3.4.1 WDDL相当のDES暗号のLSIレイアウトの生成

WDDL相当のDESのLSIレイアウト生成手法は、まず2.3.3項と同様のDES暗号のアルゴリズムをハードウェア記述言語 verilog で記述し、論理合成・配置配線を経ることでLSIレイアウトを生成した(図3.10)。このときのプロセスも350nmルールに従っている。なお、この回路は100MHzで駆動させている。最新のプロセスでのシミュレーションにおいてはまた、第5章で行っている。

このようにして生成したレイアウト情報をasciiファイルで取り出し、この中から配線情報のみを抽出した。

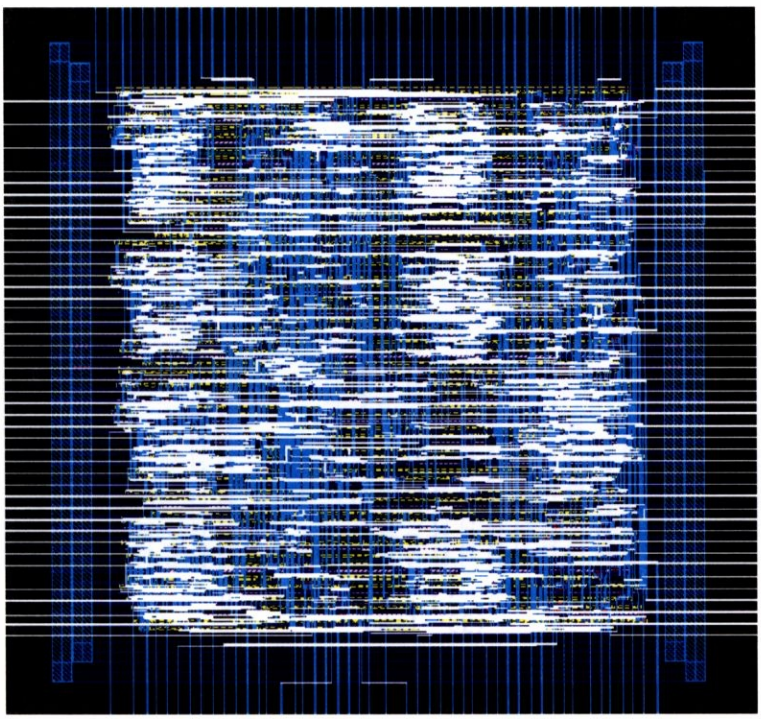

図3.10 解析対象としたWDDL相当DES回路(840um×840um)

実際に合成したLSIレイアウトは1線式標準CMOS回路である。これを攻撃対象とするWDDL相当の2線式双補配線に変換するために、生成したLSIレイアウトの各配線について1本の配線を平行した2本の2線式双補配線へ置き換える変換処理を行った(図 3.11)。なお、実際のWDDL回路配線生成手法においてもこれと同様の配線生成手法を用いている[25]。

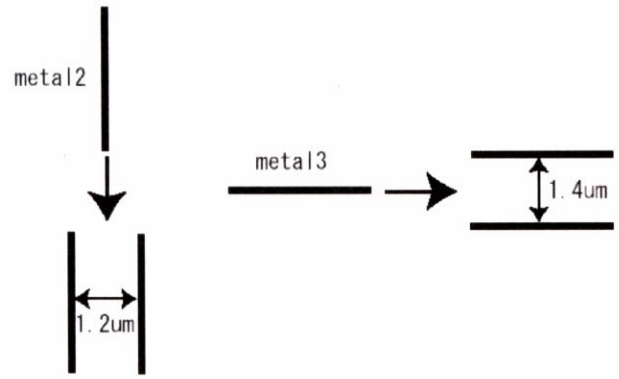

図 3.11　1 線式配線の 2 線式相補配線への変換

攻撃対象となる配線を設定する。WDDL 回路においても、DES アルゴリズムの R レジスタからの出力の 32bit バスを注目配線とした。

32 本ある注目配線（図 3.12）の中で、最も配線長が長く電磁放射も大きくなると考えられる第 24bit 配線（図 3.13：964.5um）について着目し、攻撃対象とした。

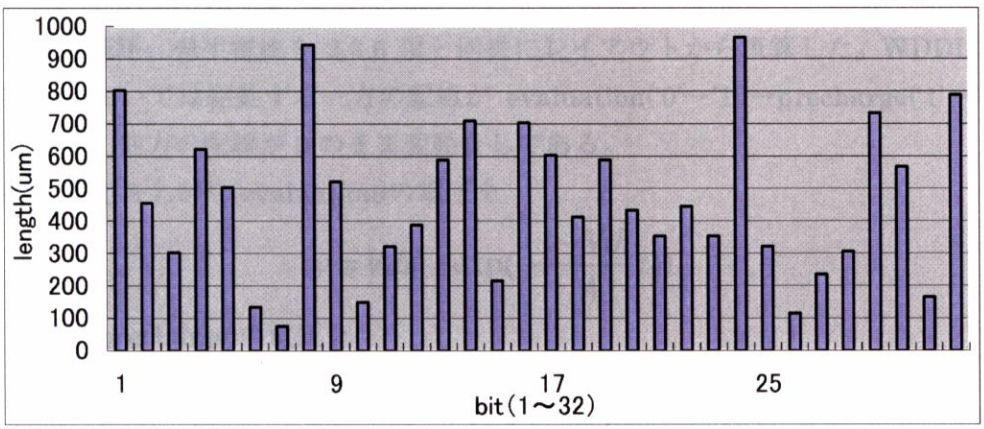

図 3.12 注目配線の長さの比較

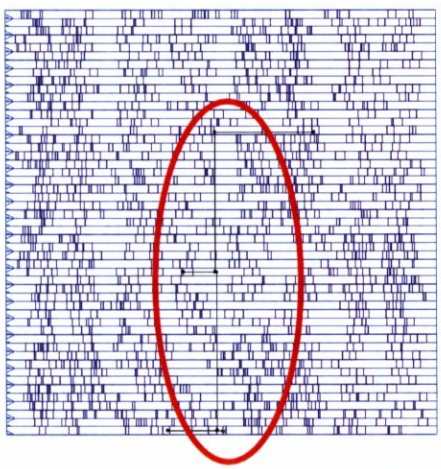

図 3.13 攻撃対象とした第 24bit 配線(964.5um)

素子ばらつきの設定として、配線の駆動力にばらつきを持たせる。多様なばらつき状況において解析手法の妥当性を検証するために様々なプロセスばらつきを考慮してばらつきを発生させた。例えば、プロセスばらつき 1%においては、注目配線のうち、一方の配線を -0.5%ばらつき、もう一方の配線を 0.5%ばらつきで設定し 2 配線間でばらつきを 1.0%としており、その他の配線は 1.0%の標準偏差の正規分布でランダム発生させている。このようなプロセスばらつきを 0%～10.0%の 0.1%刻みで発生させ、多様なばらつき環境の各々においてシミュレーションを実行した。

