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

本章では、電力解析と電磁界解析について説明を行った上で標準 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、シミュレータの有効性を確認し解析結果をまとめた。また、差分電磁界解析の対策手法を複数提案し、シミュレーションによりその有効性を確認する。

2.1 電力解析・電磁界解析の原理・概要

電力解析・電磁界解析の原理・概要の解説を行う。電磁界解析は電力解析における攻撃に利用する付加情報である消費電力を電磁界強度に置き換えたものであるから、この章では電力解析を中心に解説を行う。

2.1.1 電力解析

電力解析は暗号処理中の消費電力を観測して解析を行う解析手法である。1998 年に Kocher らが提案し[3]、共通鍵暗号の 1 つである DES 暗号を実装したスマートカードに対し実験が行なわれている。DES 暗号だけでなく、公開鍵暗号である RSA 暗号や、共通鍵暗号としての事実上標準となりつつある AES 暗号についても攻撃が行われており、暗号鍵解読に成功している[8][9]。

電力解析では、処理を行っているときの暗号デバイスの消費電力が秘密情報や処理内容と関係があることに着目し、消費電力を観察することによって秘密情報を推定している。解析手法として、単一消費電力波形に対して直接的な解析を行う単純電力解析と、複数の消費電力波形を用いて統計的手法を用いる差分電力解析とに大別される。

具体的に、消費電力波形は演算の種類、演算順序、データ、ハードウェア構成などに依存するため、電力解析の結果として消費電力波形より演算内容や、ハードウェア構成、さらに秘密情報の類推や解析などを行うことができる。

ここで、電力解析の原理について述べる。まず、CMOS 回路の消費電力を以下に示す。

$$P = Pd + Psc + Plk$$

Pd：負荷容量の充放電による消費電力

Psc：貫通電流による消費電力

Plk：漏れ電流による消費電力

と示される。ここで、Pd と Psc はスイッチング時に発生する電力で、スイッチング周波数 f に比例すると考えられ、さらに Plk はプロセスルールなどに依存するが、スタティックな値と見なせる。よって消費電力 P は以下のように表せる。

$$P = f \cdot (Kd + Ksc) + Plk$$

Kd, Ksc：定数

この式より、CMOS 回路の消費電力が遷移確率と関連があり、あるゲートの入力や出力が 0 か 1 かによってゲートの消費電力も異なってくることがわかる。この性質を利用して電力解析が行われている。

2.1.2 単純電力解析

単純電力解析とは暗号処理中の暗号デバイスの消費電力の一波形を直接測定し、解析に用いることにより秘密情報に関する情報を得ようとする解析手法である。この解析手法は主に暗号デバイスの使用している暗号アルゴリズムの推定などといった大まかな暗号処理の推定によく用いられている。

消費電力波形はデバイスが実行している一連の演算を反映するため、例えば次のような情報を得ることができる。

- 鍵スケジュール

  DES の暗号鍵生成部でのビットシフトにおいてシフトされる鍵の bit が'0'か'1'か、またシフト回数の違いが消費電力に現れる場合は、これらの情報が推測できる可能性がある。

- 転置

  転置されるデータによって転置アルゴリズムが異なる場合は消費電力の違いから情報を得ることができる。

- 比較

  比較を行う際の条件分岐やミスマッチなどの情報は消費電力に影響を与える場合が多く、情報を得る手がかりとなりやすい。

- 乗算

  乗算時の消費電力波形はオペランド値やハミング重みによって大きく異なり、消費電力波形が情報を得る手がかりとなる。

- 剰余算演算

  剰余算演算は一般に乗算と平方の組み合わせで演算され、その各々の消費電力パターンに特徴が見られることが多い。例えば、単純な剰余算演算はべき指数を上位桁か

ら順にスキャンしていき、ビット値が'1'のとき乗算を行いながら平方演算を繰り返している。もし、平方演算と乗法演算がそれぞれ異なる消費電力波形や処理時間をとる場合には、べき指数についての情報を得ることができる。

