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設計手法の提案

第3章でのシミュレーション結果によって素子ばらつきを考慮した耐タンパーLSI への解析が有効であることが示された。よって、本章では素子ばらつきなどの影響を考慮しても差分電磁界解析手法に防御できる対策手法を複数提案し、有効性をシミュレーションにて確認する。

4.1 注目配線の配線長の縮小による対策

LSI の内部配線から放射される放射電磁波は、配線長が短くなるほど小さくなるから攻撃に使われる可能性のある注目配線を短くすることが、標準1線式 CMOS 回路と同様に有効な対策となると考えられる。この原理に従って、配線長の短い注目配線に対して同様のシミュレーションを実行する。ここで、第3章で解析を行った DES 暗号の WDDL 相当回路の 32 本の注目配線のうち最も短い第 7bit 配線(図 4.1：77.25um)に注目し、第3章と同様のシミュレーションを行った。

図 4.2 と図 4.3 は注目配線のばらつきが 1.0%、その他の配線の標準偏差が 1.0%という状況についてサンプル数を 1000 と 50000 取った場合の相関値のプロットである。この場合は真の鍵を key=41 としている。この場合も 50000 サンプルを取っても正しい鍵で相関値がピークを示さず、解析が不可能となっている。なお、相関トレースの変化は図 4.4 に示す。

実際には攻撃対象の分類を正しく行っているので真の相関値に近い値は相関値に現れるはずだが、この値は非常に小さく、相関値のサンプルのばらつきの影響が大きすぎるせいで解析して取り出すのが非常に難しくなっている。

よって、本提案解析手法の対策として、攻撃に用いられる可能性のある配線の長さを極力小さくすることが有効な対策となることが確認できた。この結果を利用して例えば自動合成で暗号回路を生成する場合には、攻撃に使われるおそれのある内部配線はある一定以下に縮小するといった対策を行うことが望ましいと言える。

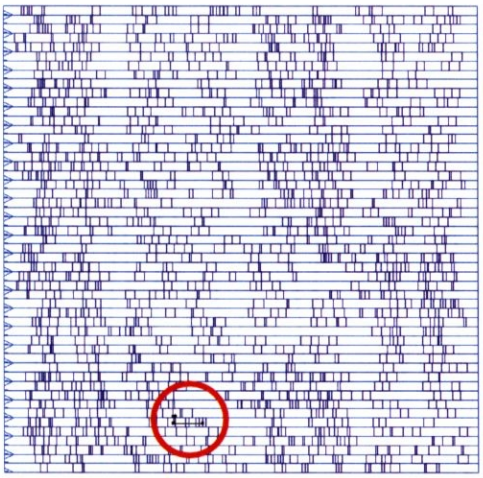

図 4.1 解析の対象とした第 7bit 配線(77.25um)

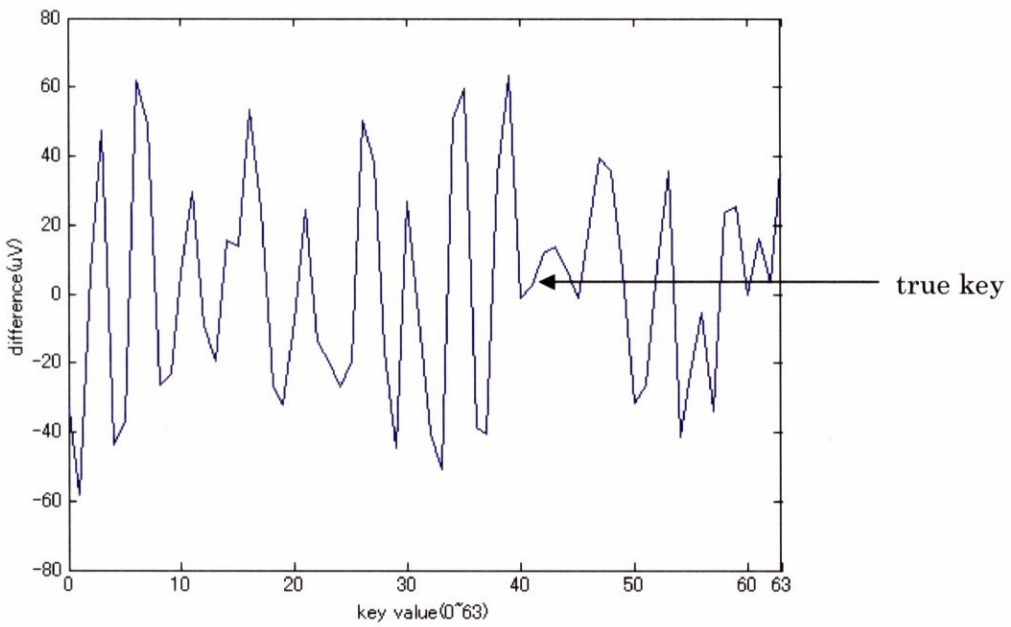

図 4.2 サンプル数 1000 の場合の予測鍵と相関値

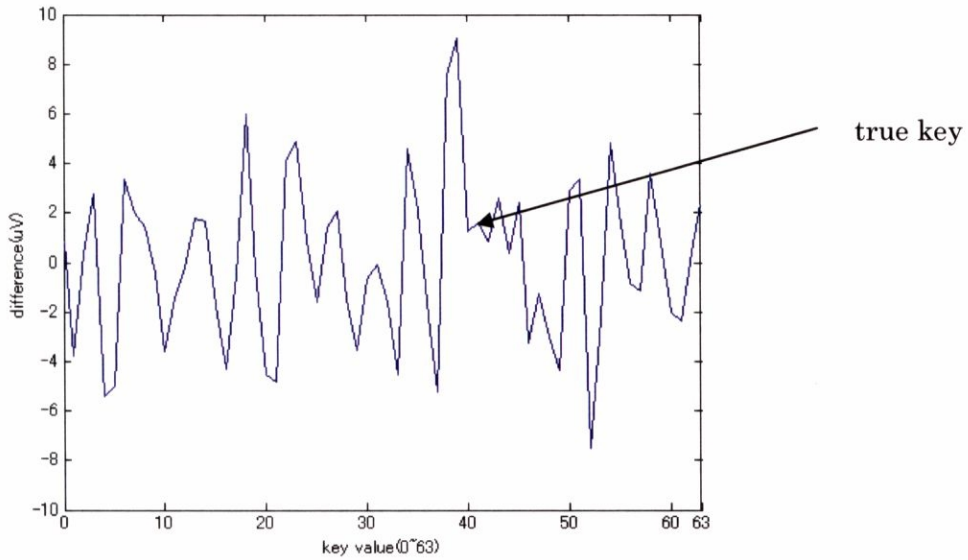

図 4.3 サンプル数 50000 の場合の予測鍵と相関値

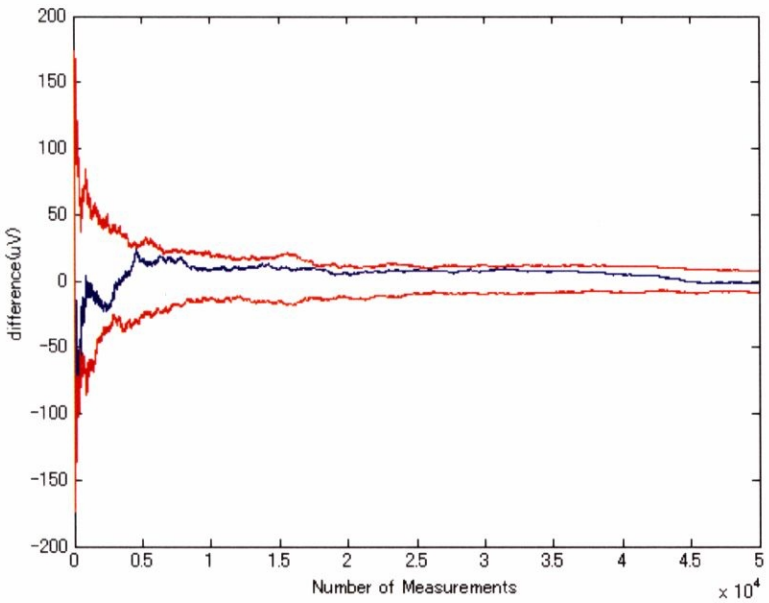

図 4.4 サンプル数の変化と相関値の変化

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

2.5.2 項と同様に注目配線の大まかなレイアウトはそのままにした上で、相関信号を小さくするような対策手法として、注目配線にインバータを用いて分割する対策手法（図 4.5）を提案する。

