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

本章では差分電磁界解析の対策手法としての固有電力消費アーキテクチャによる耐タンパーLSIを紹介した上で、これら固有電力消費アーキテクチャにおいても微細素子のパラメータばらつきを考慮することで耐タンパー性が劣化し、電磁界解析を受けるということを提案し、シミュレーションによりその有効性を示す。

3.1 固有電力消費アーキテクチャによる耐タンパーLSI

電力解析・電磁界解析では 2.1.1 項で説明したように、CMOS 回路における消費電力が遷移確率と関連があることを利用して行われている。よって対策手法としては、消費電力と遷移確率の関連をなくす手法が考えられる。これらの手法としてソフトウェア・ハードウェアの両方の手法が数々提案されているが、本論文ではこの中でもハードウェアでの手法における固有電力消費アーキテクチャに着目して解説を行う。固有電力消費アーキテクチャでは消費電力波形が固有周期波形になるような回路アーキテクチャを取り、内部状態と消費電力波形の相関を無くしている。回路の概要は 3.1.1 項から 3.1.3 項において説明する。

なお、ソフトウェア、ハードウェア両面における他の手法の解説を行う。

○ ソフトウェア手法

- ランダム遅延の挿入

  処理にランダムな遅延を挿入することで、消費電力波形の時間成分にランダム変動を与える。しかしながら、時間軸でのランダム変動しか与えていないので、消費電力波形と暗号処理の相関は残っており、根本的な対策にならない。

- 暗号処理アルゴリズムのランダム組み替え

  ある1つの暗号処理を行うに当たり、同一暗号処理に対して複数の処理アルゴリズムを用意しておき、これらをランダムに組み替えて処理を行う。しかしながら、この場合も特定の1つの暗号アルゴリズムについては同様に電力解析が行えるので、サンプル数を増やして解析を行ったり、アルゴリズムでの分類を行った後に同様の解析を行うなどをすることで電力解析が行えるとされる。

- 頻繁な鍵更新

  暗号鍵の更新を頻繁に行うことで対策を防ぐ。この効果は獲得できるサンプル数が小さくなることで、解析が難しくなるという効果と、たとえ解析ができたとしても鍵更新が頻繁に行われるので解析できた暗号鍵がすぐに使えなくなってしまうという効果の両面が期待できる。しかしながら電力解析自体の根本的な対策手法とは言えない。

- 無駄な電力消費の追加

  演算器の稼働状態をソフトウェア的に監視し、稼働率が低下しているときには無駄な演算を加える。しかしながら、秘密情報に関わる演算は通常通り行われているので、サンプル数を増加させれば解析が行われてしまう。さらに、チップ直上にアンテナをおいた電磁界解析では秘密情報に関連のある演算部分に観測アンテナを配置することで通常通り解析が行われる可能性もある。

○ ハードウェア手法

- 電源線へのノイズ挿入

  電源線へノイズ信号を挿入することで、消費電力波形と内部状態の相関を少なくする。しかしながら、サンプル数を増やして解析を行うことで電力解析を行うことが可能である。また、暗号回路自体は通常通り駆動しているのでチップ直上に観測アンテナをおいた電磁界解析には弱いと考えられる。

- ランダム遅延の挿入[13]

  処理にランダムな遅延を挿入することで、消費電力波形の時間成分にランダム変動を与える。しかしながら、時間軸での変動しか与えていないので、消費電力波形と暗号処理の相関は残っており、根本的な対策にならない。

- 電源電圧や駆動周波数のランダム変動[14][15]

  回路を駆動させる電源電圧を駆動周波数をランダム変動させることで消費電力波形と内部状態の相関を少なくする。しかしながら、この手法では相関が少なくなるだけで、電力解析の根本対策にはならない。さらに、今後の製造プロセスの進化などにより、電源電圧が低下していくなどの影響を考慮するとこの手法が新しいプロセスでも安定して駆動できるか不確実である。