具体的に DES 暗号における単純電力解析を説明する。図 2.1 は DES 暗号の一連のオペレーションにおける消費電流波形である。この波形を見るように DES 暗号の１６ラウンドがはっきりと確認できている。さらに図 2.2 は先程の DES 暗号の一連のオペレーションの中での第２、第３ラウンドでの電流波形である。DES 暗号では第２ラウンドでは鍵レジスタを１ビットシフト、第３ラウンドでは２ビットシフトしているのだが、これが消費電流波形からも確認できる。これらの例の他に単純電力解析だけでも命令実行の手順など様々な情報が解析される。

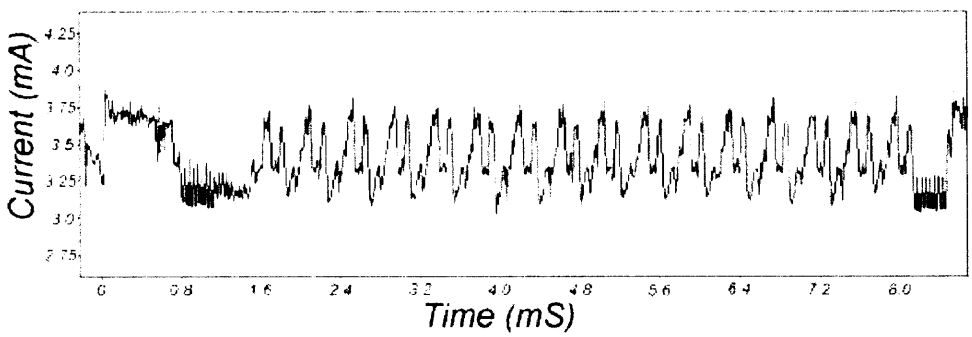


図 2.1 DES オペレーションの電流波形

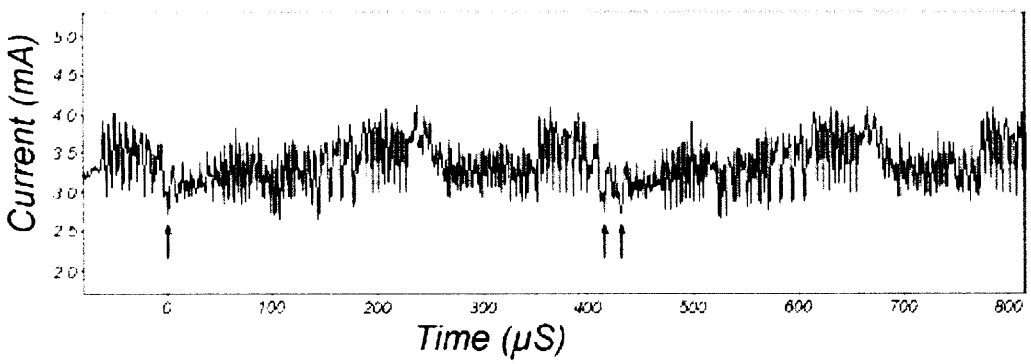


図 2.2 DES オペレーションの第２・３ラウンドの電流波形

2.1.3　差分電力解析

差分電力解析とは回路の電流を監視して、回路のトランジスタやソフトウェアなどの特性を利用して、統計的手法を用いて秘密情報を解析する方法である。差分電力解析では、

大量の測定値の平均をとって測定誤差やノイズなどの影響を小さくし、全データの平均値との差分を取ることで演算プロセスによる電力消費の影響を除いて、秘密情報に依存した消費電力の変化のみを取り出すことで効率的な解析を行っている。解析に必要な条件として以下があげられる。

- 暗号アルゴリズムは既知である。
- 平文・暗号文が既知である。
- 暗号処理中に消費電力を測定できる。
- 鍵を固定した上で、任意の大量の平文または暗号文を回路に通すことができる。