この手法では、攻撃に用いられる注目配線はインバータで分割されて短配線の集合となる。インバータで分割された効果により全体としてのアンテナ電位差が小さくなり、さらに、ばらつきの影響が短配線の集合に拡散されて素子ばらつきが与える相関値自体が小さくなることが考えられる。

インバータ分割の対策手法の実証としてシミュレーションを行った。解析対象として第 3 章と同じ WDDL 相当 DES の LSI レイアウトの第 24bit 配線（964.5um）に対し、インバータ分割を行い、解析シミュレーションを行った。ここでは、分割数を 1(分割なし)～10 と変化させ、注目配線がほぼ等長配線の集合になるようにインバータ分割を行った。ばらつき環境は多様に存在しうるので、注目配線のばらつき環境を 1.0%の標準偏差の正規分布で発生させ、1000 回のばらつき環境を発生させた。この 1000 回の相関信号の平均値と、平均的な相関電位差が得られるときの解析必要サンプル数の変化を調べた。

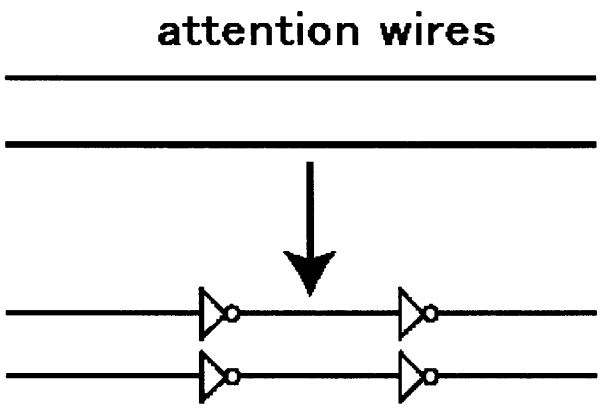

図 4.5 インバータによる WDDL 配線分割

シミュレーションの結果を示す。図 4.6 は配線の分割数と相関電位差の変化を示したものだが、配線分割数の増加につれて相関電位差は小さくなっている。図 4.7 は配線の分割数と解析必要サンプル数の変化を示したものである。配線の分割数の増加に従って必要なサンプル数も増加し、解析が難しくなることがわかった。実際には攻撃対象とした第 24bit 配線においては、6 分割以上に配線を分割すればサンプル数 50000 においては解析不可能となることが示された。

インバータ分割による対策手法はある一定以上の内部配線をインバータで分割すればよいので自動合成にも適応しやすい対策手法であるといえる。

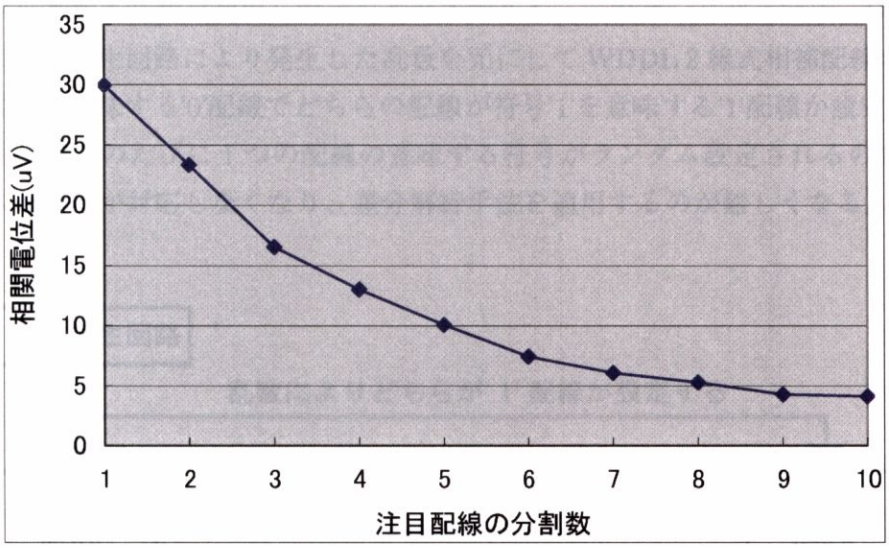

図 4.6 注目配線の分割数と相関電位差の変化

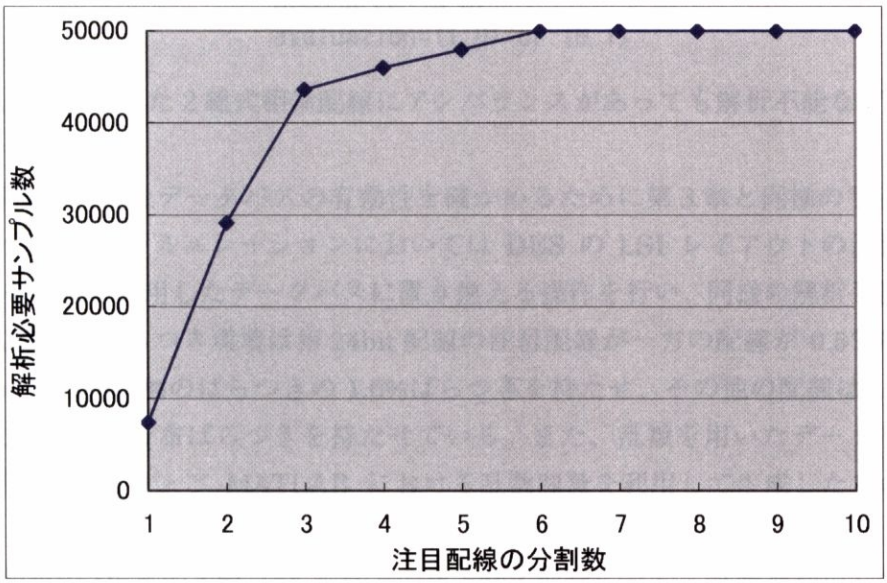

図 4.7 注目配線の分割数と解析必要サンプル数の変化

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

2 線式相補配線には素子ばらつきやレイアウトの不整合によるアンバランスが少なからず必ず生じているので、これらのアンバランスが有ったとしてもデータバスをランダム化することによって、差分解析手法を回避する対策手法を提案する。

図 4.8 が提案する乱数を利用したデータバスである。このデータバスでは、DES の暗号処理ごとに乱数発生回路により発生した乱数を元にして WDDL 2 線式相補配線のどちらの配線が符号'0'を意味する'0'配線でどちらの配線が符号'1'を意味する'1'配線か設定する。これにより、暗号操作のたびに 1 つの配線の意味する符号がランダム設定されるので配線のアンバランスと符号が対応しなくなり、差分解析手法を適用するのが難しくなる。

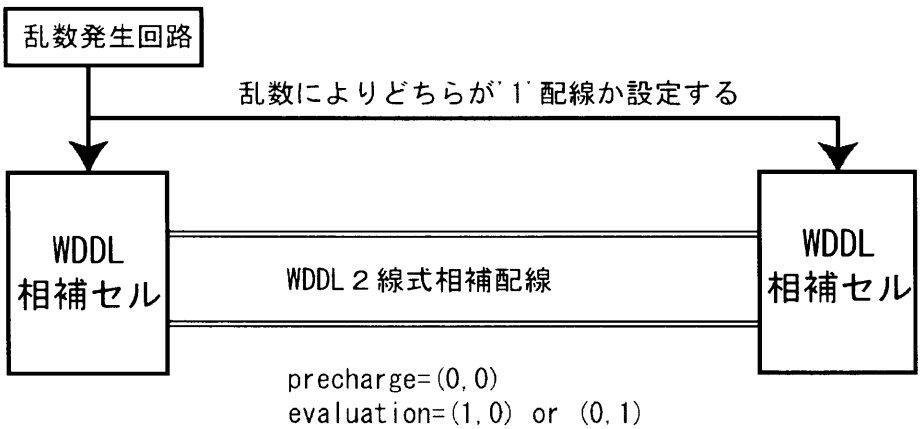

図 4.8 乱数を利用した 2 線式相補配線にアンバランスがあっても解析不能なデータバス

この乱数を利用したデータバスの有効性を確かめるために第 3 章と同様の手法でシミュレーションを行う。シミュレーションにおいては DES の LSI レイアウトの注目配線の第 24bit 配線を乱数を利用したデータバスに置き換える操作を行い、同様の解析手法を行っている。なお、回路のばらつき環境は第 24bit 配線の注目配線が一方の配線が-0.5%ばらつき、他方のばらつきが 0.5%のばらつきの 1.0%ばらつきを持たせ、その他の配線は 1.0%の標準偏差を持たせた正規分布ばらつきを持たせている。また、乱数を用いたデータバスにおける乱数は計算ソフトウェア MATLAB における乱数関数を利用して生成したものを用いている。