内部配線の論理値についても verilog 論理シミュレータから全ての配線の論理を導くことで、50000 パターンの論理パターンを作った。これらの平文・暗号文の値、配線論理の値を解析シミュレーションに用いている。

3.4.2 2 線式相補配線における各配線からの配線電流の見積もり

配線の信号電圧、発生電流を 2.3.6 項と同様にレイアウトから概算した。WDDL の 2 線式相補配線においては駆動する一方の配線が evaluation('0'→'1')→precharge('1'→'0')の電圧変動を経て、他方の配線が 0 のまま変動なしである。

駆動配線で立ち上がり(evaluation)の電圧を

$$v = Vdd \cdot (\exp(-\frac{1-Vth}{A}t))$$

立ち下がり(precharge)の電圧を

$$v = Vdd \cdot (1-\exp(-\frac{1-Vth}{A}t))$$

で概算した。(Vdd:電源電圧(3.3V)、Vth:しきい値(ばらつきなしで 0.7V)、A:時定数(120ps))さらに、配線容量を C として i=C*dV/dt から電流値を求めた。配線容量 C はレイアウトから得られた配線長に 0.17fF/um を乗じて求めている。この i に高速フーリエ変換(FFT)をかけることで電流の周波数成分を求めた。

3.4.3 注目周波数の決定と観測アンテナ位置の最適化

本解析では、しきい値ばらつきの影響が放射電磁波の周波数成分の差に表れることを利用している。よって、解析に利用するに当たって最適な解析周波数を決定する必要がある。

ここで、注目する周波数を 100MHz から 5GHz まで変化させてアンテナ電位差に表れるばらつき相関電位差信号の変化を調べた。ここでは、注目配線において 1%のばらつきが与えるアンテナ相関電位差('0'配線と'1'配線単独配線からの各々の電位差の差分値)を求めて

いる。観測状況としてアンテナ長 1mm、アンテナ高さ 1mm で固定している（図 3.14）。さらに、アンテナ位置はアンテナ空間電位差が最大になるように周波数を変えるごとに最適化している。解析結果を図 3.15 に示すが、基本周波数である 100MHz で最も大きい電位差が得られた。

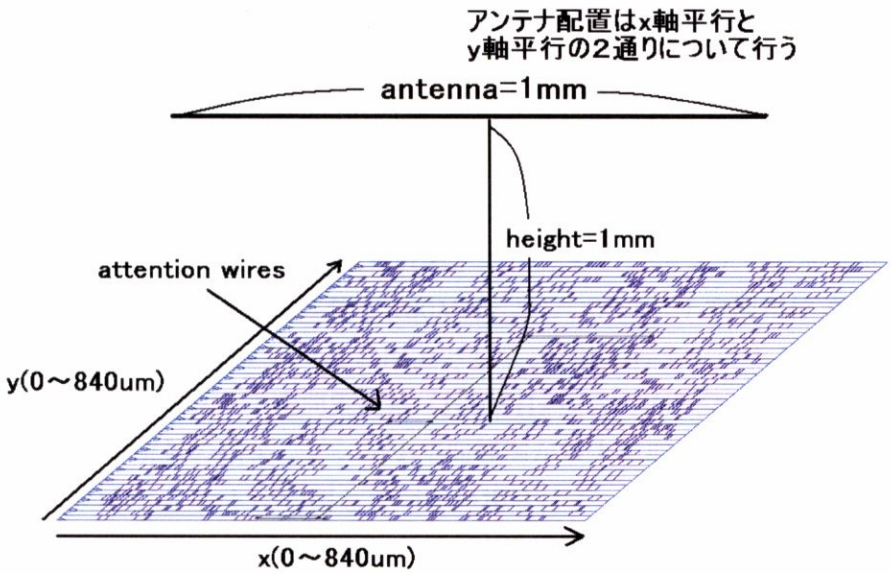

図 3.14 観測アンテナ配置

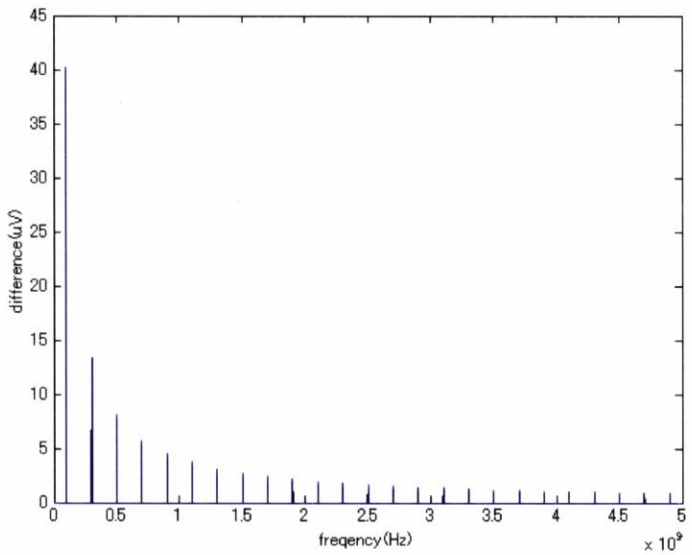

図 3.15 注目周波数と相関信号

回路の基本周波数である 100MHz で相関信号が最大となった理由を説明する。WDDL 回路では駆動側の配線は evaluation→precharge のサイクルを行い、このサイクル周期が

100MHz となる。よって配線電流の周期も 100MHz となっている。ここで、しきい値ばらつきが起こりしきい値が低下したとすると、電圧波形の立ち上がり・立ち下がりが鋭くなり、これに伴い、電流波形のピーク値が大きくなる結果となる。これは、基本周波数である 100MHz 成分が増えることに直結する。これにより基本周波数の 100MHz で相関信号が最大となったことが説明できる。

さらに、チップ上に観測アンテナを配置するにあたり、もっとも効率のよい配置にする必要がある。本シミュレーションでも 2.3.8 項と同様に、注目配線のレイアウトが判明している場合はアンテナ配置の最適化を行った。このときに用いるアンテナ長は 1mm、チップ表面からの高さは 1mm で固定とした。チップのレイアウトが判明している場合は注目配線からの電磁波の影響が最も大きく受け、観測アンテナ空間電位差が最大となる点に観測アンテナを配置するのが望ましいと考えられる。このために、アンテナ空間電位差を示すマップを作った。この場合、注目周波数を 100MHz とし、アンテナ空間電位差の 100MHz 成分のみを取っている。また、アンテナの配置として、x 軸平行アンテナと y 軸平行アンテナの両方をとっている。アンテナ空間電位差（100MHz 成分のみ）マップを図 3.16 と図 3.17 に示す。このような解析の結果、アンテナ空間観測が最大に取れる点で解析した。