ここで、差分電力解析の簡単な原理を説明する。差分電力解析では回路中のある中間データのビットに着目し、その参照値の予想値によって測定した消費電力のデータを2つのグループに分類する。回路の消費電力は真の参照値と相関があり、演算に関係する鍵を予想すると、予想した鍵と既知の暗号文（または平文）から参照値の予想値が得られることになる。この参照値の予想値を返す関数を選択関数と呼ぶ。そして、攻撃者は鍵を予想した上で選択関数により参照値を予想する。予想値が正しいときに限り、選択関数は真の参照値を返すため、参照値により測定した消費電力を分類するとグループ毎の消費電力の平均値には、参照値による消費電力の差が生じる（表 2.1)。これに対して予想値が正しくなければ、選択関数はほぼランダムな値を返すため、測定した消費電力は相関なく分類され、グループ毎の消費電力の平均値の差はほぼ0 になる（表 2.2)。

すなわち、予想した鍵のうちグループ毎の消費電力の平均値の差が最も大きいものが正しい鍵であることが期待される。

予想値(選択関数)	実際の値	消費電力
1	1	P
0	1	P+a
1	0	P
0	0	P
1	1	P+a
1	0	P
0	1	P+a
0	0	P

予想値(選択関数)	実際の値	消費電力	グループの電力平均
1	1	P+a	P+a/2
1	0	P	
1	1	P+a	
1	0	P	
0	1	P+a	P+a/2
0	0	P	
0	1	P+a	
0	0	P	

表 2.1 差分電力解析の手法（予想値が間違っている場合）

予想値(選択関数)	実際の値	消費電力
1	1	P+a
1	1	P+a
0	0	P
0	0	P
1	1	P+a
0	0	P
1	1	P+a
0	0	P

予想値(選択関数)	実際の値	消費電力	グループの電力平均
1	1	P+a	P+a
1	1	P+a	
1	1	P+a	
1	1	P+a	
0	0	P	P
0	0	P	
0	0	P	
0	0	P	

表 2.2 差分電力解析の手法（予想値が正しい場合）

2.1.4　電磁界解析

電磁界解析は電力解析における消費電力を電磁界強度におきかえたものである。この場合、回路から放射される電磁波を測定分析することで秘密情報を推定する。解析の方法としては電力解析と同様であり、以下の単純電磁界解析と、差分電磁界解析の２つに大別できる。電磁界解析の手法自体は 2001 年に、K. Gandolfi らにより、DES や RSA 実行中に放射される電磁波を測定分析すると秘密鍵を特定できることが具体的に示され、実際に有効性が確かめられた[7]。

- 単純電磁界解析（SEMA：Simple ElectroMagnetic Analysis）
  回路から発生する電磁界を直接解析に用いる。電力解析の単純電力解析に相当する。
- 差分電磁界解析（DEMA：Differential ElectroMagnetic Analysis）
  複数の電磁波を用いて統計的に解析を行う。電力解析の差分電力解析に相当する。

前提条件は、最低条件としてチップが発生する電磁界を電磁プローブ等を用いて観測できることが条件となるが、単純電磁界解析と差分電磁界解析によって以下の条件が加えられる。

- 単純電磁界解析
  - 解析したい一連の処理の電磁波を測定できることが必要である。
- 差分電磁界解析
  - 暗号アルゴリズムが既知である。
  - 平文・暗号文が既知である
  - 暗号処理中に電磁波を測定できる
  - 鍵を固定した上で、任意の大量の平文または暗号文を回路に通すことが出来る。

また、解析できる情報としては電力解析と同様に以下があげられる。

- 単純電力解析
  - 鍵スケジュール
  - 転置
  - 比較
  - 累乗演算
  - バスのハミング重み
- 差分電磁界解析
  - 回路のある特定の bit 値