WDDL 相当の DES の LSI レイアウトの第 24bit 配線に対して乱数を利用したデータバスを適応した場合の解析シミュレーションの結果を図 4.9～図 4.11 に示す。この場合も真の鍵は key=41 としている。各サンプルにおいて'0'配線と'1'配線の対応がランダム化されているので、これにより、予測鍵に対しての相関信号もほぼランダムな分布を示しており、サンプル数を増加させてもほぼランダムなまま推移している。実際に 50000 サンプルを用いても解析は不可能であった。また、同様に注目配線のばらつきを 1.0%の標準偏差でランダムに発生させて同様の解析を 100 回行ったが、この 100 回の全てにおいて解析は不可能であった。

乱数を利用した差分解析対策手法は対策の信頼性は乱数の精度に大きく左右されると考えられるが、ハードウェアのコストも少なくて精度のよい乱数生成手法が実現できるなら

ば安全で確実な対策手法となりうると考えられる。

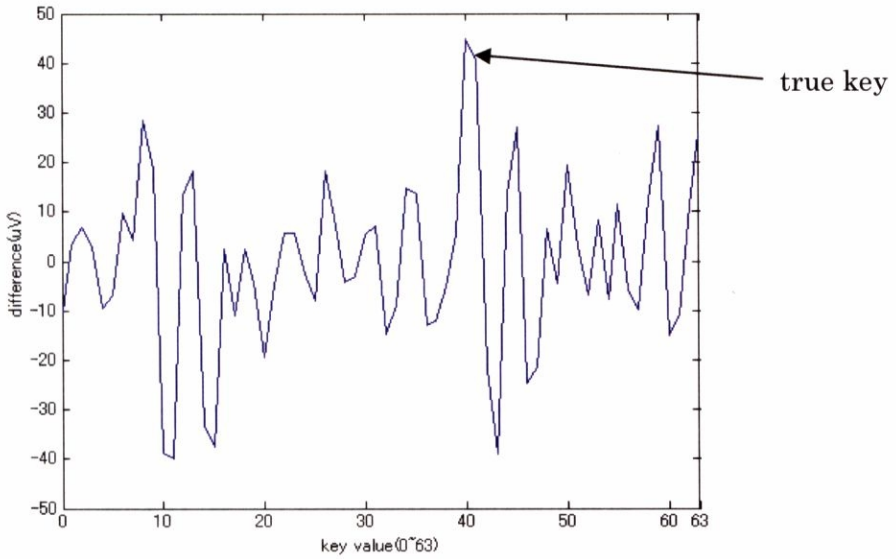

図 4.9 サンプル数 1000 の場合の予測鍵と相関値

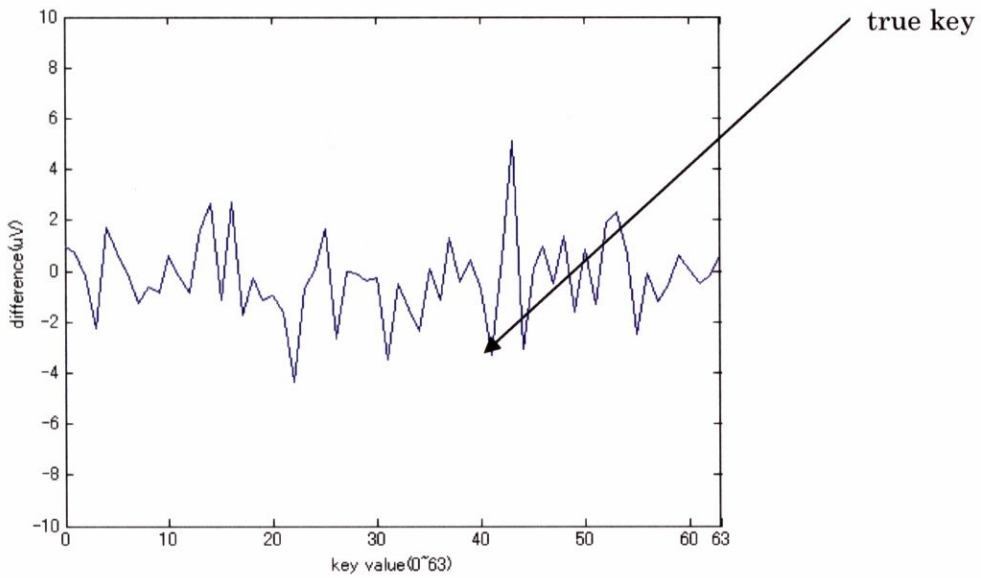

図 4.10 サンプル数 50000 の場合の予測鍵と相関値

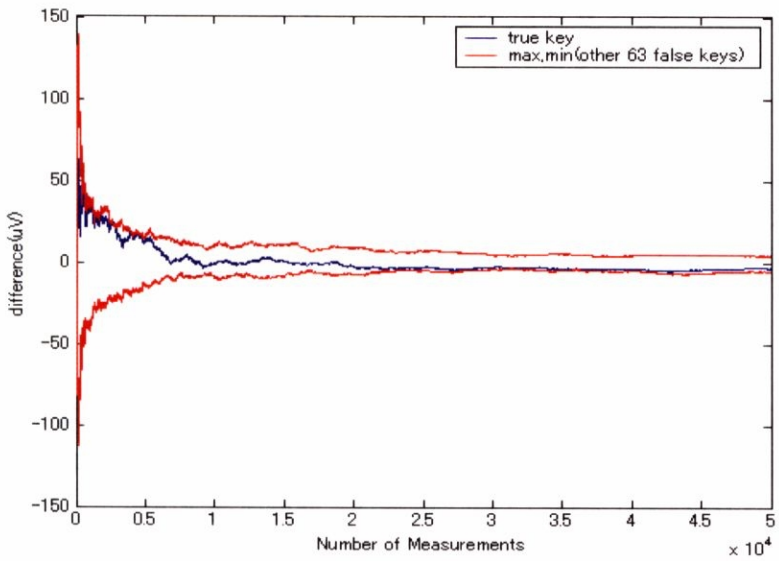

図 4.11 サンプル数の変化と相関値の推移

4.4 3線式データエンコード方式を利用した対策

われわれの研究室では新しいデータバス手法として3 相式伝送方式を提案している[26]。この方式では図 4.12 のようにデータバスの論理が変化しない場合でも 3 本の配線のうち 2 本を必ず遷移するようにエンコードするため、タイミング信号とデータを同時に送ることができる。例えば、ある周期において 3 本の信号線の状態が“010” であったとすると、次の周期でパスの論理が 1 となる場合には“100” に配線を駆動し、論理が 0 となる場合には“001” に駆動する。その状態遷移は図 2.2 に示す。

本対策手法ではこの 3 線式データエンコード方式を元にして、駆動方法では WDDL 的に precharge→evaluation 駆動をさせることで、差分解析手法の対策になりうるか確認する。なお、この場合においては precharge 状態において 3 つの全ての配線が'0'状態となり、一般的な 3 線式伝送方式の駆動とは異なっている。

