2.3.9　アンテナ空間電位差の値を用いた差分解析

取得したアンテナ空間電位差を用いて差分電力解析的解析手法を適用した。シミュレーションで得られた多数のサンプル値を分類することにより、差分値を得る。解析に用いる差分値は以下の式を用いて求める。

$$Difference = \frac{1}{N_1}\Sigma V_1 - \frac{1}{N_0}\Sigma V_0$$

N_0：注目配線の論理が'0'である測定数
N_1：注目配線の論理が'1'である測定数
V_0：アンテナ空間電位差のうち注目配線の論理が'0'である場合
V_1：アンテナ空間電位差のうち注目配線の論理が'1'である場合

この式に従って、本シミュレーションにおいては 50000 個のサンプル集合のうち、予測鍵に応じて計算した注目配線の論理が'0'であるか'1'であるかで場合分けし、その各々の平均値の差分をとって差分値を求めている。

2.4　シミュレーション結果

2.3 で説明した手順に従って、DES の LSI レイアウトに対してシミュレーションを行い、部分鍵解析を行った結果を示す。

2.4.1　DES の LSI レイアウトへの解析結果

本シミュレーションでは部分鍵の 6bit 値（0～63）を予測することになるが、あらかじめ正しい鍵を 41 とした。

図 2.23 と図 2.24、は鍵の予測値と相関値の関係を示した図である。相関値は正と負両方の値を取っているが、鍵の予測としては相関値の絶対値が最も大きい予測値が正しい鍵だと推測できる。サンプル数が 1000 と 50000 の時の結果を示しているが、サンプル数 1000 の場合では、key=41 ではない鍵で相関値が最大となっており正しい推測値が得られていない。しかし、サンプル数 50000 の時は正しい鍵のピーク値が他の鍵と比べても鋭く現れていることが確認できた。また、key=41 以外の鍵の複数において鋭いピークが見られる鍵があるが、これらの鍵は真の鍵の値ではないが選択関数の論理と相関が有る鍵であり、その相関値が現れている結果だと考えられる。

図 2.25 は相関値の値をサンプル数を変化させるにつれてプロットしたものを示したものである。この図では相関値のトレースは真の鍵の値（key=41）のトレースと、他の 63 個の

鍵のうち、もっとも大きいものと小さいもののトレースの3種のみ表示している。ここで、真の鍵のトレースを見るとサンプル数が増えるに従ってほぼ一定値に近づいていくことがわかる。この一定値が、注目配線の相関値を示していると判断できる。また、誤った鍵のトレースは、サンプル数が増えるに従って、小さくなっていくことも確認できる。これは、アンテナ空間電位差のサンプルが注目配線の論理と無関係に分類されていることで、差分値が統計的に小さくなる方向に向かっていくということを示している。実際に図 2.24 から判断する限りサンプル数が5000もあれば解析は可能であるということがシミュレーションから示された。

以上のような解析を第 24bit 配線だけでなく、他の注目配線にも行い、配線長の長い配線を優先的に選んで、同様に解析を行うことで全体の 64bit 暗号鍵も求めることができた。