- 演算途中のデータを乱数でマスキングを行う方式

  暗号処理の途中のデータにマスキングを施し、内部で処理する内容を変化させることによって、電力解析を困難としている。マスキングにより、演算中の中間データが乱数でマスキングされることで、マスクがわからない限り中間データを予測できなくなる。マスキングの手法としては使用している平文や暗号文全体に乱数でマスキングをかけて暗号アルゴリズム自体をマスキングに合わせて修正する手法[16][17][18]や、論理ゲート自体に乱数でマスキングを施し、内部信号の状態をランダム化する方式[19][20]などが挙げられる。

3.1.1 Wave Dynamic Differential Logic

Kris Tiri らによって提案された LSI の回路の内部論理によって電力消費変動が発生しにくくした回路方式である WDDL（Wave Dynamic Differential Logic）という回路方式を紹介する[21][22]。

WDDL は 2 線式回路の構成を取っており、スタンダードセルを組み合わせて相補的なゲートの組を構成することにより、新しいスタンダードセルを作っている（図 3.1）。これにより、消費電力のばらつきを小さくしている。さらに、レイアウトを相補的に構成するなど工夫することで、相補となる 2 線の配線容量の均一化も図っており（図 3.2）、'0'配線と'1'配線の両配線に流れる駆動電流も同一となるように図っている。

さらに、WDDL では 1 サイクルごとにプリチャージを行い、プリチャージ信号が 1 の時は AND、OR ゲートに与えられる入力は全て 0 になり、プリチャージ期間となる。プリチャージ信号が 0 となり、論理評価される場合には通常の相補入力が与えられることとなる。これにより、入力ゲートの遷移も完全に相補となっている。

WDDL は、実際のスタンダードセル構成に比べ、消費電力の変動幅は 50 分の 1 以下にとどまり（図 3.3）、この回路で実際に LSI チップに実装された AES 回路に対しての電力解析攻撃の耐性も実証されており、攻撃の成功例は報告されていない。