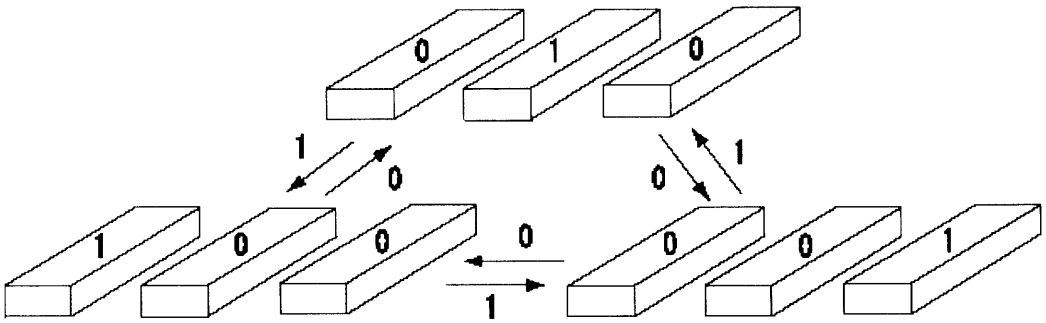

図 4.12 3線式伝送方式

3線式伝送方式においては前状態と次状態において図 4.12 に示すような回転方向（回転方向は初期設定により'1'符号が右回りであるか左回りであるかどちらにも設定できる。）を取っているのである一つの配線の状態と符号が1対1に対応していない。このため、差分解析手法が適応しにくく、データバスの状態も前状態に依存しているのでこの面を考えても解析が難しくなると考えられる。

WDDL 相当の DES の LSI レイアウトの第 24bit 配線に対して乱数を利用したデータバスを適応した場合の解析シミュレーションの結果を示す。このとき3線式伝送方式の3配線のばらつき環境は図 4.13 に示すようなばらつき環境を持たせ、その他の配線のばらつき環境は 1.0%の標準偏差をもつ正規分布ばらつきを取っている。図 4.14 と図 4.15 に予測鍵と相関値の関係を示す。この場合も真の鍵は key=41 としている。各サンプルにおいて配線と符号の対応がとれないので予測鍵に対しての相関信号もほぼランダムな分布を示しており、サンプル数を増加させてもほぼランダムなまま相関値の値を示している（図 4.16)。実際に 50000 サンプルを用いても解析は不可能であった。また、同様に注目配線のばらつきを 1.0%の標準偏差でランダムに発生させて同様の解析を 100 回行ったが、この 100 回の全てにおいて解析は不可能であった。

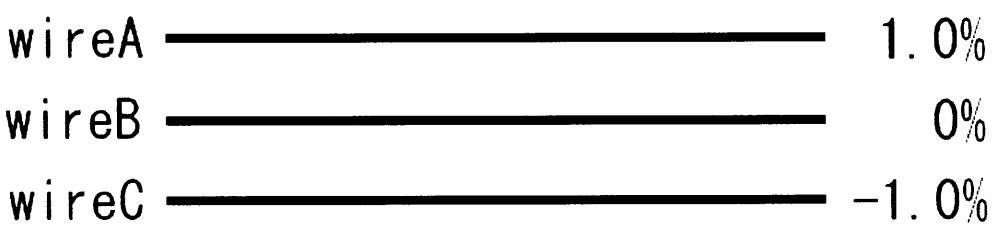

図 4.13 シミュレーションに用いた3線式データバスのばらつき環境

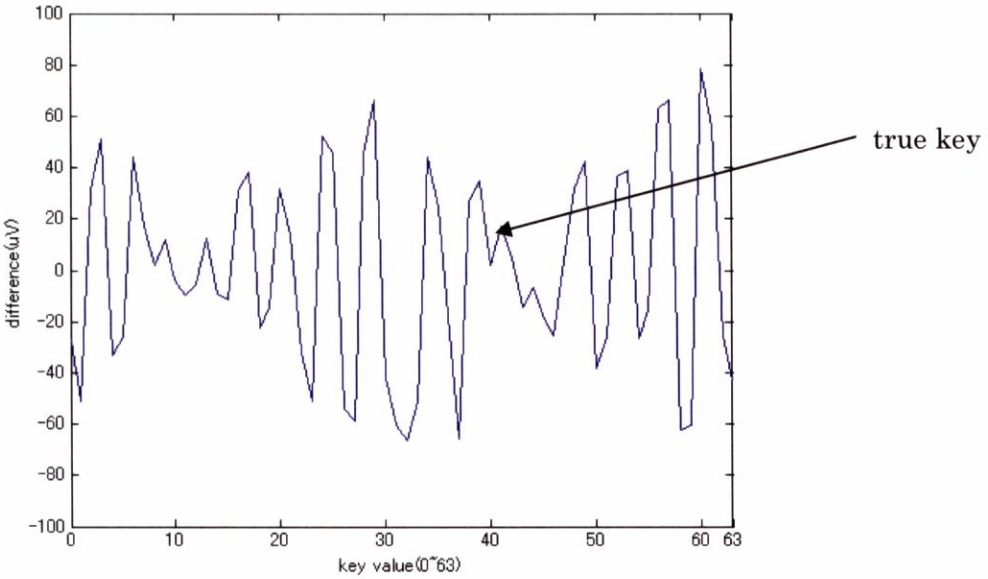

図 4.14 サンプル数 1000 の場合の予測鍵と相関値

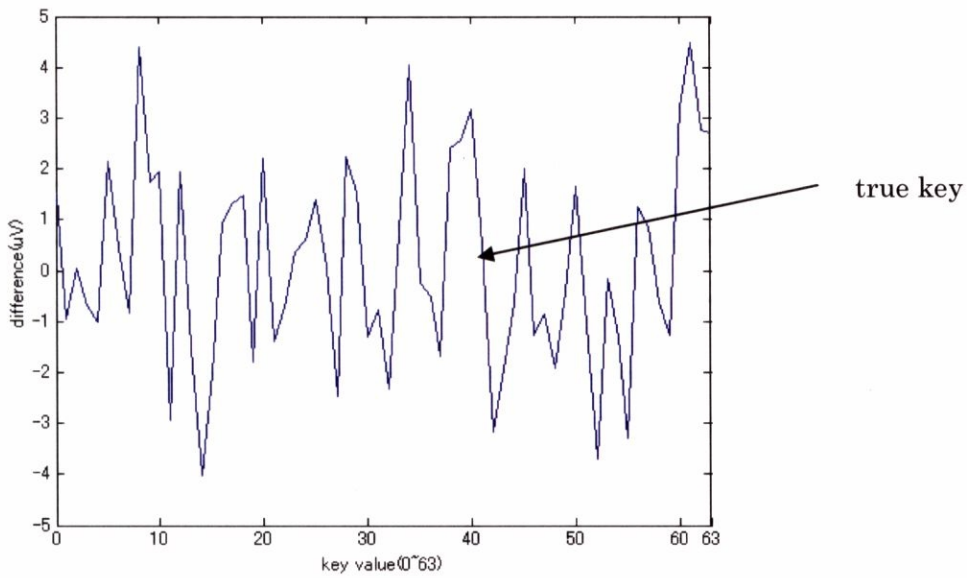

図 4.15 サンプル数 50000 の場合の予測鍵と相関値

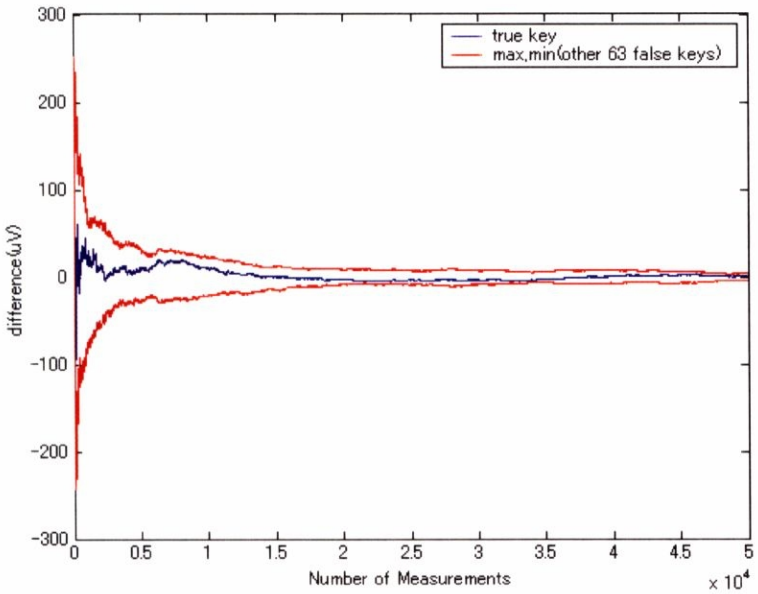

図 4.16 サンプル数の変化と相関値の推移

シミュレーションにより、3線式伝送方式を用いた対策手法の有効性が示されたが、さらに図 4.17 に示すように初期状態と回転方向をオペレーションごとにランダム化すれば安全性はさらに増加すると考えられる。