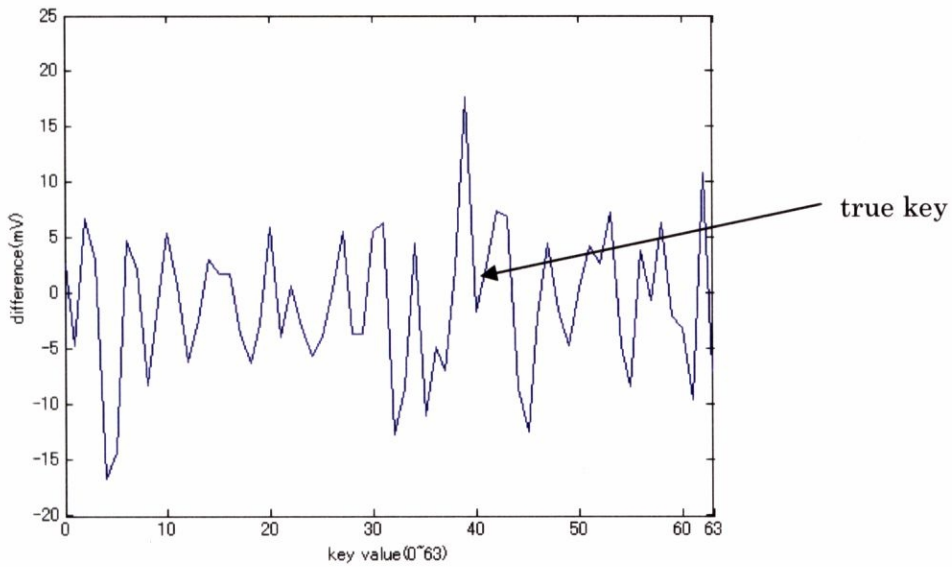

図 2.23 サンプル数 1000 の場合の予測鍵と相関値

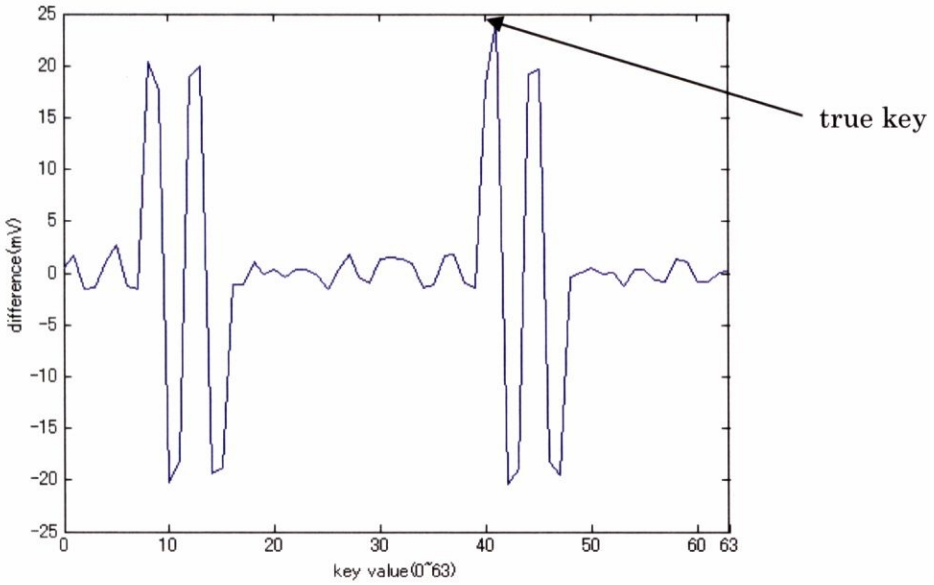

図 2.24 サンプル数 50000 の場合の予測鍵と相関値

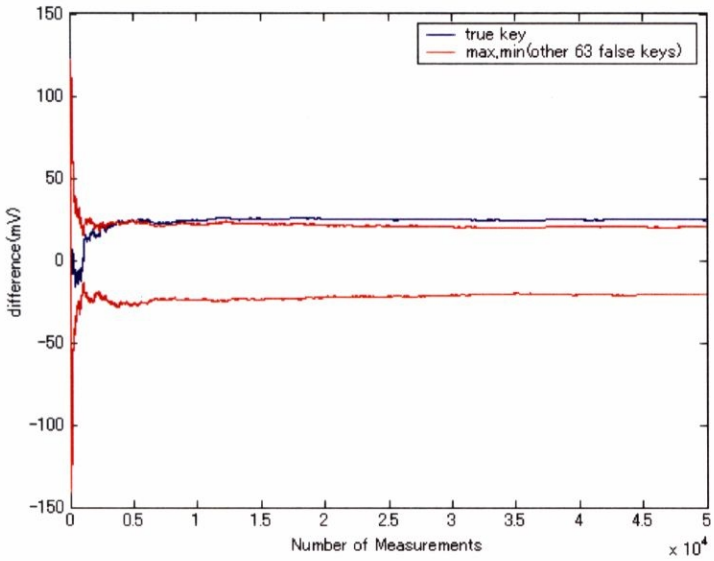

図 2.25 サンプル数の変化と相関値の推移

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

2.4.1 項における解析シミュレーションは観測アンテナの高さを 1mm で固定しているが、実際の電磁界解析にはアンテナ配置やアンテナ高さなどを様々に変化させた観測アンテナ