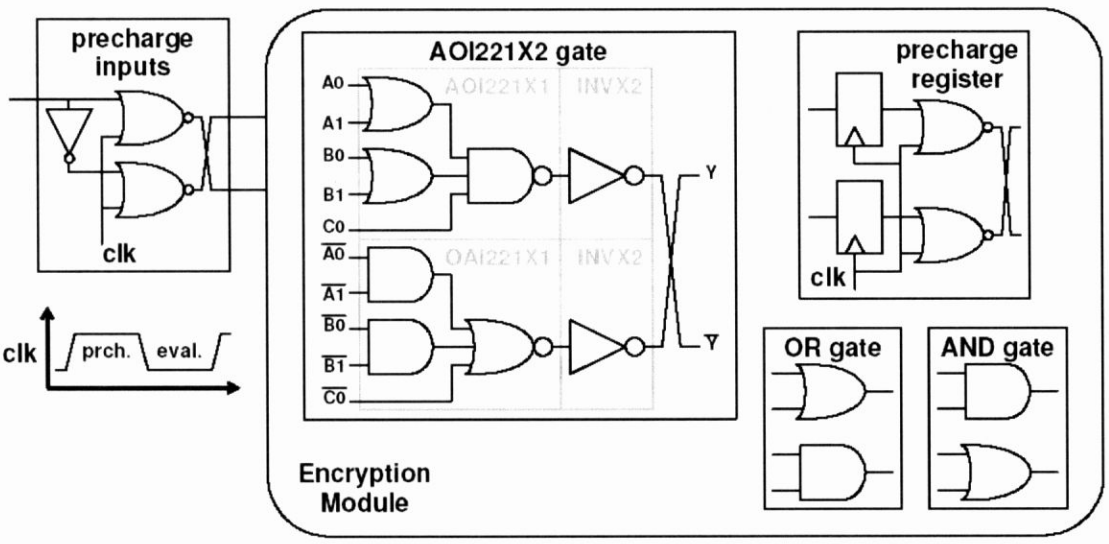

図 3.1 WDDL 回路の構成

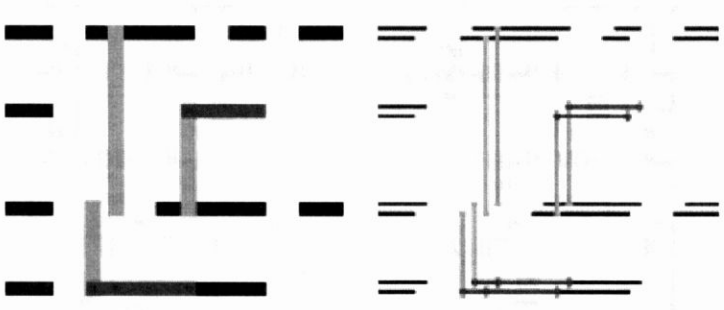

図 3.2 正論理と負論理の配線容量の均等化

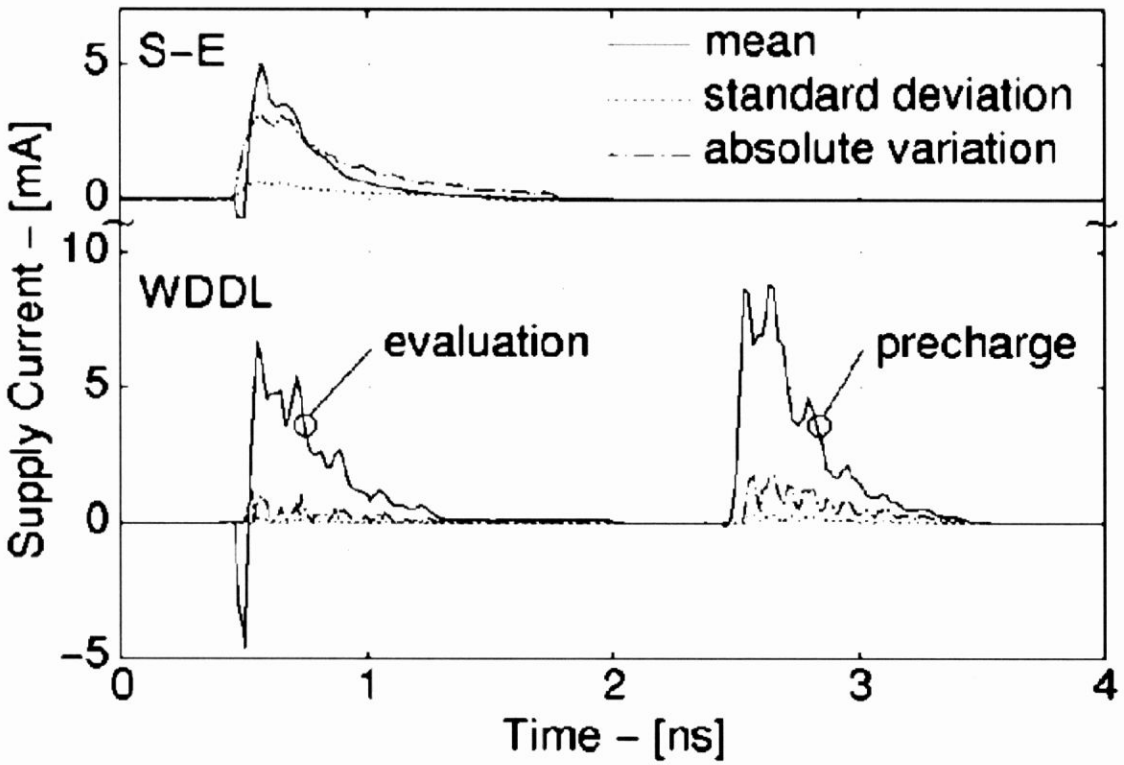

図 3.3 標準 1 線式 CMOS 回路と WDDL 回路における電流波形の比較

3.1.2 Sense Amplifier Based Logic

SABL(Sense Amplifier Based Logic)回路はセンスアンプと nMOS のプルダウンネットワークを組み合わせたダイナミック回路（図 3.4）である[23]。相補入出力を取る 2 線式回路の構成を取り、precharge→evaluation の動作を取ることにより消費電力変動が小さくなっている。さらに、この回路ではトランジスタ M1 が常に on になっているので論理出力時に全ての出力が discharge され、演算ごとの消費電力の変動を小さくしている。