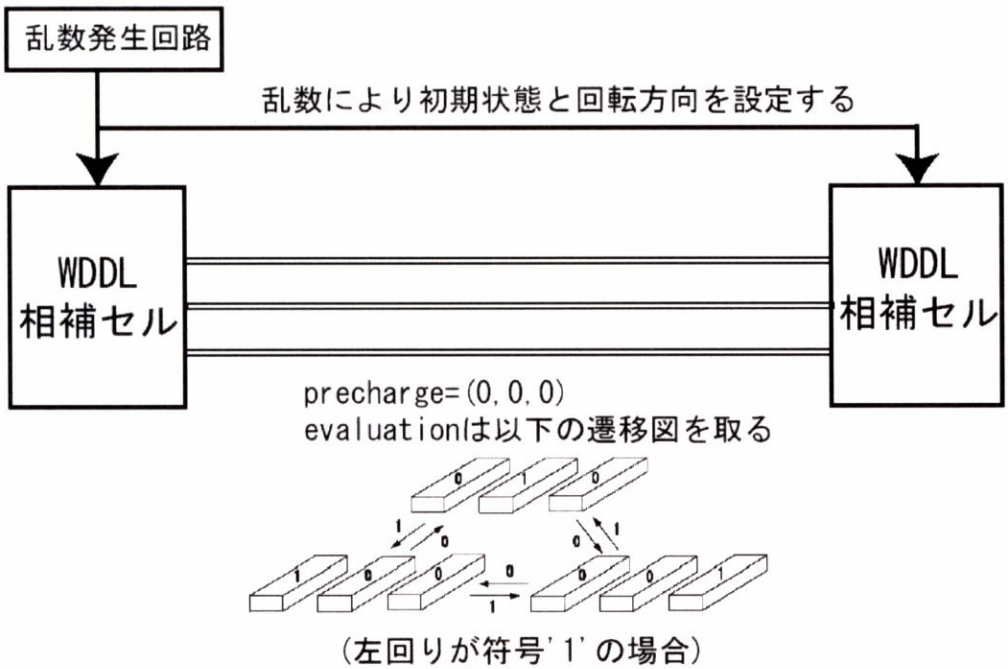

図 4.17 3線式伝送方式と乱数を組み合わせたデータバス

第5章

デバイスのスケーリングにおける、素子ばらつきを考慮した電磁界解析への脆弱性の変化

本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リングを適応させて、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の脆弱性の関連を調べる。

5.1 製造プロセスをスケーリングにより変化させた解析結果

多様な LSI 製造プロセスに対応するため、本シミュレーションでレイアウト生成した350nm プロセスのレイアウトを図 5.1 に示すように比例縮小することにより、180、90、45nm 相当のレイアウトを生成し、さらにばらつき環境を 0%～10.0%と変化させて第3章と同様のシミュレーションを行った。このときスケーリングに当たって用いた物理パラメータなどは表 5.1 の値を用いている。これら製造プロセスを変えた DES 暗号の LSI レイアウトにおいても、すべてのプロセスについてその都度もっとも効率のよい周波数をシミュレーションにより選んで解析しているが、どの製造プロセスの場合も基本周波数において最大の相関値が得られた。この理由は 3.4.3 項と同様に説明できると考えられる。アンテナ配置においても、全ての解析の場合においてアンテナ電位差マップに従って注目配線からもっとも大きいアンテナ電位差が得られるように配置している。また、どの製造プロセスにおいても観測アンテナの長さは 1mm、観測点の高さも 1mm で固定している。このとき、解析必要サンプル数とは正しい鍵のトレースが全ての誤った鍵のトレースの外側になったとされるサンプル数を定義している。

プロセスの進化と解析必要サンプル数の関連についてのシミュレーション結果を図 5.2 と図 5.3 に示す。どのプロセスの場合もばらつきを素子ばらつきがない場合（ばらつき 0%）に比べてばらつきがある環境の方が解析に非常に有利になっている。しかしながら、ばらつきの程度と解析必要サンプル数の関連はあまり判断されなかった。また、プロセスが進

化するにつれて解析必要サンプル数は大きくなり、解析が難しくなっている。これは、DES のチップは同一のレイアウトを比例縮小して作っているので、配線の長さもスケーリングを受けて小さくなり、注目配線からの電流値の絶対値が減っているからであると考えられる。よって、同一の IP コアなどを用いて暗号回路を実装する場合には最新のプロセスを用いて製造した方が本提案手法の耐性が得られるということが示された。

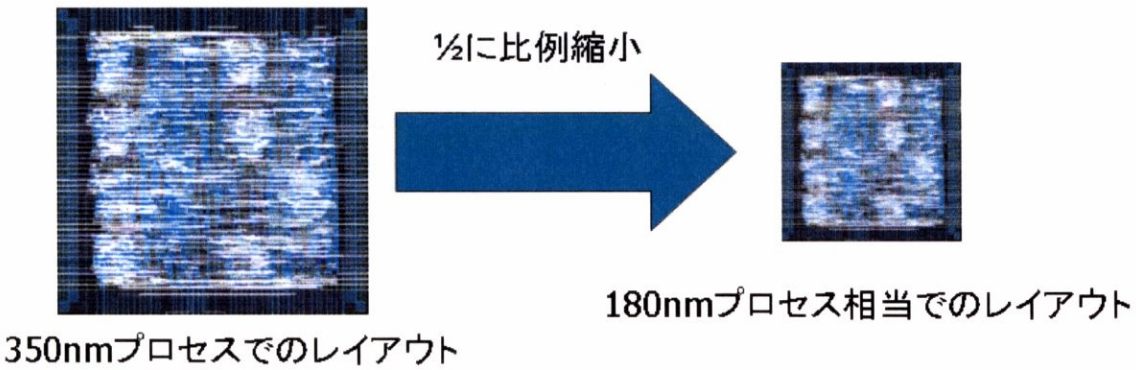

図 5.1 LSI レイアウトの比例縮小

製造プロセス	Vdd [V]	Vth [V]	配線容量 [fF/um]	時定数 [ps]	駆動周波数 [MHz]
350nm	3.3	0.7	0.17	120	100
180nm	1.8	0.4	0.24	60	200
90nm	0.9	0.26	0.24	30	400
45nm	0.7	0.22	0.24	15	800

