妨害波の許容値	31
2.28	第 27bit 注目配線 (85.4um)	32
2.29	サンプル数 1000 の場合の予測鍵と相関値	32

2.30	サンプル数 50000 の場合の予測値と相関値	33
2.31	サンプル数の変化と相関値の推移	33
2.32	注目配線のインバータ分割	34
2.33	注目配線の分割数の変化と相関電位差の変化	34
2.34	注目配線の分割数の変化と解析必要サンプル数の変化	35
3.1	WDDL 回路の構成	38
3.2	正論理と負論理の配線容量の均等化	39
3.3	標準 1 線式 CMOS 回路と WDDL 回路における電流波形の比較	39
3.4	SABL 回路の構成	40
3.5	回路の外部に 2 つのキャパシタを接続した回路方式	41
3.6	キャパシタを用いた回路方式の動作波形	41
3.7	しきい値ばらつきが駆動波形に与える影響	42
3.8	素子ばらつきを考慮した電磁界解析手法の概要	44
3.9	素子ばらつきを考慮した電磁界解析シミュレーション手順	45
3.10	解析対象とした WDDL 相当 DES 回路(840um×840um)	46
3.11	1 線式配線の 2 線式相補配線への変換	47
3.12	注目配線の長さの比較	47
3.13	攻撃対象とした第 24bit 配線(964.5um)	47
3.14	観測アンテナ配置	49
3.15	注目周波数と相関信号	49
3.16	x 軸平行にアンテナを配置した場合のアンテナ空間電位差マップ (100MHz 成分)	51
3.17	y 軸平行にアンテナを配置した場合のアンテナ空間電位差マップ (100MHz 成分)	52
3.18	注目配線からの電界強度マップ (100MHz 成分)	53
3.19	注目配線からの磁界強度マップ (100MHz 成分)	54
3.20	サンプル数 1000 の場合の予測値と相関値	55
3.21	サンプル数 50000 の場合の予測値と相関値	56
3.22	サンプル数の変化と相関値の推移	56
3.23	しきい値のばらつき環境と解析必要サンプル数	57
3.24	観測アンテナの高さと解析必要サンプル数	58
3.25	空中雑音を考慮した場合の観測アンテナの高さと解析必要サンプル数	59
3.26	モデル 1 の場合の解析結果	60
3.27	モデル 2 の場合の解析結果	60
3.28	モデル 3 の場合の解析結果	61
3.29	モデル 4 の場合の解析結果	61

4.1	解析の対象とした第 7bit 配線(77.25um)	64
4.2	サンプル数 1000 の場合の予測値と相関値	64
4.3	サンプル数 50000 の場合の予測値と相関値	65
4.4	サンプル数の変化と相関値の変化	65
4.5	インバータによる WDDL 配線分割	66
4.6	注目配線の分割数と相関電位差の変化	67
4.7	注目配線の分割数と解析必要サンプル数の変化	67
4.8	乱数を利用した 2 線式相補配線にアンバランスがあっても解析不能なデータバス	68
4.9	サンプル数 1000 の場合の予測値と相関値	69
4.10	サンプル数 50000 の場合の予測値と相関値	69
4.11	サンプル数の変化と相関値の推移	70
4.12	3 線式伝送方式	71
4.13	シミュレーションに用いた 3 線式データバスのばらつき環境	71
4.14	シミュレーションに用いた 3 線式データバスのばらつき環境	72
4.15	サンプル数 50000 の場合の予測値と相関値	72
4.16	サンプル数の変化と相関値の推移	73
4.17	3 線式伝送方式と乱数を組み合わせたデータバス	73
5.1	LSI レイアウトの比例縮小	75
5.2	各製造プロセスにおけるしきい値ばらつき環境と解析必要サンプル数 (縦軸が linear)	76
5.3	各製造プロセスにおけるしきい値ばらつき環境と解析必要サンプル数 (縦軸が semilog)	76
5.4	MOSFET の模式図	77
5.5	LSI の製造プロセスの進化と解析必要サンプル数の変化	79
5.6	しきい値ばらつきの分散の絶対値と解析必要サンプル数	79