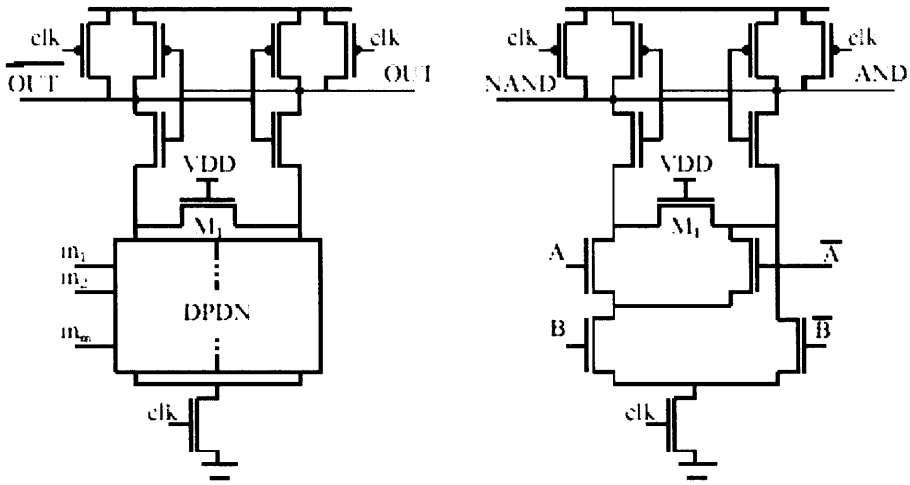

図 3.4 SABL 回路の構成

左：基本回路　右：SABL 回路の AND-NAND ゲート

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

暗号回路にキャパシタを接続して電源線から見た回路の消費電力の固有化を図る回路方式を説明する[24]。図 3.5 に示すように、2 つのコンデンサと 4 つのスイッチを用い、交互に充電と回路への電流供給を繰り返すことで電源線から見える回路の消費電力を隠蔽している。この回路では以下のサイクルで回路を動作させる。

① No.1 コンデンサを外部電力から切断
② No.1 コンデンサをチップに接続
③ No.2 コンデンサをチップから切断
④ No.2 コンデンサを外部パワーに接続

この方法では、チップは常にひとつのコンデンサによって電力供給されているが、外部電力は内部のチップに直接接続しない。また、電力分析防御を強めるため、チップから切断し（③）、外部パワーに接続（④）する前に外部より観察不可能な方法でコンデンサを放電する要素を追加している。