表 5.1 スケーリングの際に用いたパラメータ

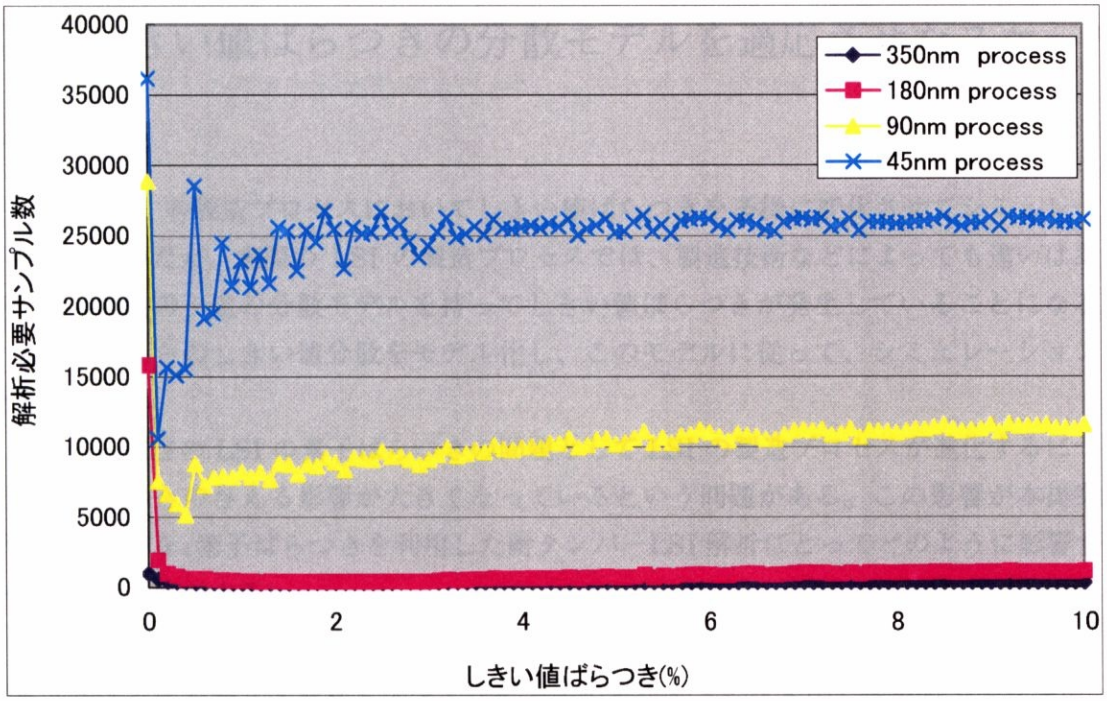

図 5.2 各製造プロセスにおけるしきい値ばらつき環境と解析必要サンプル数
（縦軸が linear）

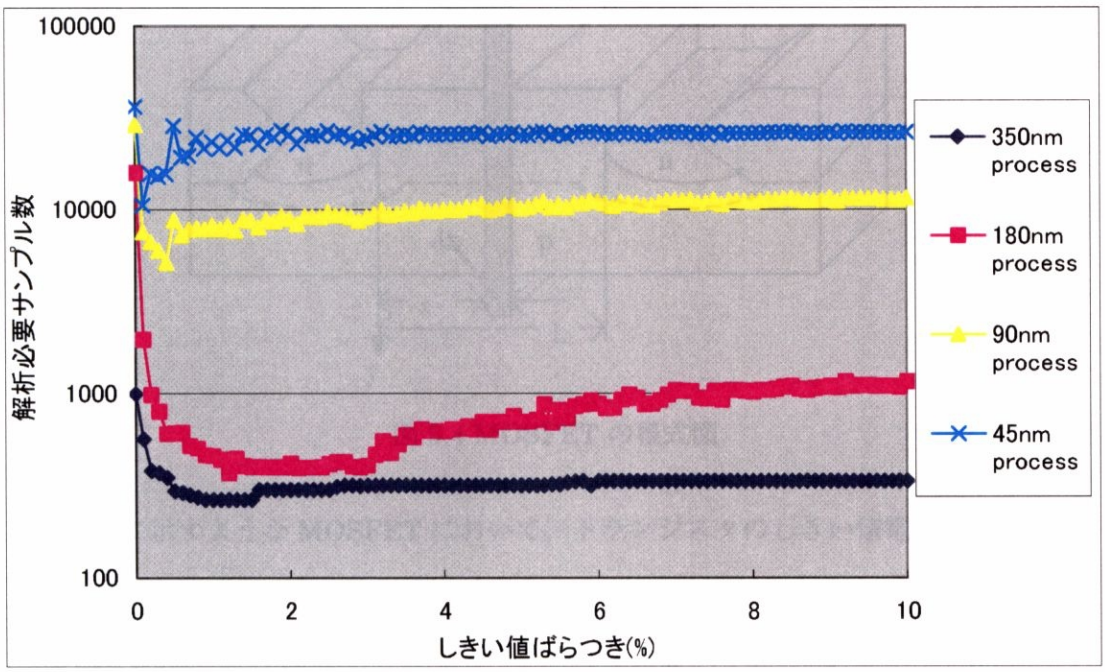

図 5.3 各製造プロセスにおけるしきい値ばらつき環境と解析必要サンプル数
（縦軸が semilog）

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リング結果

5.1 項では、各製造プロセスにおいてしきい値ばらつきを多様に変化させてシミュレーションしたものだが、実際の LSI の製造プロセスでは、製造技術などによっても違いはあるが、ある程度の一定の分散モデルを持ってしきい値ばらつきが発生していることになる。よって、これらのしきい値分散をモデル化し、このモデルに従って、シミュレーションを行ってみる。

さらに、現在の LSI の素子ばらつきの問題として LSI の製造プロセスが進化するにつれて素子ばらつきの与える影響が大きくなっているという問題がある。この影響が本提案解析手法のような、素子ばらつきを利用した耐タンパーLSI 解析にとってどのように影響するかも追加して検討する。

しきい値ばらつきの分散のモデルと、しきい値ばらつきがプロセスの進化するにつれどのようなモデルを取って影響を及ぼすのかトランジスタモデルを用いて解析してみる。

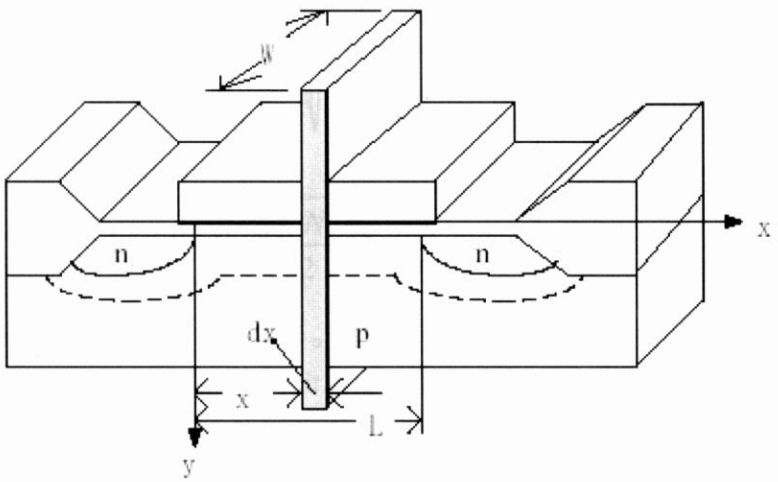

図 5.4 MOSFET の模式図

図 5.4 に示すような MOSFET において、トランジスタのしきい値電圧は、

$$V_{th} = V_{fb} + 2\phi_B + \frac{\sqrt{4\varepsilon_{Si} q N_A \phi_B}}{C_{ox}}$$

と表せる。V_{fb} はフェルミ電位、ϕ_B はシリコンのフラットバンド電圧、ε_{Si} はシリコンの誘電率、q は素電荷、N_A は不純物濃度、C_{ox} は酸化膜容量である[27]。

空乏層内の不純物原子数$N = N_A LWW_d$はポアソン分布に沿って発生するが、正規分布で十分近似できる。このときの標準偏差は$\sigma N = \sqrt{N}$になる。空乏層幅は$W_d = \sqrt{2\varepsilon_{Si}\phi_B / qN_A}$より、

$$\begin{aligned}\sigma V_{th} &= \frac{\partial V_{th}}{\partial N_A}\sigma N_A \\ &= \frac{1}{C_{ox}}\sqrt{\frac{\varepsilon_{Si} q \phi_B}{N_A}}\sqrt{\frac{N_A}{LWW}} \\ &= \frac{1}{C_{ox}}\sqrt[4]{\frac{\varepsilon_{Si} q^3 N_A \phi_B}{2}}\frac{1}{\sqrt{LW}}\end{aligned}$$

が導かれる。これにより、しきい値電圧の分布も正規分布にほぼ一致することがわかる。

ここで、不純物濃度を一定に保ったままスケーリングを行い、Lを$\frac{1}{k}L$、Wを$\frac{1}{k}W$に置き換えるとする。このとき、C_{ox}はゲート酸化膜にもスケーリング則を適用したことにより、容量がk倍に増加し、kC_{ox}に置き換わることとなる。このとき、スケーリング則を受けたδ_{Vth}は、

$$\begin{aligned}\sigma V_{th} &\to \frac{1}{kC_{ox}}\sqrt[4]{\frac{\varepsilon_{Si} q^3 N_A \phi_B}{2}}\frac{1}{\sqrt{\frac{1}{k}L\frac{1}{k}W}} \\ &= \frac{1}{C_{ox}}\sqrt[4]{\frac{\varepsilon_{Si} q^3 N_A \phi_B}{2}}\frac{1}{\sqrt{LW}} \quad \text{(一定)}\end{aligned}$$