なお、チップのレイアウトが判明していない場合はチップの中央直上において解析を行っている。

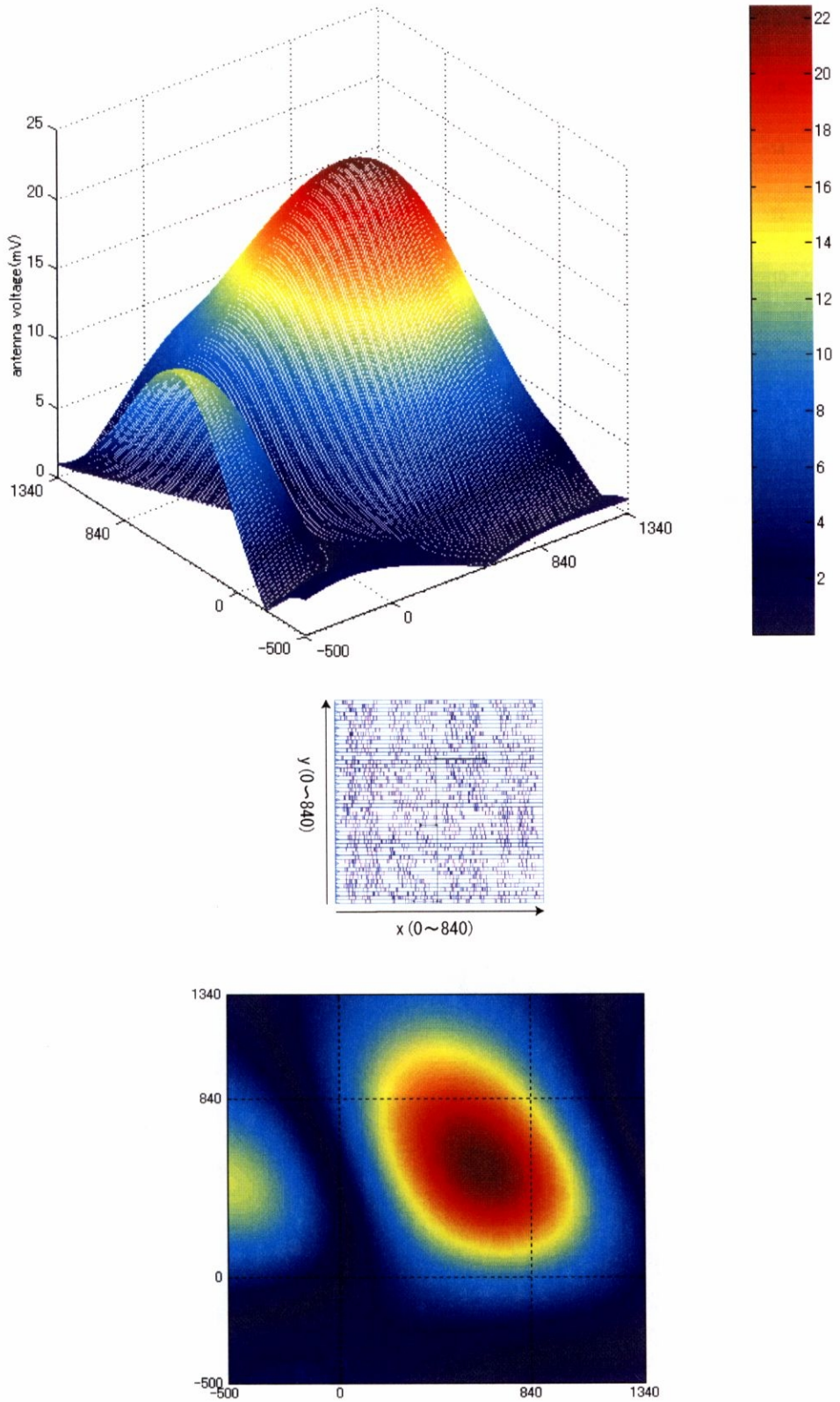

図 3.16 x 軸平行にアンテナを配置した場合のアンテナ空間電位差マップ（100MHz 成分）

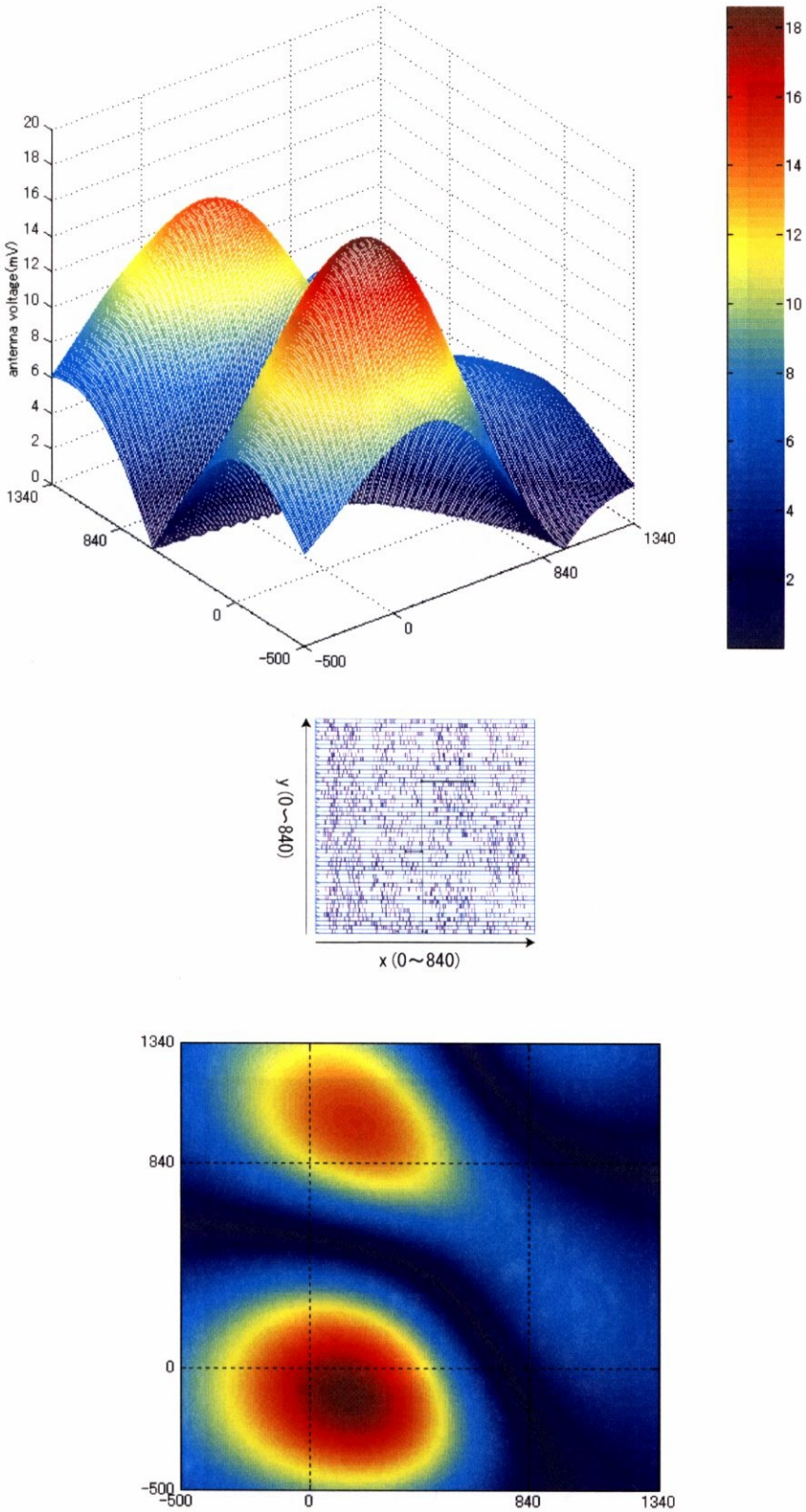

図 3.17 y 軸平行にアンテナを配置した場合のアンテナ空間電位差マップ（100MHz 成分）

また、参考として注目配線からの電界・磁界強度（100MHz 成分）は図 3.18、図 3.19 のようになっている。

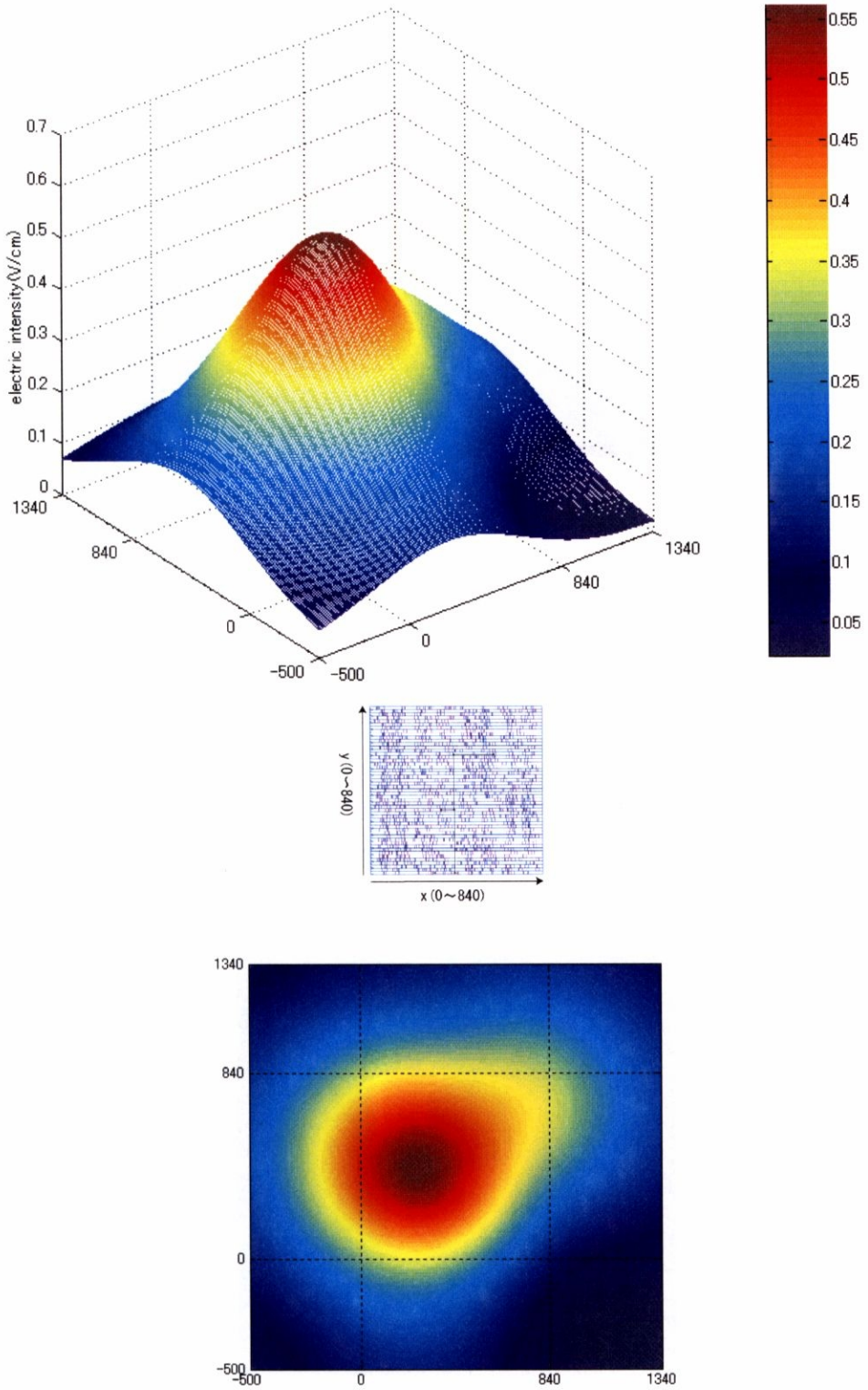

図 3.18 注目配線からの電界強度マップ（100MHz 成分）

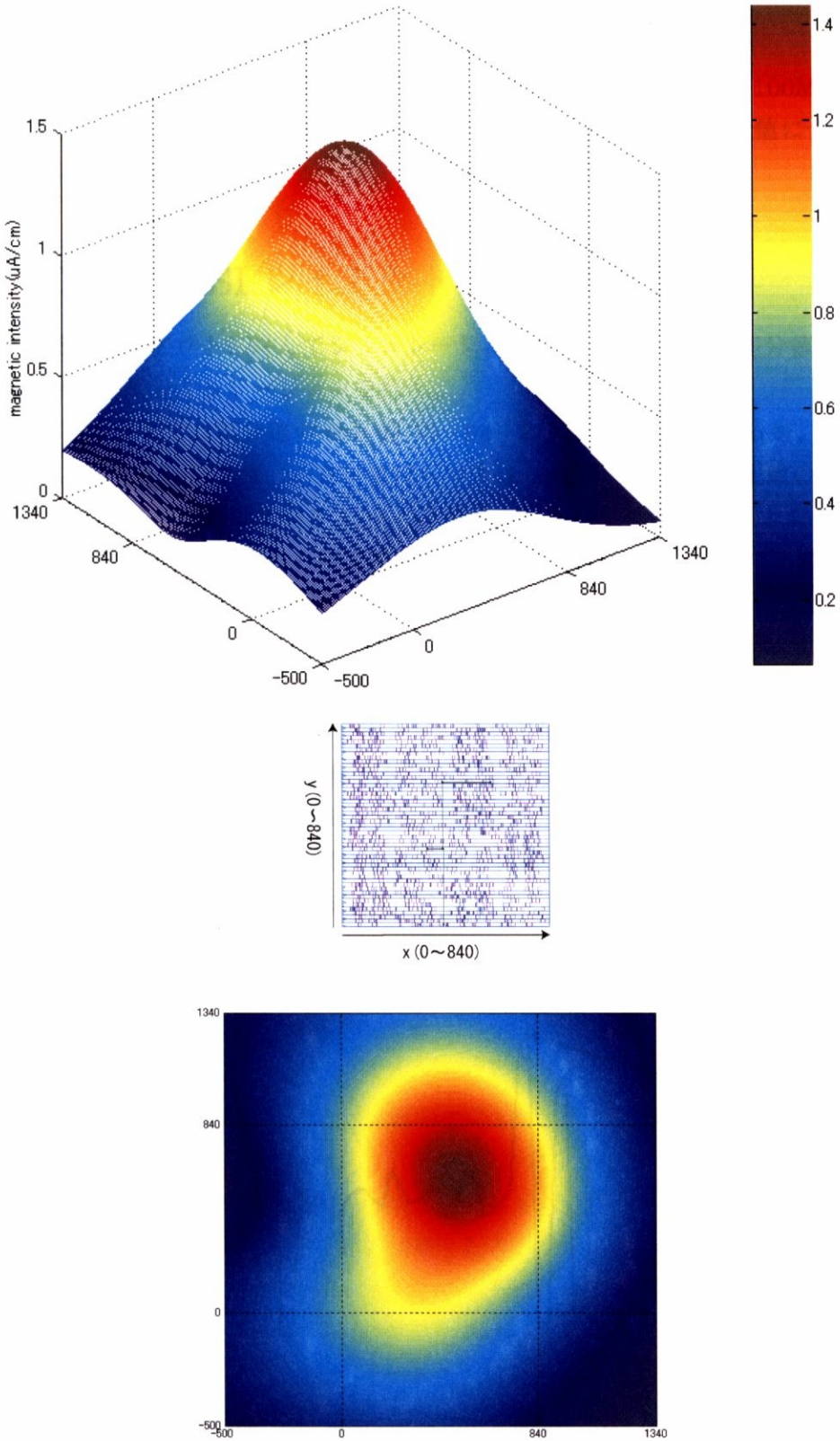

図 3.19 注目配線からの磁界強度マップ（100MHz 成分）

3.5 シミュレーション結果

3.4 に示すシミュレーションを適応して得られたアンテナ空間電位差（100MHz 成分のみ）の集合について 2.3.9 項の式に従って差分解析を適応し、得られた差分値について DES の暗号鍵の解析を行う。

3.5.1 DES の LSI レイアウトへの解析結果

DES の LSI レイアウトに対してシミュレーションを行って得られた差分値を解析して DES の部分鍵の解析シミュレーションを行う。

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。以下は、しきい値ばらつき 1.0%ばらつき（注目配線の 2 線間ばらつき 1.0%、その他の配線のばらつき 1.0%の正規分布）の結果を示す。

図 3.20 と図 3.21 は鍵の予測値と相関値の関係を示した図である。サンプル数が 1000 と 50000 の時の結果を示しているが、どちらの場合も真の鍵である 41 において最も高い相関値が得られている。また、サンプル数 50000 の時はサンプル数 1000 の時と比べても、正しい鍵のピーク値が鋭く現れていることが確認できた。

図 3.22 に示すような、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、2 線式相補配線のアンバランスを示す相関値であると判断できる。実際にこの図から判断する限りサンプル数が 1000 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。