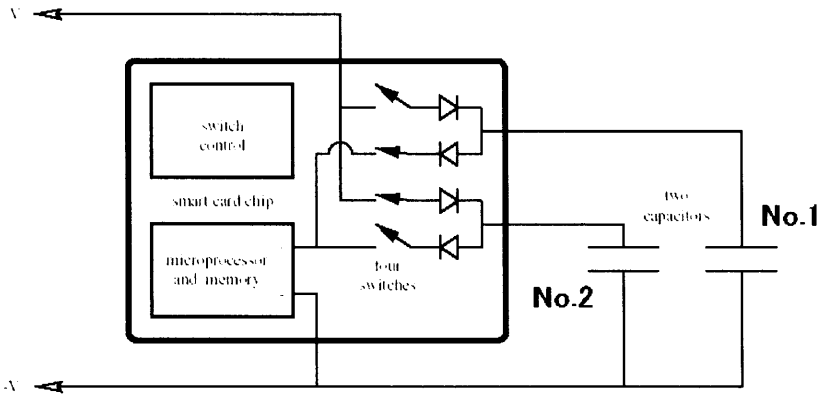

図 3.5 回路の外部に 2 つのキャパシタを接続した回路方式

装置の電源線から観測できる電流波形は図 3.6 のような周期波形となる。

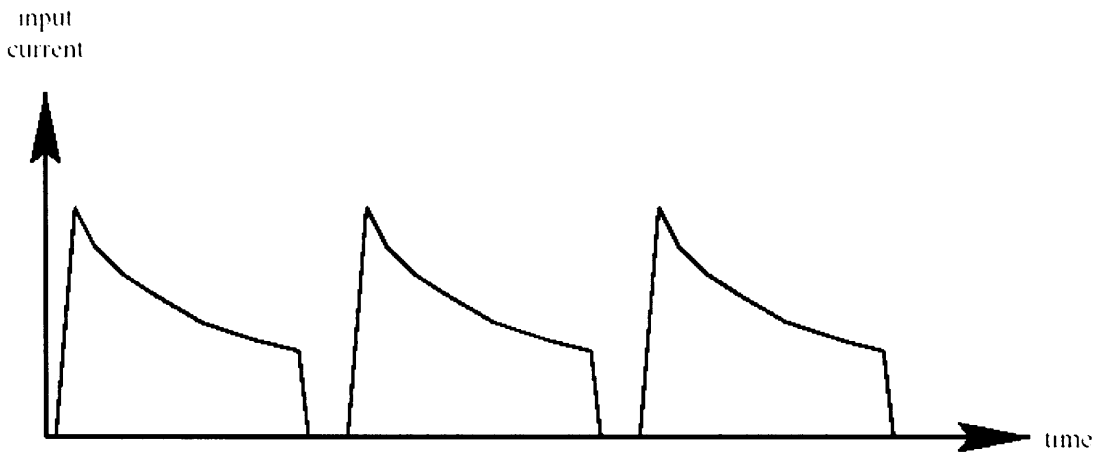

図 3.6 キャパシタを用いた回路方式の動作波形

この手法ではキャパシタを利用しているので電圧降下が起こり、今後のプロセスの電源電圧の低下の影響などを考えても動作に不安性がある。さらに、暗号回路自体は通常通り演算を行っているので、プローブや裁断機を利用して、直接回路が消費する電流を測定された場合には対処できず、さらに暗号回路直上に観測アンテナをおいた電磁界解析にも弱いと考えられる。

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

3.1 項で説明した、WDDL のような消費電力波形の固有化を図った耐タンパーLSI 回路方式では、回路が完全に相補的に構成されることになると秘密情報が関連している演算内容と消費電力の相関は全く生じないこととなり、電力解析が不可能となると考えられる。

ここで、回路のアンバランスを引き起こす要因として、新たに素子ばらつきについて着目する。素子ばらつきとしては不純物ばらつきやレイアウトのばらつきなど様々あるが、本研究では特に、トランジスタのしきい値のばらつきについて考えることとする。

図 3.7 を用いて WDDL 回路を例にして、トランジスタのしきい値ばらつきが耐タンパーLSI に対して与える影響を説明する。図 3.7 は WDDL のセル間をつなぐ 2 線式相補配線をイメージした図である。WDDL の 2 線式相補配線は、論理'0'を示す'0'配線と論理'1'を示す'1'配線から構成されている。ここで、2 配線を駆動するトランジスタのしきい値にばらつきが生じたとする。本説明では'0'配線を駆動するトランジスタが'1'配線を駆動するトランジスタよりもしきい値が下がっていると仮定する。この場合、しきい値が低下した'0'配線は駆動時に立ち上がり、立ち下がり波形が急になる。これにより、電流の持つ高周波成分が高くなることになる。また、しきい値が増加した'1'配線は立ち上がり、立ち下がり波形が鈍ることにより、低周波成分が増加することになる。この違いから、理想的には生じないとされる WDDL の相補的 2 線式配線に流れる電流においても、しきい値ばらつきを考慮することでアンバランスが生じていると考えられる。すなわち、しきい値ばらつきにより'0'論理と'1'論理の間で生じるアンバランスが消費電力や電磁放射に影響を与えることになる。なお、これら同様の影響は WDDL だけでなく他の固有電力消費アーキテクチャにおいても同様に起こっていると考えられる。