となり、分散は一定となることがわかる。

このモデルに従ってLSIの製造プロセスが進化しても、しきい値ばらつきの絶対値が一定であるというモデルを取って本解析シミュレーションを行った。このとき与えたしきい値ばらつきの絶対値としては分散値5mV～50mVの10パターンを取った。

結果を図5.5に示す。図から判断する限り、しきい値ばらつきの絶対値の値と解析必要サンプル数の関連はあまり見られなかった。また、350nmプロセス、180nmプロセスでは緩やかであるが、ばらつき絶対値が大きいほど解析必要サンプル数は大きくなり、解析が若干難しくなることが示された。しかし、90nm以下の90nm、45nmプロセスにおいては解析必要サンプル数が若干ではあるが小さくなって容易となることが示された（詳細な値、傾向は図5.6、表5.2を確認）。

これらの結果から90nm以下におけるディープサブマイクロン環境においては若干ではあるがしきい値ばらつきの増大が耐タンパーLSIにおいては耐タンパー性の劣化につながり、十分留意すべき点となりうるということが示された。

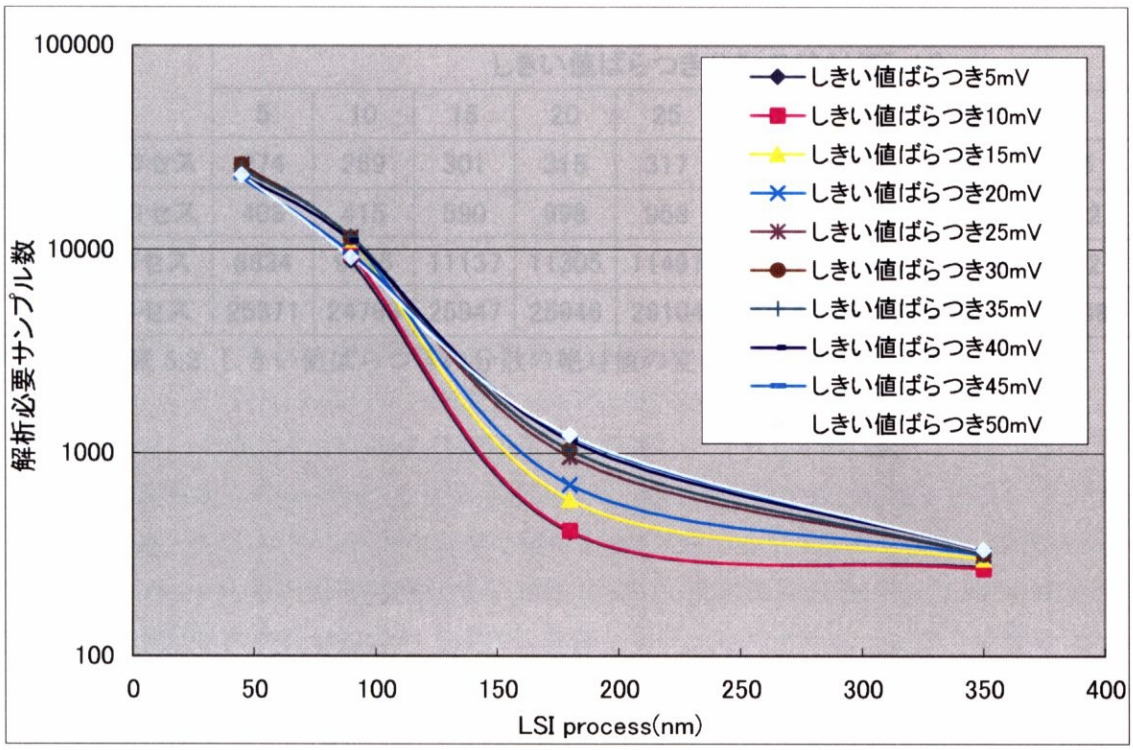

図 5.5 LSI の製造プロセスの進化と解析必要サンプル数の変化

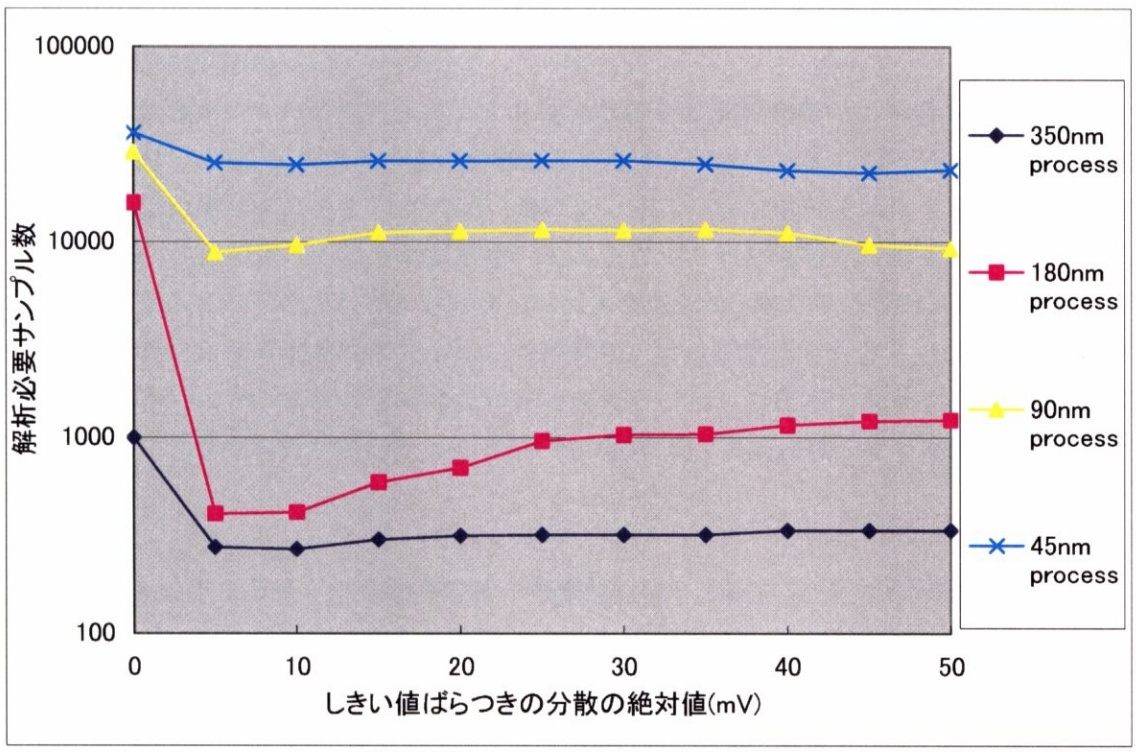

図 5.6 しきい値ばらつきの分散の絶対値と解析必要サンプル数

	しきい値ばらつき分散の絶対値[mV]									
	5	10	15	20	25	30	25	40	45	50
350nm プロセス	274	269	301	315	317	317	317	335	335	335
180nm プロセス	408	415	590	698	958	1033	1040	1156	1212	1226
90nm プロセス	8834	9575	11137	11305	11491	11417	11574	11028	9602	9204
45nm プロセス	25371	24768	25947	25946	26104	26114	24869	23154	22508	23238

表 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

第6章

結論

本論文では以下のような結論が得られた。

1. LSIレイアウトに対しての差分電磁界解析シミュレータの提案

LSIのレイアウトに対して、内部配線からの放射電磁波を計算することにより観測アンテナを設置した場合のアンテナ空間電位差を計算し、これらの値を用いて差分解析する差分電磁界解析シミュレータを提案した。また、この手法をDES暗号のLSIレイアウトに対して適応し、シミュレーションの有効性を示した。このシミュレーション手法はDES暗号だけでなく一般の暗号処理を行うLSIにおいて汎用的に応用でき、LSIの製造前の差分電磁界解析耐性評価について非常に有益となると考えられる。また、攻撃対象となる注目配線からの放射電磁波削減に着目することによる差分電磁界解析への対策手法を提案した。注目配線の縮小と、注目配線のインバータ分割の2つの対策手法を提案し、シミュレーションにより有効性を確認した。