表目次

2.1	差分電力解析の手法（予想値が間違っている場合）	8
2.2	差分電力解析の手法（予想値が正しい場合）	8
2.3	測定距離 10m での情報技術装置の放射妨害波の許容値	30
3.1	DES 暗号に対しての全体の暗号鍵解析結果 （サンプル数 50000 の場合）	62
5.1	スケーリングの際に用いたパラメータ	75
5.2	しきい値ばらつきの分散の絶対値の変化と解析必要サンプル数	80

第 1 章

序論

1.1 研究の背景

近年、コンピュータや IT (Information Technology) 技術、電子商取引の急速な発展に伴ってユビキタス時代が到来している。ユビキタスとは、人々が社会の中でその場所や存在を感じることなくコンピュータやネットワークと接しているような状況を表している言葉である。このユビキタス時代において、IT 技術を安全に利用するための暗号技術、耐タンパーデバイスが非常に重要となってきた。

耐タンパーデバイスとは外部からの攻撃に対して保護対象となるデバイス内の暗号鍵などの秘密情報や秘密情報の処理メカニズムを守秘し、さらにその秘密情報の改変を困難とする性質 (耐タンパー性) を実現するデバイスであり、情報セキュリティ社会を支える重要な技術となっている。

これら耐タンパーデバイスの中で代表的なものとしてされているのが、IC カード・スマートカードである。一般に、IC カードは IC 内にデータを記憶する機能を持ったカード、スマートカードは IC カードのうちで記憶機能の他に処理機能を持っているものと定義されている。これら IC カード・スマートカード (以下、スマートカードで名称を統一) はキャッシュカードほどの大きさのカードの中に CPU、RAM、ROM、EEPROM などで構成された LSI チップが搭載されており (図 1.1)、従来の磁気カードでは実現できない複雑な演算機能や判断機能、大きな記憶容量を実現している。このため、高度な暗号・認証処理を実現することができ、高度なセキュリティを実現している。これらは、社員証などの個人認証や電子マネーなどの多岐にわたる分野において実用化されており (図 1.2)、今後も利用範囲が広がってくると考えられる。