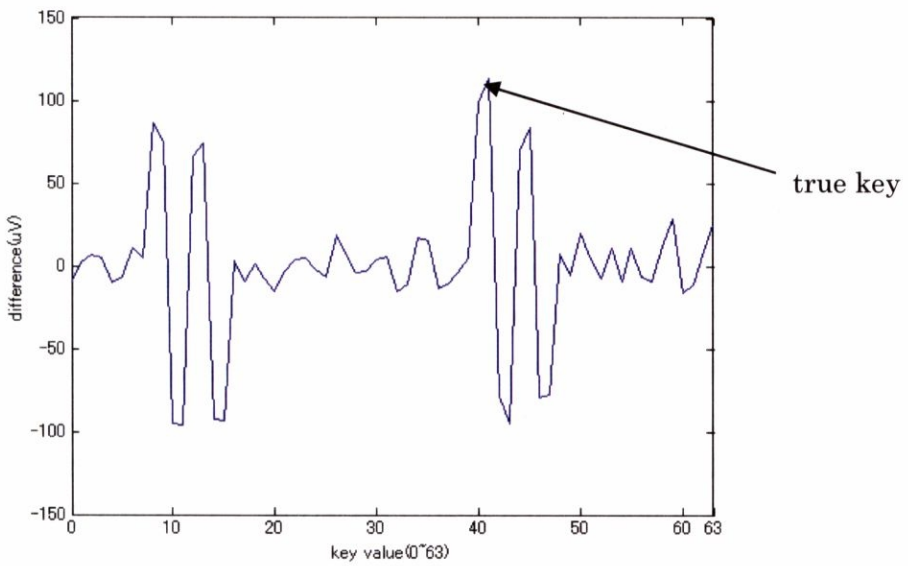

図 3.20 サンプル数 1000 の場合の予測鍵と相関値

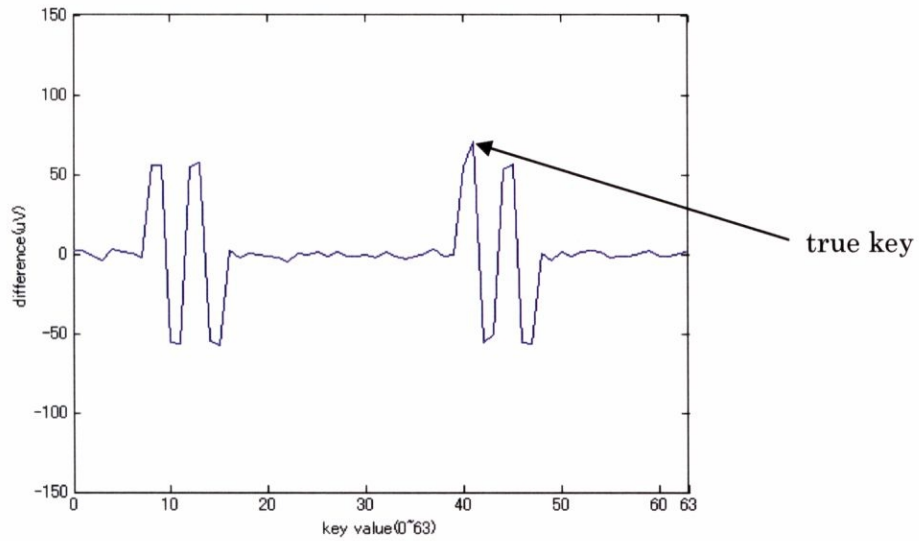

図 3.21 サンプル数 50000 の場合の予測鍵と相関値

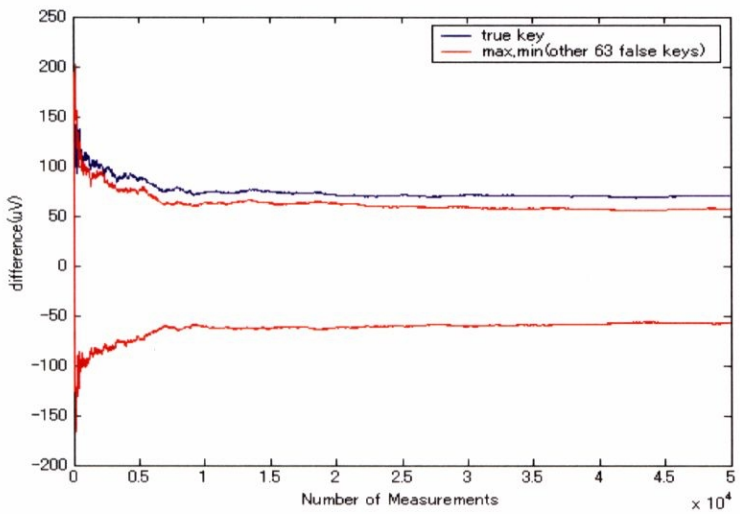

図 3.22 サンプル数の変化と相関値の推移

同様の解析をばらつき環境を 0%～10.0%と変化させて同様にシミュレーションを行った結果を図 23 に示す。シミュレーションの結果、しきい値ばらつきが生じている環境ではしきい値ばらつきなしの環境（ばらつき=0%）よりも少ないサンプル数で解析ができることが確認できた。また、ばらつき環境が非常に大きくなっても解析に必要なサンプル数は若干増えるがそれほど変わらないことも確認できた。これは、注目配線のばらつきが大きくなって相関値が大きくなる代わりに、他の配線から受けるノイズ部分も大きくなる体と考えられる。しかしながら、信号成分の絶対値は大きくなっているので解析の雑音耐性については強くなっていると考えられる。

また、シミュレーションの結果から、ばらつきが0%の場合においてもばらつきが無い場合に比べて多くのサンプル数を必要とするが、解析が可能であることが示された。これは、ばらつきの影響が全くない環境でもWDDLの2線式相補配線のレイアウトのずれが生じる影響のみを考慮しても解析が可能であるということを示している。

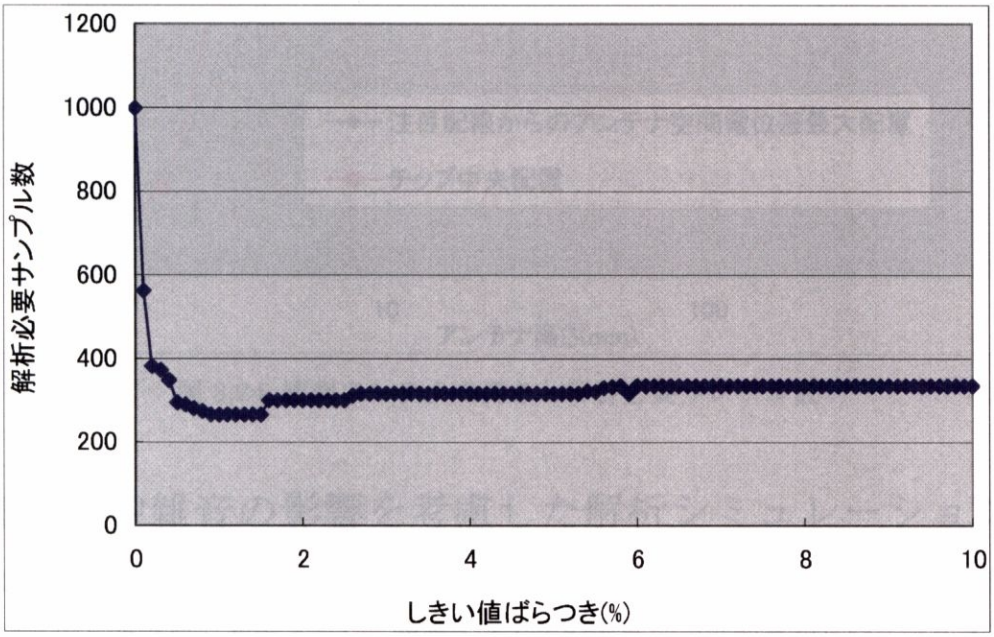

図 3.23 しきい値のばらつき環境と解析必要サンプル数

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