環境での解析が考えられるのでこれらを変化させたシミュレーションを行う。

LSI チップからの観測アンテナ高さを 1mm から 1m へと変化させて解析シミュレーションを行った。このときサンプル数は 50000 が最大であるので 50000 サンプルでも解析が行えない場合は解析が不可能であるとしている。また、アンテナ配置はその都度アンテナ位置を注目配線からの空間電位差が最大となるように配置し直した場合とチップの中央に配置した場合の 2 通りを取った。

解析結果を図 2.26 に示す。アンテナの高さが大きくなるにつれて解析に必要なサンプル数が大きくなるはずであるが、チップ中央配置の場合は逆に解析必要サンプル数が下がって解析しやすくなっている。これは、観測アンテナの高さが大きくなるにつれてアンテナの配置が解析に有利な位置に近づいていったからではないかと考えられる。また、レイアウト情報が無く、チップ中央に観測アンテナを配置した場合でも解析に必要なサンプル数は大きくなるが、十分解析できることがわかった。

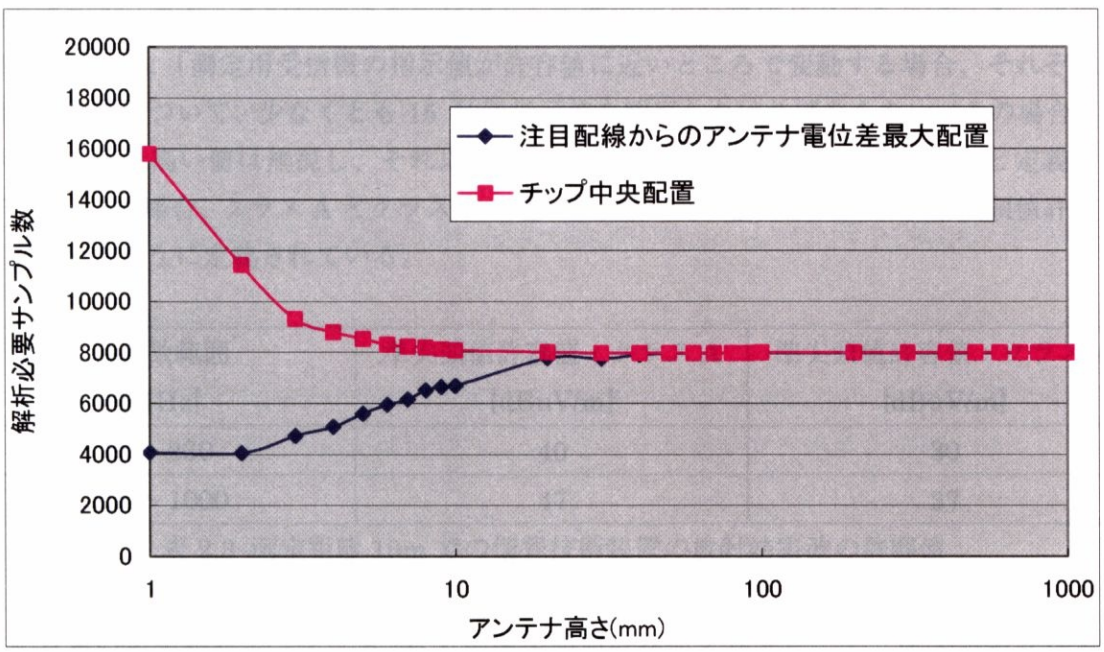

図 2.26 観測アンテナの高さと解析必要サンプル数

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

これまでのシミュレーションは解析空間上に生じる空中雑音の影響を考慮せずに解析を行っている。しかし、実際には測定環境にもよるが、わずかであっても空中雑音が発生しているはずであり、観測点の高さが大きくなるにつれて、その影響は無視できなくなり、解析が難しくなると考えられる。これらの影響を考えるために、空中雑音を含めて、アンテナ高さを変化させた場合も同様にシミュレーションした。

参考にする雑音値として、日本のVCCI（情報処理装置等電波障害自主規制協議会）規格[12]の値を参考にする。実際には、電磁雑音（EMI）に関する規格は複雑で、地域や国により違っていて数多くの組織が自ら電磁雑音に関することを規制している。しかし、最初に電磁雑音に関する規格を規制したのは国際無線障害特別委員会（CISPR：International Special Committee on Radio Interference）であり、現在、各国の規格は殆どCISPRのものに従っている。日本のVCCI規格も同様にCISPR規格に準拠しており、VCCI規格中の、「情報技術装置からの妨害波の許容値と測定法」という日本国内規格は、国際電気標準会議（IEC）/国際無線障害特別委員会（CISPR）により勧告された国際規格CISPR22第三版（1997-11）「情報技術装置(ITE)からの妨害波の許容値と測定法」に準拠するものでありこれを説明する。