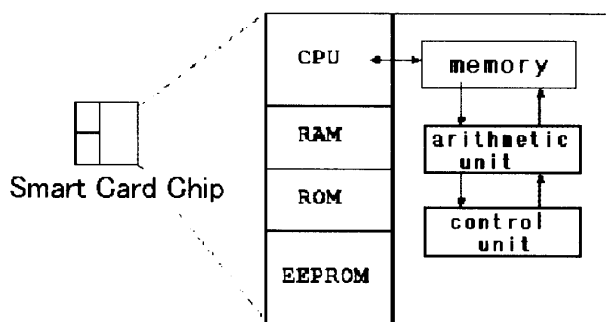


図 1.1 スマートカード内のチップの概要

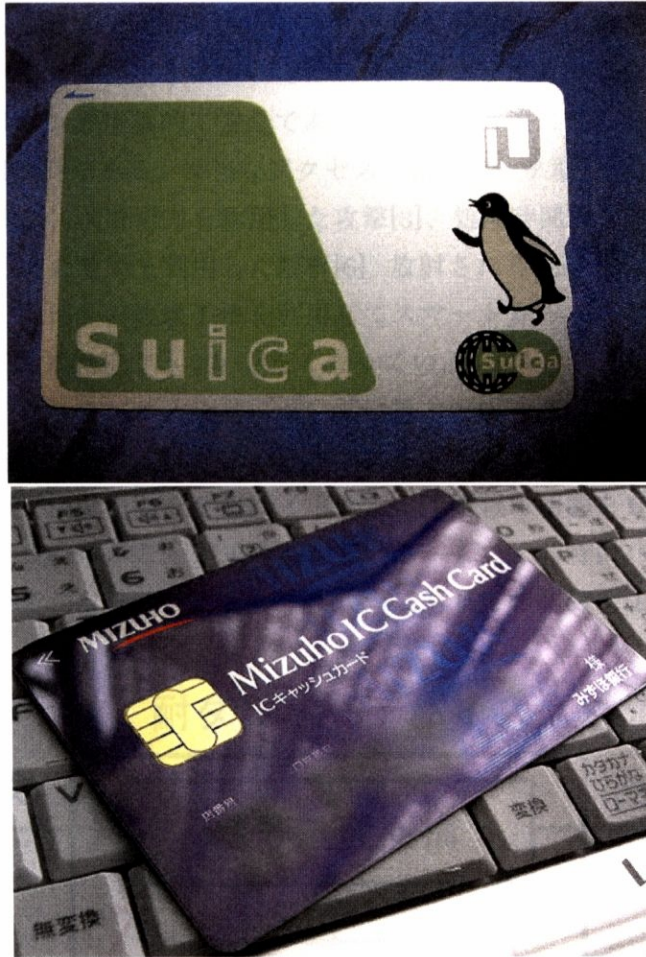


図 1.2 スマートカードの例

上：スマートカードを利用した電子マネー（Suica：JR 東日本）

下：スマートカードを利用した銀行キャッシュカード

このように、スマートカードなどの耐タンパーデバイスに対して重要性が高まってくるのと同時に、これら耐タンパーデバイスの耐タンパー性自身に対しての攻撃に対して関心が高まっている。

これらの耐タンパー性に対しての攻撃は主に耐タンパーデバイス自身を破壊して内部の秘密情報を得る破壊攻撃（Invasive attack）と耐タンパーデバイス自身には被害を与えずに秘密情報を得る非破壊攻撃（Non-invasive attack）に分類される。一般に非破壊攻撃において攻撃に用いられる消費電力や処理時間、放射される電磁波のような、設計者の予想しなかった暗号デバイス固有の付加情報を用いた解析はサイドチャネル攻撃と呼ばれている[1]。

従来は、暗号デバイスから秘密鍵などの秘密情報を取り出す攻撃手法としては、総当たりで鍵を検索したり、暗号アルゴリズムの脆弱性をつくことで強度を下げる方法がとられていた。これら従来の暗号デバイスに対しての攻撃に対しての安全性の検討としては、鍵

長の検討などといった暗号アルゴリズム自身に対する安全性に対するものが殆どであった。しかし、サイドチャネル攻撃については暗号アルゴリズムの安全性だけでは不十分であり、暗号アルゴリズムが理論的に安全であっても実装方法によってはより短時間で秘密情報を抽出できる可能性がある。不当なアクセス・秘密データ取得手法（図 1.3）としてはプローブによる攻撃[2]、消費電力を利用した攻撃[3]、処理時間のタイミングを利用した攻撃[4][5]、意図的に与えた故障を利用した解析[6]、放射される電磁波を用いた攻撃[7]等が挙げられる。実際に、これらの攻撃手法を利用してスマートカードなどを対象とした攻撃の成功例も報告されており無視できない状況となっている。

そのため、現在の暗号デバイス設計においては電力解析・電磁界解析などのサイドチャネル攻撃に対して耐性のある設計が求められており、暗号デバイスの設計者には、暗号デバイス内の秘密情報が消費電力などのサイドチャネル情報に相関をもって現れないように注意深くデバイスを設計することが求められている。また、同時にハードウェア、ソフトウェアの両面においてこれらサイドチャネル攻撃に対する防御手法が多数提案されている。