2.2　差分電力解析・差分電磁界解析の手順

差分電力解析・差分電磁界解析の手順を説明する。差分電磁界解析では差分電力解析での消費電力を電磁界強度に置き換えたものであるから差分電力解析に絞って説明を行う。

DES での差分電力解析の例を説明する。

① 消費電力波形の測定

平文をランダムに変化させて DES 暗号処理を多くの回数行い、波形を測定する。今回は処理数を 1000 とし、1 回の測定におけるサンプル点を 100000 として、電力波形を S[k][j]=S[0…999][0…99999] (k：サンプルナンバ、j：サンプル点)の 2 次元配列で定義する（図 2.3)。また、このとき得られた暗号文を C[0…999]とする。測定する波形は後に述べる選択関数が関係する部分の付近の波形で十分である。この場合は第16ラウンドのレジスタの特定の1bitに着目しているので処理部分が正しく区別できるならばこの第 16 ラウンド付近の消費電力を測定する。

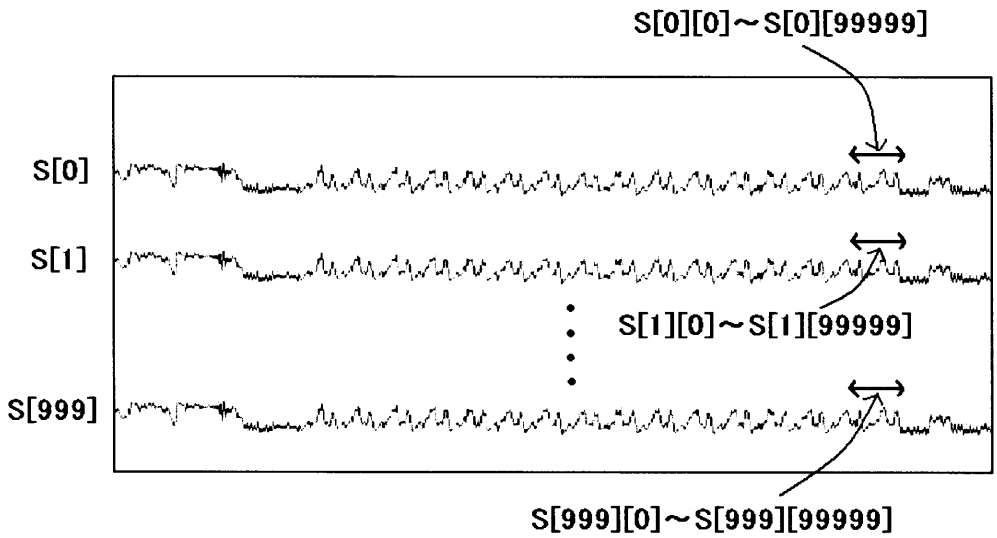


図 2.3 DES 暗号処理における消費電力の測定

② 選択関数の決定

鍵の値をある特定の値に予測した場合に推測される回路内の特定のビットを求める関数を「選択関数」D と定義する。選択関数は暗号文または平文と推測した鍵から一意的に計算可能なものを定義する。ここで、選択関数を D(Ki,C)と定める(Ki は予測した部分鍵、C は出力された暗号文)。今回の例では選択関数を DES 暗号の第 16 段の L15 レジスタのある特定の 1bit に定め、以下のような選択関数を用いて攻撃を行うとする（図 2.4)。

$$D(c_1, c_6, K_{16}) = c_1 \oplus SBOX_1(c_6 \oplus K_{16})$$

K16 は第 16 段の S-Box1 に入力される 6 ビットの値に対応する部分鍵の予想値、c6 は K16 と XOR される出力された暗号文 6 ビット、SBOX1(x) は非線形関数である S-Box1 に 6 ビットの入力 x を与えたときの出力の 1 ビット目、c1 は SBOX1 の出力結果と注目するビットを XOR した結果の 1 ビットである。