「情報技術装置(ITE)からの妨害波の許容値と測定法」では、電磁雑音を発生する情報技術装置として、クラスAとクラスBの2種類を定義する。ここで、クラスA情報技術装置は、工業用の機器のほとんどを定義している。クラスBの装置は一般的な住宅で使われる機器である。また、放射妨害波の許容値として準尖頭値許容値が定められている。準尖頭値許容値とは、「測定用受信機の指示値が許容値に近いところで変動する場合、それぞれの測定周波数について、少なくとも15秒間指示値を観察しなければならない。その場合、瞬時の孤立した高い値は無視し、それ以外の最も高い指示値を記録した観測値」と定義されている。この場合、クラスAとクラスBの各々において測定距離10mでの準尖頭値許容値は表2.3のように定義されている。

周波数範囲 [MHz]	準尖頭値許容値・クラスA [dBuV/m]	準尖頭値許容値・クラスA [dBuV/m]
30～230	40	30
230～1000	47	37

表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

これらの値を参考に、クラスAでの準尖頭値許容値を参考にして、準尖頭値許容値が40dBuV/m=1uV/cm程度となる程度の電磁雑音が空中雑音として発生しているとし、その空中雑音は0.3uV/cmの正規分布で発生させることで実現している。観測アンテナの位置は注目配線からのアンテナ空間電位差が最大となるように最適化した配置と、とLSIチップ中心配置の両方を取る。

解析の結果を図2.27に示す。解析の結果から雑音の影響は2cm程から大きくなることが確認でき、10cm近くなると50000サンプルでは解析が不可能になることが示された。しかしながら、アンテナの高さが1cm以下の場合ではでは雑音の影響をほとんど受けることなく解析可能であるといえる。また、アンテナ中央配置の結果をみても最適配置よりは結果は劣るが、雑音を考慮しても十分に解析を行うことが可能であることがわかった。