2.4.2 項と同様にアンテナ環境を変化させたシミュレーションを行う。LSI チップからみた観測アンテナの高さを 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。解析の結果を図 3.24 に示す。観測アンテナの高さが大きくなるにつれて解析必要サンプル数も大きくなっていることがわかる。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、十分解析が可能であることがわかった。

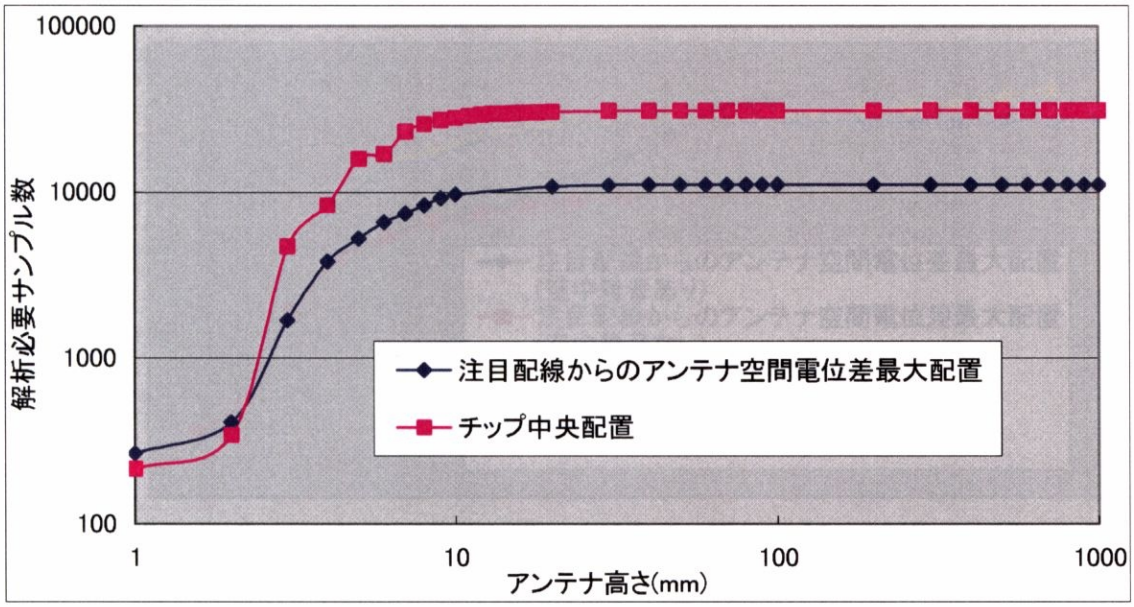

図 3.24 観測アンテナの高さと解析必要サンプル数

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

2.4.3 項と同様に空中雑音の影響を考慮した。空中雑音の値も 2.3.4 項と同じく標準偏差 0.3uV/cm の正規分布で発生させた。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 LSI チップ中心配置の両方を取る。

解析の結果を図 3.25 に示す。解析の結果から雑音の影響は 8mm 程から大きくなることが確認でき、1.5～2cm 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 7mm 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。

素子ばらつきが与える放射電磁波に与える相関値は、標準 1 線式 CMOS 回路における差分電磁界解析での相関値に比べて非常に小さいので、雑音耐性もこれに伴い弱くなっているはずである。しかしながら、本提案手法である素子ばらつきの影響を利用した解析では、空中雑音の影響を考慮しても標準 1 線式 CMOS 回路での差分電磁界解析に比べれば雑音耐性は低いが、現実的なアンテナ高さにおいて十分解析できることがわかった。