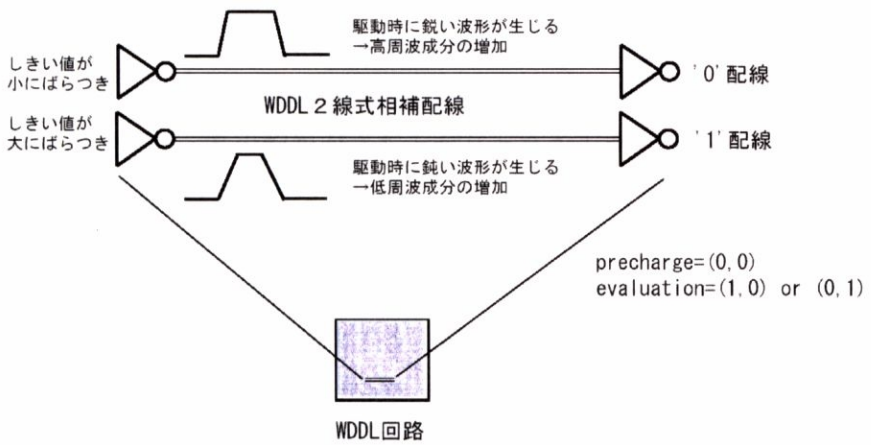

図 3.7 しきい値ばらつきが駆動波形に与える影響

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

3.2項で説明した、しきい値ばらつきに由来するアンバランスと差分解析手法を用いて2線式相補配線においてどちらの配線が変動したか区別できないか検討し、耐タンパーLSIの解析を行うことにする。

まず、トランジスタのしきい値ばらつきを利用して電力解析を行う場合を考える。しかしながら、この場合ではしきい値ばらつきが与える影響は駆動電流の俊敏さにとどまるので、全体としての消費電力は殆ど一定である。よって、しきい値ばらつきが影響を与える程度の瞬時電力を観測することは非常に困難だと考えられ、さらに測定時の容量の影響などを考えてもこれを再現するのは非常に難しいと考えられる。

ここで、配線から発生する電磁波を観測して区別を行う電磁界解析を検討する。この場合は消費電力の観測と違い、配線から発生された電磁波を直接観測することができ、解析に有利な生に近い情報が得られると考えられる。さらに、信号波形の俊敏さが電磁波の周波数成分の違いに現れることで、観測した電磁波を処理し、周波数成分を調べることにより両配線の区別が出来る可能性が高まると考えられる。また、レイアウト情報を把握している場合は攻撃対象となる配線から強い影響が得られる位置で観測することができるので、電力解析と比べても、より信号成分が多い情報が得られると考えられる。

さらに、電磁界解析では2線式相補配線の配線レイアウトのずれの影響が観測される電磁波の強度や位相差に微妙にではあるが現れるので、ばらつきの影響だけでなく、電力解析では観測するのが非常に難しいとされるレイアウトのアンバランスが与える影響も検出できる可能性もある。

以上の考察から、WDDLにおける2線式配線から放射される電磁波を利用して秘密情報を解析する方法を提案する（図3.8）。WDDLにおいては2線式配線を用いていてデータ'0'の伝送に(1,0)、データ'1'の伝送に(0,1)を用いている。さらに、プリチャージ状態を(0,0)と定義している。よって、evaluation→prechargeの1サイクルにおいて2本の配線は、一方の配線が0のまま、もう一方の配線が立ち上がりと立ち下がり（evaluation→precharge）を行う、といった組み合わせになっている。ここで、双方を駆動するトランジスタにばらつきが生じていると考えると電流波形の立ち上がり、立ち下がりの俊敏さにも違いが出る。この違いは放射される電磁波にも影響を与え、しきい値が小さくばらつくほど高周波成分が大きくなると考えられるので、発生する電磁波を処理し、注目する周波数成分の強度に着目することにより、攻撃対象とする配線の論理の区別を行う手がかりとする。この場合、攻撃に使う配線としては差分電力解析における選択関数の値となっている配線を用いており、解析手法としては、観測アンテナから得られた測定値から特定周波数成分のみを取り出し、これを差分電力解析的解析手法で解析し、秘密情報を推測するという手法を用いる。

この解析における前提条件としては、

- LSI の近傍にアンテナをおいて電磁波を観測できる。
- 使用している暗号アルゴリズムが既知である。
- 入出力されるメッセージが取得できる。
- 鍵を固定しながら多くの暗号処理を行える。
- LSI のレイアウト情報を把握している。(レイアウト情報が無くても解析が可能であるが、アンテナ位置を最適化できるので有った方が望ましい。)