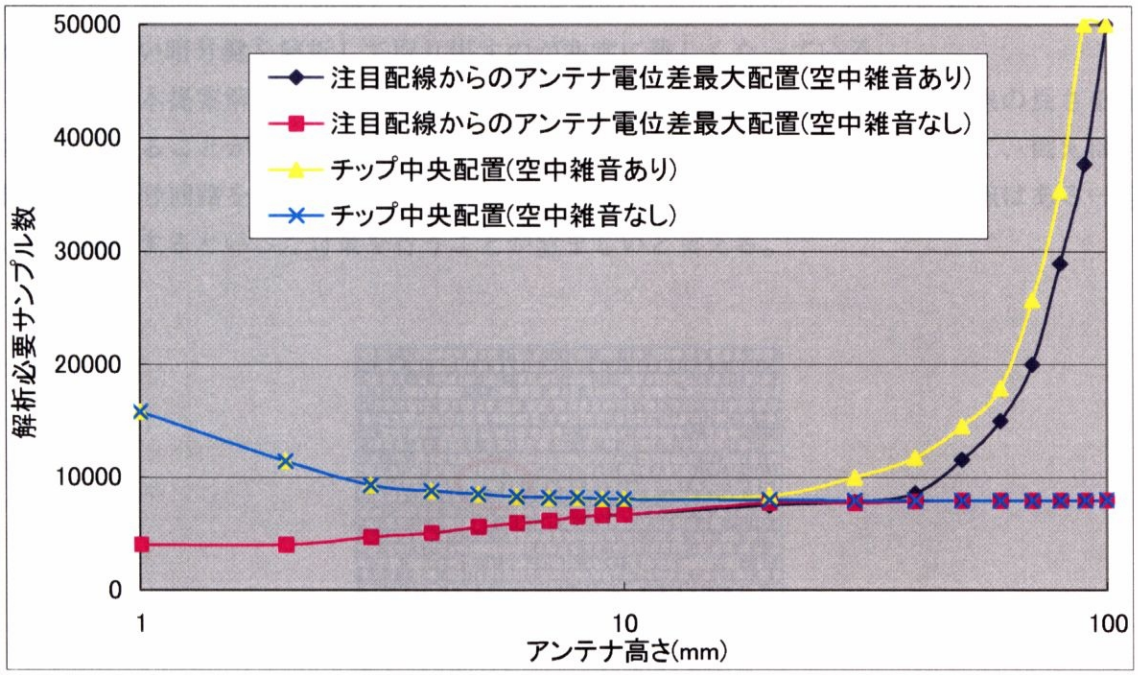

図 2.27 空中雑音を考慮した場合のアンテナの高さと解析必要サンプル数

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

差分電磁界解析の対策手法を注目配線からの放射電磁波削減に注目して複数提案する。これらの対策手法を差分電磁界解析シミュレーションを用いて有効性を確認する。

2.5.1 注目配線の配線長縮小による対策手法

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、解析を行った DES 暗号の 32 本の注目配線のうち最も短い第 27bit 配線（図 2.28：85.4um）に注目し、差分電磁界解析シミュレーションを行った。

図 2.29 と図 2.30 はサンプル数を 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 2.31 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自体は相関値に現

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正しい暗号鍵を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。