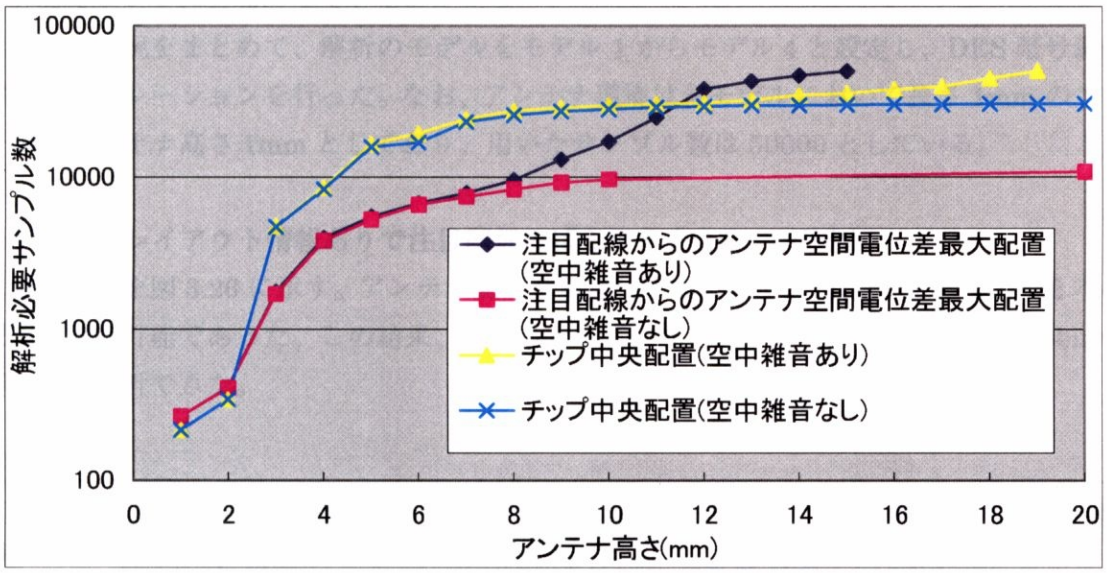

図 3.25 空中雑音を考慮した場合の観測アンテナの高さと解析必要サンプル数

3.5.4 全体の DES 暗号鍵解析

これまで行ってきた、DES の LSI レイアウトに対しての解析シミュレーションは単独の注目配線にしか解析を行っておらず、6bit の部分鍵のみしか解析していない。よって DES のすべての 56bit 暗号鍵を解析するには対象注目配線を変化させて 48bit の全部分鍵の解析を行う必要がある（8bit の鍵が残るが高々256 通りなので全探索で求められる）。なお、差分解析手法においては、原理的に 1 グループのサンプル集合で全注目配線の解析が行える。

全体の DES 暗号鍵を解析にするに当たって、レイアウト情報の有無によって 2 通りの環境を設定する。

① レイアウト情報あり

対象注目配線ごとに DES の LSI レイアウトからアンテナ配置を最適化して解析を行う。

② レイアウト情報なし

DES の LSI レイアウトの中央に観測アンテナを固定した上で解析を行う。

また、しきい値ばらつき環境によって解析の難易度も大きくなるのでばらつき環境を以下の 2 通り設定する。

① 注目配線のばらつき固定

注目配線の 32 本のばらつきを 1.0%で固定した。その他の配線のばらつきは 1.0%の標準偏差を持った正規分布でランダム分布させている。

② 注目配線のばらつきをランダム分布

注目配線の 32 本のばらつき 1.0%の標準偏差の正規分布でランダム分布させたばらつき状況の 1 パターンで固定した。その他の配線のばらつきも 1.0%の標準偏差を持った正規

分布でランダム分布させている。
これらの状況をまとめて、解析のモデルをモデル 1 からモデル 4 と設定し、DES 暗号鍵の解析シミュレーションを行った。なお、アンテナ環境は各モデルにおいて長さ 1mm のアンテナ、アンテナ高さ 1mm としており、用いたサンプル数は 50000 としている。

モデル 1 （レイアウト情報ありで注目配線のばらつきを 1.0%で固定）

解析結果を図 3.26 に示す。アンテナ配置を最適化することで、注目配線 32 本中 22 本の配線が解析可能であった。この結果、8 つのすべての部分鍵が解析でき、56bit 中 48bit の暗号鍵が解析できた。

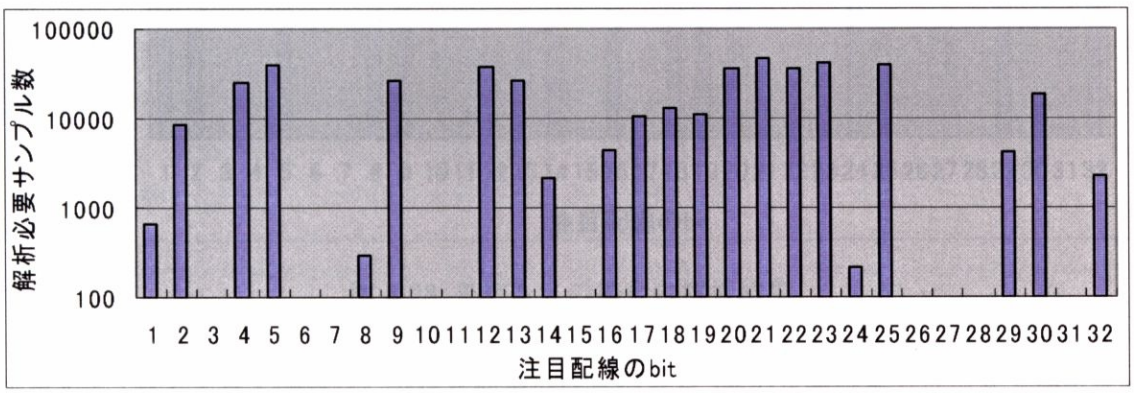

図 3.26 モデル 1 の場合の解析結果

モデル 2 （レイアウト情報なしで注目配線のばらつきを 1.0%で固定）

解析結果を図 3.27 に示す。アンテナ配置をチップ中央で固定し、32 本中 19 本の配線が解析可能であった。この結果、8 つのすべての部分鍵が解析でき、56bit 中 48bit の暗号鍵が解析できた。