2. 素子ばらつきによる耐タンパーLSIの劣化の説明と、素子ばらつきの影響を利用した電磁界解析の提案

固有電力消費アーキテクチャのような電力解析や電磁界解析への耐性を持つ耐タンパーLSIに対しても、素子ばらつきの影響が新たなサイドチャネルになりうることを示した。特に、しきい値ばらつきが駆動波形の俊敏さ、さらに放射電磁波に与える影響を考慮することで、注目周波数の成分の値を用いることにより差分電磁界解析を適応させる手法を提案した。この手法をシミュレーションにより実際のDESのWDDL相当のLSIレイアウトに行い、暗号鍵解析を行った。この結果、暗号鍵解析を行うことができ、現実的な環境において十分解析できることが示された。また、本提案手法は一般の差分電力解析と同様に、差分解析が適応できるAES等の他の暗号方式に対しても同様に応用可能である。

3. 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の提案

シミュレーションにより有効性が確かめられた素子ばらつきを考慮した電磁界解析に対しての対策手法を複数提案した。どの手法も攻撃に用いられる注目配線から放射される放射電磁波の符号相関値を小さくすることに着目して提案している。注目配線の配線長を縮小する方式、注目配線をインバータ分割する方式、乱数を使って符号の割り当て

をランダム化する方式、3線式データエンコード方式を用いる方式の4つを提案し、シミュレーションにより有効性を確認した。

4. デバイスのスケーリングにおける、素子ばらつきを考慮した電磁界解析への脆弱性の変化に対してのシミュレーション

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の脆弱性の関連を調べた。同一のLSIレイアウトをそのままスケーリングしたものに対しての解析では注目配線からの電流の絶対値が減っていることが影響して、最新の製造プロセスほど攻撃が難しくなるという結果が得られた。さらに、しきい値ばらつきモデルをMOSFETモデルを用いてモデル化すると、不純物濃度が一定ではスケーリングを行ってもしきい値ばらつきの分散の絶対値は一定であるという結果が得られた。この結果に従い、さらに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を行った。また、しきい値ばらつきの程度と解析に対しての脆弱性の関連はあまり見られなかった。

以上の結果により、これからの耐タンパーLSIの設計では、特に固有電力消費アーキテクチャを用いた耐タンパーLSIにおいて、素子ばらつきの影響に十分注意して設計を行う必要があることが示された。また、耐タンパーデバイスにおいてサイドチャネル耐性がますます求められる今後の状況では、本論文の解析シミュレーション手法やその結果はこれからの耐タンパーLSIの設計に対して非常に有益になるであろうと考えられる。

参考文献

[1]J. Kelsey, B. Schneier, D. Wagner, C. Hall, "Side Channel Cryptanalysis of Product Ciphers", ESORICS '98 Proceedings, pp.97-110, September 1998.

[2]H.Handschuh, P.Paillier, J.Stern, " Probing Attacks on Tamper-Resistant Devices ", CHES99

[3]P. Kocher, J. Jaffe, B. Jun, "Introduction to Differential Power Analysis and Related Attacks", 1998,
available at http://www.cryptography.com/dpa/technical/index.html

[4]P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", Advances in Cryptology: Proceedings of CRYPTO '96,
Springer-Verlag, 1996, pp.104-113.

[5]J.-F. Dhem, F. Koeune, P.-A. Leroux, P. Mestre, J.-J. Quisquater, J.-L. Willems, "A Practical Implementation of the Timing Attack", UCL Report, 1998, CG1998-1,
available at http://www.dice.ucl.ac.be/crypto/techreports.html

[6]D. Boneh, R. A. DeMillo, and R. J. Lipton, "A New Breed of Crypto Attack on "Tamperproof" Tokens Cracks Even the Strongest RSA Code", 1996

[7]K. Gandolfi, C. Mourtel, F. Olivier, "Electromagnetic analysis: concrete results", CHES2001, pp.251-261, 13-16 May 2001.

[8]T. S. Messerges, E. A. Dabbish, R. H. Sloan, "Power Analysis Attacks of Modular Exponentiation in Smartcards", Proceedings of CHES '99, Springer-Verlag, 1999, pp.144-157.

[9]S. B. Ors, F. Gurkaynak, E. Oswald and B. Preneel. "Power-Analysis Attack on an ASIC AES implementation", Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) 2004

[10]"Data Encryption Standard (DES)", Federal Information Processing Standard (FIPS), Publication 46-3, 1999

[11]Wolff, E. A., "Antenna Analysis" 2nd Edition, Artech House Inc., Norwood, 1988

[12]「情報処理装置等電波障害自主規制協議会」http://www.vcci.or.jp/

[13]M. Bucci, R, Luzzi, M.Guglielmo, "A Countermeasure against Differential Power Analysis based on Random Delay Insertion", IEEE International Symposium on Circuits and Systems (ISCAS) 2005

[14]Eric Sprunk, "Clock Frequency Modulation for Secure Microprocessors", US Patent 5404402

[15] Shengqi Yang, Wayne Wolf, Vijaykrishnan Narayanan, Dimitrios Serpanos, and Yuan Xie, "Power-attack resistant cryptosystem design: a dynamic voltage and frequency switching approach," in Proceedings, DATE '05 Designers Forum, 2005.

[16]M.Akkar and C.Giraud, "An Implementation of DES and AES, Secure against Some Attacks", CHES'01

[17]Elena Trichina, "Combinational Logic Design for AES SubByte Transformation on Masked Data" 2003

[18]N. Pramstaller, E K. Giirkaynak, S. Haem, H. Kaeslin, N. Felber, and W. Fichtner, "Towards an AES Crypto-chip Resistant to Differential Power Analysis", Proceedings of ESCIRC 2004 Leuven, Belgium, Sept 21-23, 2004

[19]市川 哲也、鈴木 大輔、佐伯 稔、「データマスクを利用したDPA対策に対する攻撃」、電子情報通信学会情報セキュリティ研究会(ISEC) 2004

[20] 清水秀夫、「マスク論理素子を使ったサイドチャネル攻撃対策」、電子情報通信学会情報セキュリティ研究会(ISEC) 2004

[21]K. Tiri and I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation," Proceedings of DATE2004, pp.246-251, 2004.

[22] Kris Tiri, David D. Hwang, Alireza Hodjat, Bo-Cheng Lai, Shenglin Yang, Patrick Schaumont, and Ingrid Verbauwhede, "A Side-Channel Leakage Free Coprocessor IC in 0.18μm CMOS for Embedded AES-based Cryptographic and Biometric Processing", 42nd Design Automation Conference (DAC 2005), pp. 222-227, June 2005.

[23] Kris Tiri、 Moonmoon Akmal、 and Ingrid Verbauwhede、 "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards"、 28th European Solid-State Circuits Conference (ESSCIRC 2002)、 pp。 403-406、 September 2002.

[24] Adi Shamir, "Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies", CHES 2000

[25]Kris Tiri, and Ingrid Verbauwhede, "Design Method for Constant Power Consumption of Differential Logic Circuits", Design, Automation and Test in Europe Conference (DATE 2005), pp. 628-633, March 2005

[26] N. Li, M. Ikeda, and K. Asada, "Analysis of Low Noise ThreePhase Asynchronous Data Transmission", in Proc. of European Solid-State Circuits Conference (ESSCIRC), pp. 479 -- 482, Sep. 2005.

[27]N. Arora "MOSFET Models for VLSI Circuit Simulation", Springer-Verlag, Wien, 1993

[28]池野信一、小山謙二、「現代暗号理論」、電子情報通信学会、1986

[29]岡本龍明、山本博資著、「現代暗号」、産業図書、1997

本研究に関する発表

山内裕史、池田誠、浅田邦博、”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”、電子情報通信学会情報セキュリティ研究会（ISEC）、2006年3月

謝辞

本研究を進めるに当たり、日頃から熱心なご指導をして頂き、また適切な助言を頂きました浅田邦博教授、池田誠助教授に深く感謝いたします。

浅田池田研究室において研究活動をともにした助手の鄭若丹彡氏、佐々木昌浩氏、大学院生の皆さん、卒論生の方々、技官の鈴木真一さんに心から感謝致します。