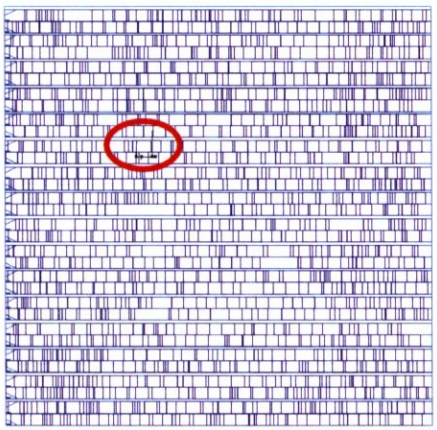

図 2.28 第 27bit 注目配線（85.4um）

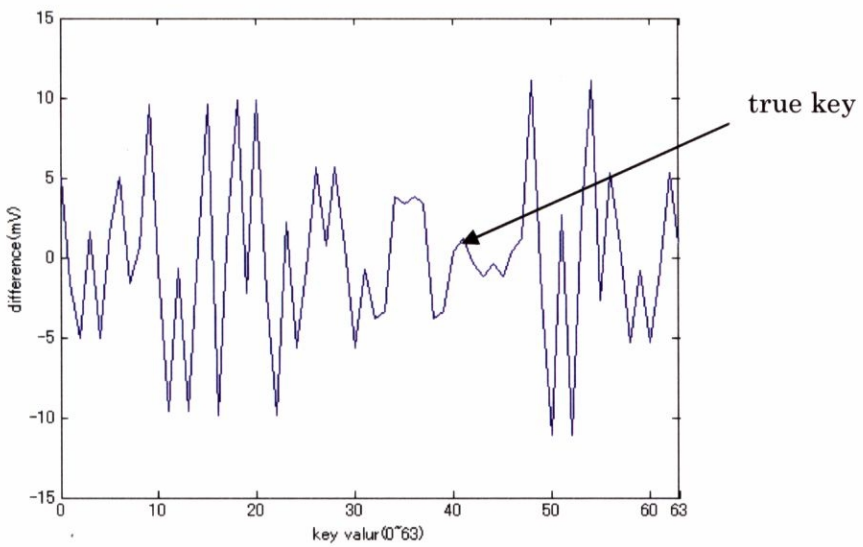

図 2.29 サンプル数 1000 の場合の予測鍵と相関値

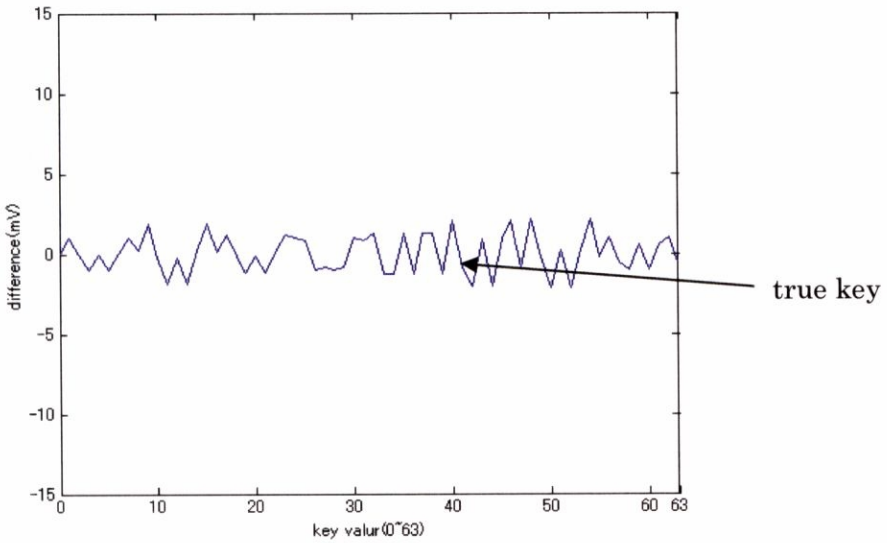

図 2.30 サンプル数 50000 の場合の予測鍵と相関値

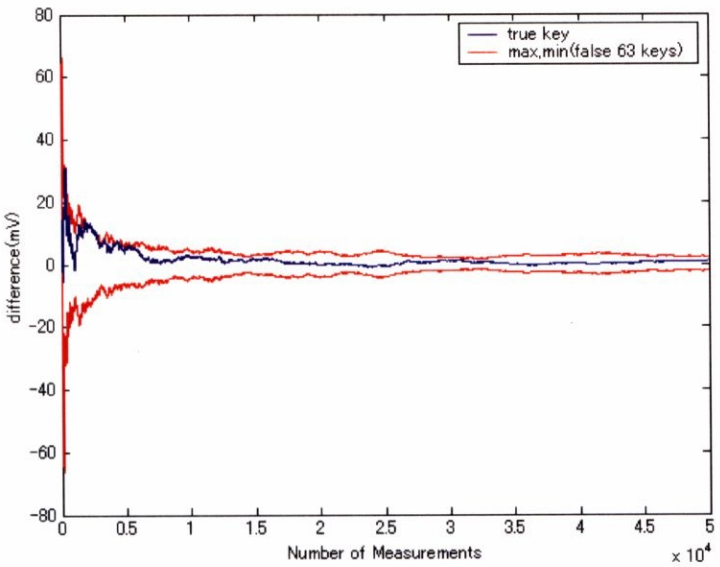

図 2.31 サンプル数の変化と相関値の推移

2.5.2 注目配線のインバータ分割による対策手法

図 2.32 に示すように攻撃に用いられる注目配線にインバータを挟んで分割することによって符号'0'と'1'の電磁波の信号差を小さくできる。これにより、配線長が短い配線の集合となり、'0'と'1'の両符号で電磁波が発生するので両符号の信号差が小さくなる。この手法もシミュレーションを行い有効性を確かめる。インバータ分割を第 24bit 配線の注目配線（821.68um）に行い、相関電位差の推移と解析必要サンプル数の変化を調べた。ここでは

分割数を 1(分割なし)～10 と変化させ、ほぼ等長分割になるように分割した。また、分割数を変化させるにつれて、その各々の場合の解析必要サンプル数を調べた。アンテナ配置は 2 配線からの相関信号が最大になるような最適配置をとっている。

図 2.33 に注目配線の分割数とその配線からの相関電位差の変化を示す。シミュレーションの結果、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傾向にある。図 2.34 に解析必要サンプル数の変化を示すが、相関電位差の減少につれて解析に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、相関電位差が 2mV 以下になる程度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原理的にも簡単であり、自動合成にも適応しやすい対策手法であるといえる。