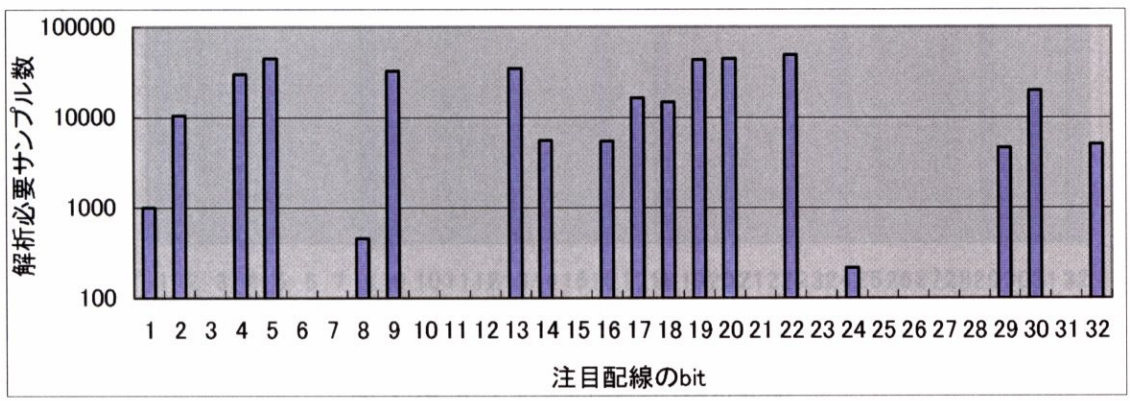

図 3.27 モデル 2 の場合の解析結果

モデル3（レイアウト情報ありで注目配線のばらつきを1%の正規分布でランダム発生させた特定の1パターン）

解析結果を図3.28に示す。アンテナ配置を最適化することで32本中14本の配線が解析可能であった。この結果、8つのすべての部分鍵が解析でき、56bit中48bitの暗号鍵が解析できた。

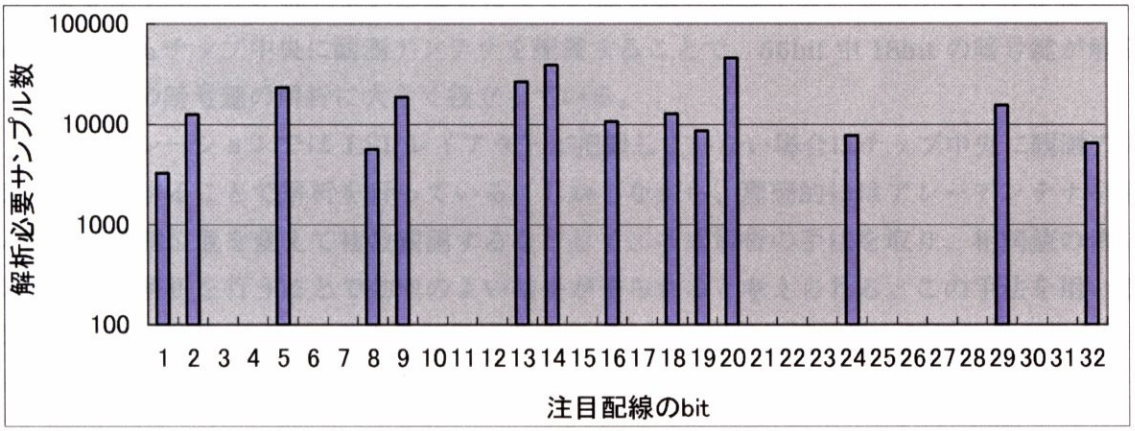

図3.28 モデル3の場合の解析結果

モデル4（レイアウト情報なしで注目配線のばらつきを1%の正規分布でランダム発生させた特定の1パターン）

解析結果を図3.29に示す。アンテナ配置をチップ中央固定し、32本中7本の配線が解析可能であった。8つ中3つの部分鍵が解析でき、56bitの暗号鍵中18bitが解析できた。

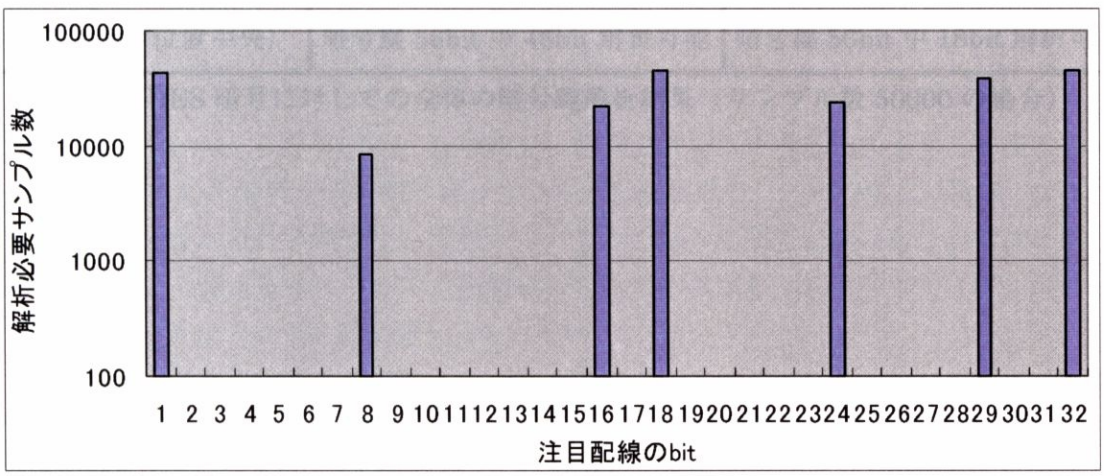

図3.29 モデル4の場合の解析結果

以上の結果を表にまとめると表 3.1 のようになる。解析の結果から、注目配線のばらつきを 1.0%と固定したばらつき環境では 32 本の注目配線のうち、過半数の配線において解析が可能であり、アンテナの位置を最適化できなくても 56bit の全体の暗号鍵を解読する十分な解析を行うことができるとわかった。

しかしながら、実際にはこれらの解析結果はばらつき環境の変化により大きく変わると考えられる。ばらつき環境をランダム分布で発生させた現実的なばらつきでの 1 状況においてもレイアウトが把握している場合は全ての暗号鍵が解読でき、レイアウトが把握していない場合もチップ中央に観測アンテナを配置することで、56bit 中 18bit の暗号鍵が解読でき、全体の暗号鍵の解析に大きく役立っている。

本シミュレーションでは LSI レイアウトが把握していない場合はチップ中央に観測アンテナを配置することで解析を行っている。しかしながら、理想的にはアレーアンテナを用いたり、観測位置を変えて複数観測するなどして、多重解析の手法を取り、相関値の値に応じた多重解析を行うことで効率のよい結果が得られると考えられる。この手法を用いることにより、理想的にはモデル 2 解析結果はモデル 1 の解析結果に近い解析結果が得られ、モデル 4 の解析結果はモデル 3 の解析結果に近い結果が得られると考えられる。

	注目配線すべて 1%固定 その他の配線 1%正規分布	注目配線 1%正規分布 その他の配線 1%正規分布 で発生させた一例 (現実的ばらつき環境)
レイアウト情報あり (アンテナ位置最適化)	注目配線 32 本中 22 本解析可能 暗号鍵 56bit 中 48bit 解析可能	注目配線 32 本中 19 本解析可能 暗号鍵 56bit 中 48bit 解析可能
レイアウト情報なし (アンテナ位置中央)	注目配線 32 本中 14 本解析可能 暗号鍵 56bit 中 48bit 解析可能	注目配線 32 本中 7 本解析可能 暗号鍵 56bit 中 18bit 解析可能

表 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）