が挙げられる。この解析手法は WDDL 以外の固有電力消費アーキテクチャにおいても同様に適応できると考えられる。

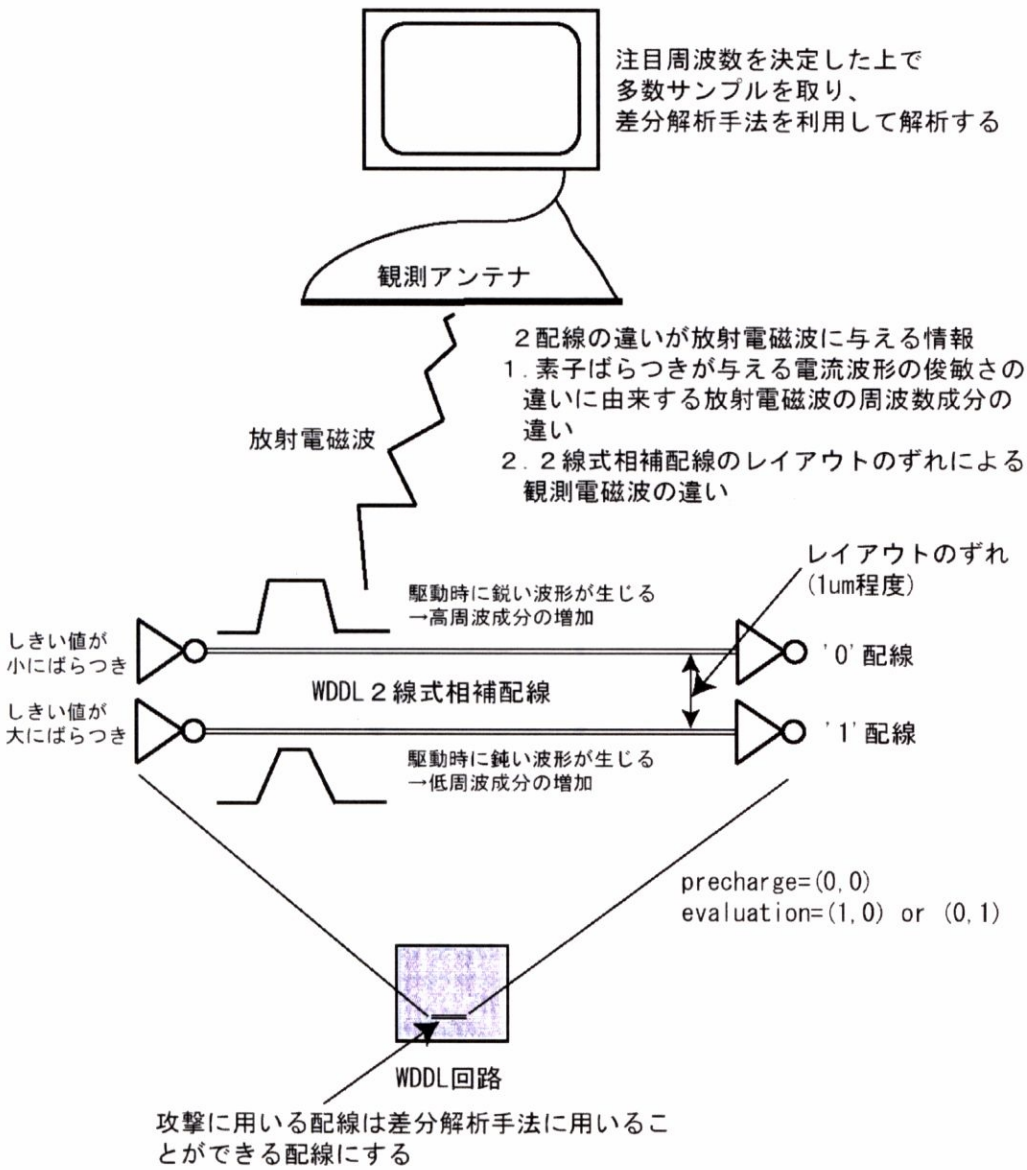

図 3.8 素子ばらつきを考慮した電磁界解析手法の概要

3.4 WDDL 回路に対しての解析シミュレーション

提案する解析手法の妥当性を検証するために、実際の DES 暗号の LSI レイアウトを元に電磁波を用いた解析シミュレーションを行った。図 3.9 が流れ図である。