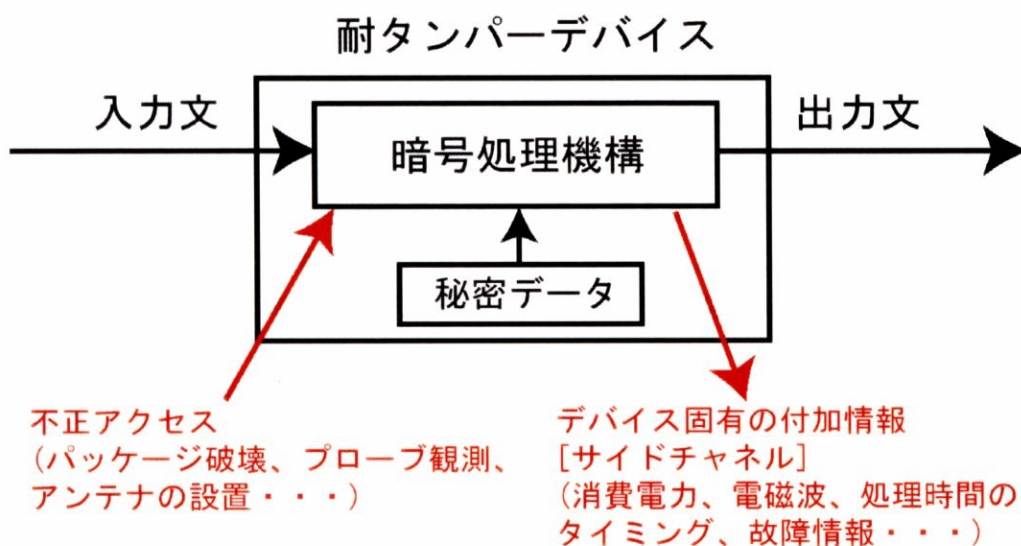


図 1.3 耐タンパー性についての攻撃

1.2 研究の目的

本研究では、これら耐タンパー性に対する攻撃のうち、消費電力やデバイスから放射される電磁波を利用した解析について特に着目する。

これらの攻撃に対する防御例としてハードウェア、特に LSI 回路のレベルからのアプローチとしては 2 線式回路などを利用した電力消費変動が発生しにくい耐タンパー LSI 回路方式が提案されている。しかし、これらの固有電力消費を削った耐タンパー LSI 回路方式についてもさらに隠された脆弱性が存在するかどうか検討する。

特に、本研究では、LSIの素子ばらつきに着目し、レイアウト的に完全に双補的に構成された固有電力消費電力回路であっても、しきい値ばらつきが電流波形、さらに外部に放射される電磁波に対して与える影響を考慮することで、ばらつきによるアンバランスが隠されたサイドチャネルとなり、LSI自身の耐タンパー性が劣化しないか検討し、解析シミュレーションを行う。さらに、十分に攻撃が行えるための解析手法の提案や攻撃に必要な素子ばらつきのレベルを調査する。また、これらの素子ばらつきを利用した解析手法に対しての防御策も検討し、提案する。

1.3 本論文の構成

本論文の構成を説明する。第2章では、電力解析と電磁界解析について説明を行い、標準1線式CMOS回路に対しての差分電磁界解析シミュレーションを行い差分電磁界解析シミュレータの有効性を示した上で解析結果を示す。さらに、差分電磁界解析への対策手法を提案し、有効性をシミュレーションによって確認する。第3章では、差分電磁界解析に耐性を持つとされる固有電力消費アーキテクチャを持ったWDDL回路に対して、素子ばらつきを考慮した上で差分電磁界解析を適応させた解析を行うことで暗号鍵の解析を行うことが可能であることを提案し、シミュレーションによって解析の有効性を確認する。第4章では、素子ばらつきを考慮した電磁界解析を行うことを防ぐための対策手法を複数提案して、シミュレーションにより有効性を確認する。第5章では、素子ばらつきを考慮した電磁界解析のシミュレーションにデバイススケールリングを適応して、今後の製造プロセスの進化と素子ばらつきを考慮した電磁界解析への脆弱性の関連を調べる。最後に第6章で結論を述べる。