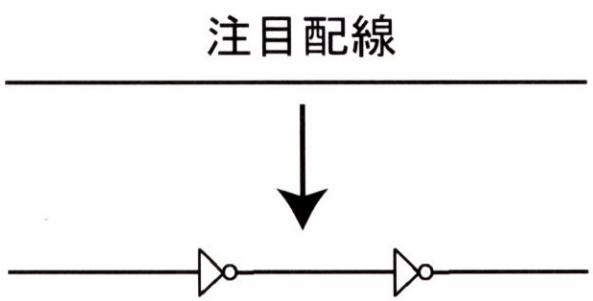

図 2.32 注目配線のインバータ分割

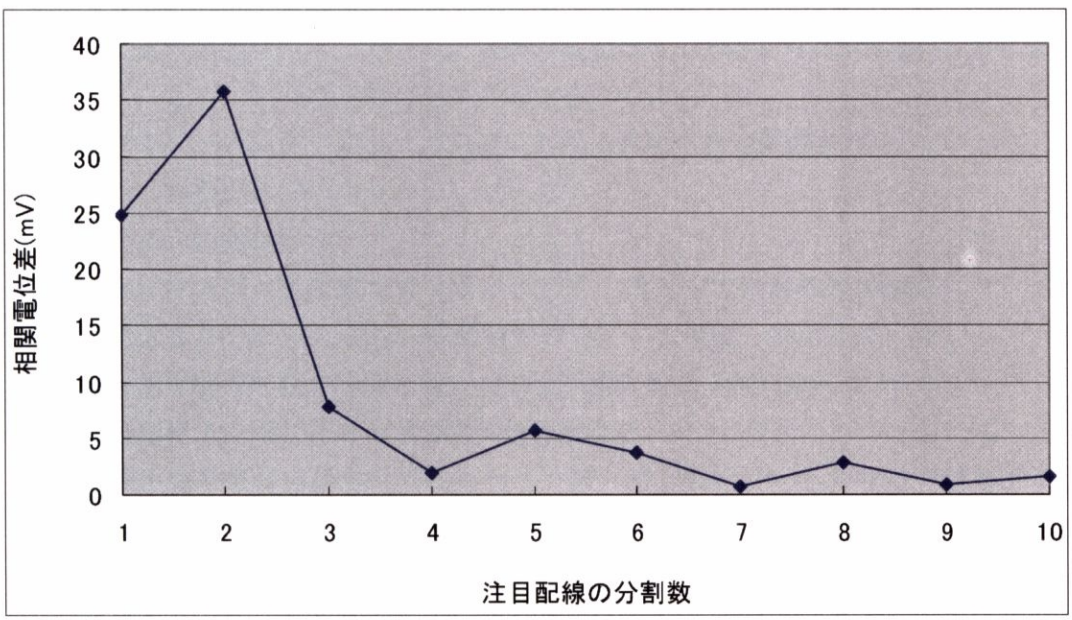

図 2.33 注目配線の分割数の変化と相関電位差の変化

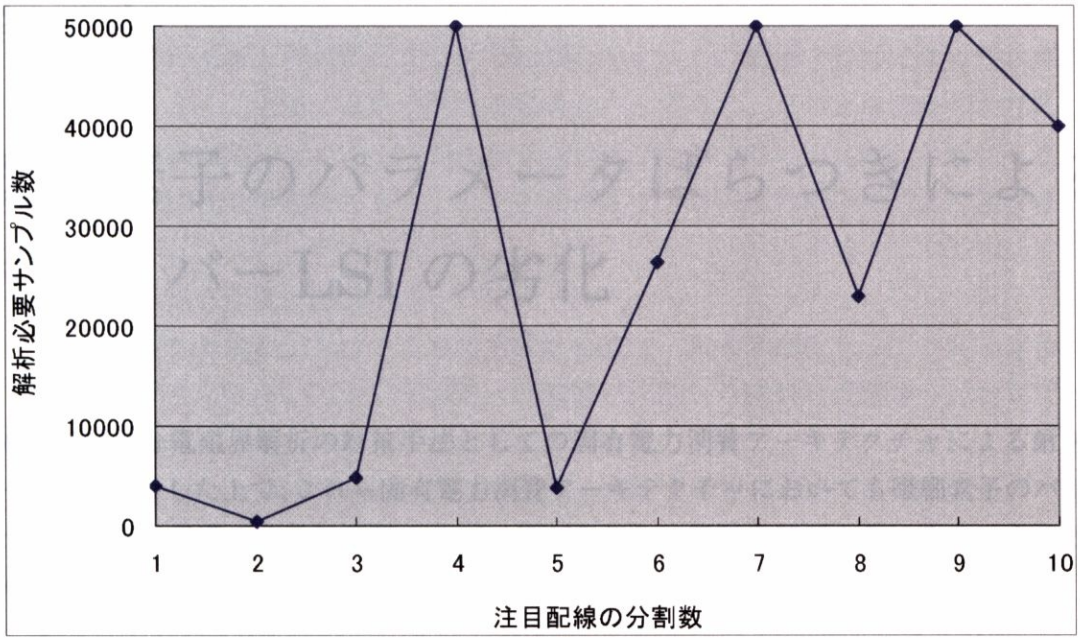

図 2.34 注目配線の分割数の変化と解析必要サンプル数の変化