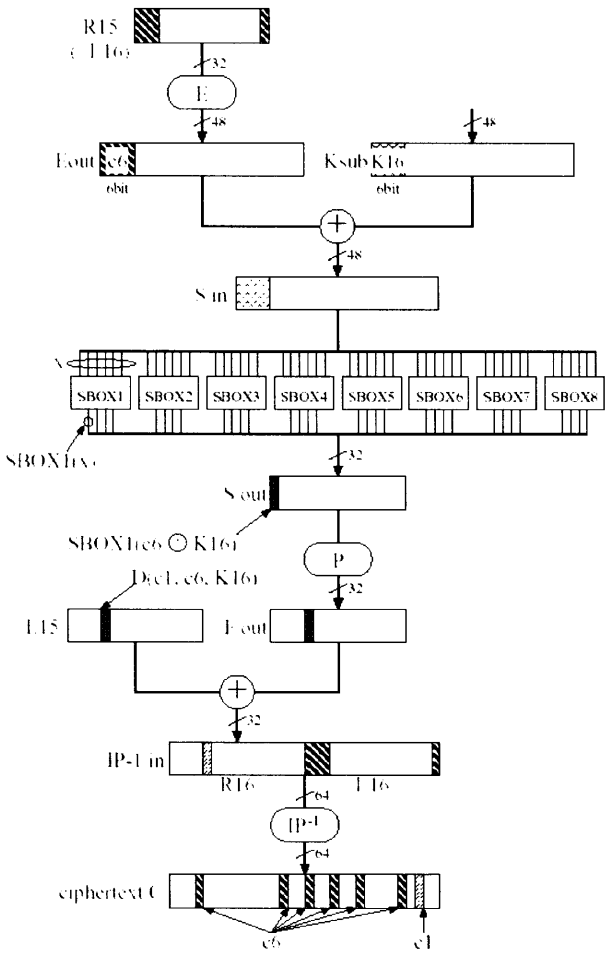


図 2.4 DES の第 16 段から暗号文出力まで

③ 差分電力波形、相関電力波形を計算する

①で得られた電力波形を用いて、電力波形の差分波形、または相関波形 T[i][j]（i：鍵の予測値、j：サンプル点 i=0…63、j=0…99999）を計算する。

相関波形については

$$P_0 = \{S[k][j] | D(i, C(k) = 0)\} \qquad P_1 = \{S[k][j] | D(i, C(k) = 1)\}$$

$$A_0 = \frac{1}{|P_0|} \sum_{S \in P_0} S \qquad A_1 = \frac{1}{|P_1|} \sum_{S \in P_1} S$$

$$T[i][j] = A_0 - A_1$$

差分波形については

$$T[i][j] = \sum_{k=0}^{999} (D(i, C[k]) - 1/2)(S[k][j])$$

と定義される

④ 差分電力波形・相関電力波形を用いた解析

③で得られた T[i][0…99999]において予測鍵の値 i の値が実際の鍵の値と一致しているときは注目ビットの影響が T[i][j]に大きく現れることになる（図 2.5)。なぜなら、予測が正しく合っているときには、選択関数が 1 と予測したときの電力波形と選択関数が 0 と予測したときの電力波形には注目するビット選択関数の影響分だけ消費電力に差が生じており、その分だけの影響が T[i][j]に現れるからである。また、i の値が実際の鍵の値と異なっている場合は選択関数はほぼランダムな値を返すので消費電力は相関無く分類され、T[i][j]はほぼゼロとなる。よって、全ての鍵の予測値 i=0…63 において T[i][j]の変動のピーク値を比較し、最も大きかった場合の i を正しい部分鍵とする（図 2.6)。