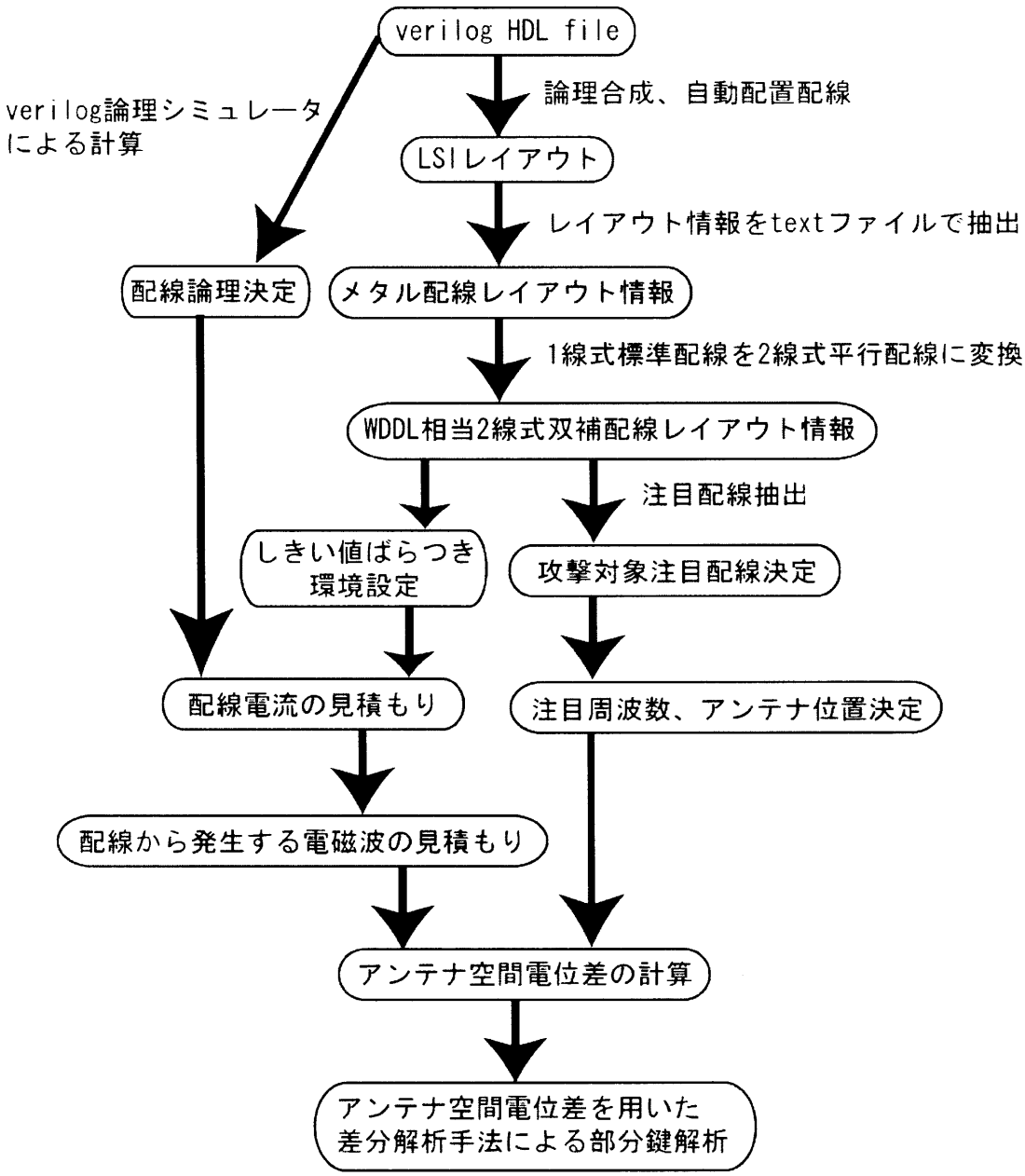

図 3.9 素子ばらつきを考慮した電磁界解析シミュレーション手順