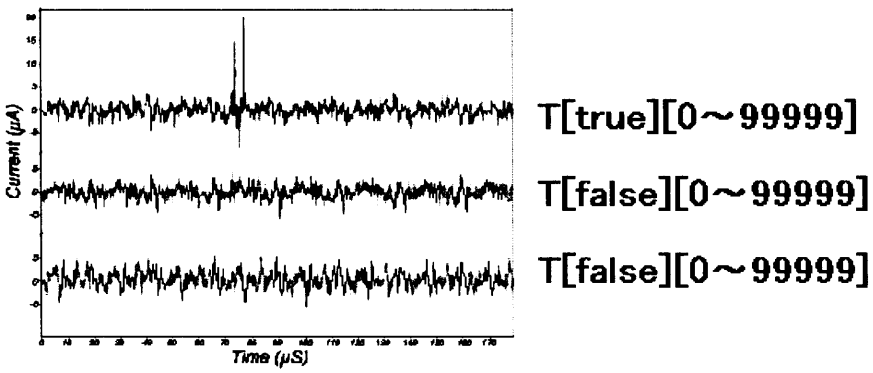


図 2.5 相関波形の比較

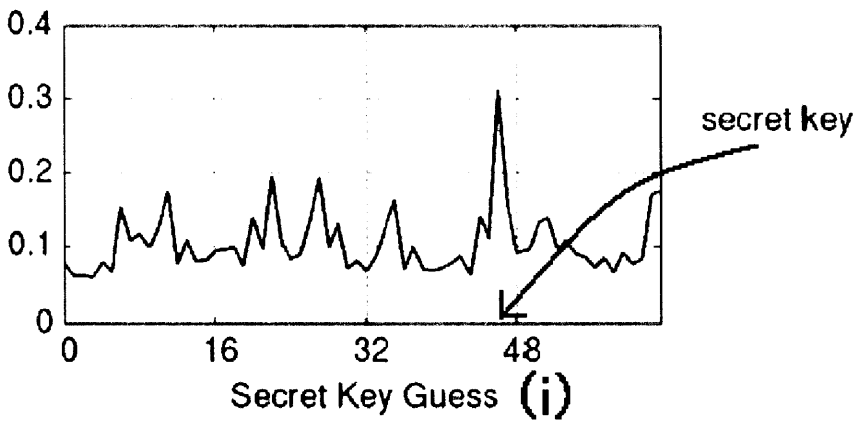


図 2.6 予測鍵と相関波形のピークの比較

これらの推定は測定波形数が多くなればなるほど正確さが増すことになる。図 2.7 に使用した測定波形数と差分値のピークの比較を示す。測定波形数が多くなるほど予測の正確さは増すことになる。

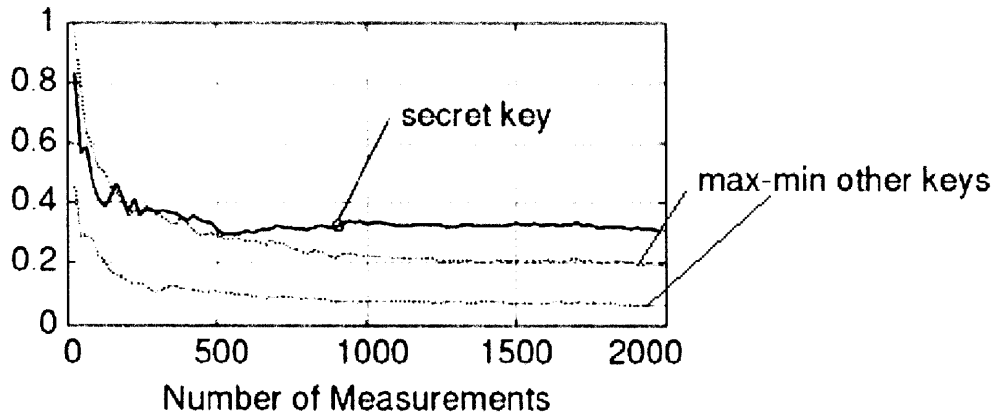


図 2.7 測定波形数と相関関数のピークの関係

⑤ 全体の暗号鍵の推定

②から④を、選択関数を変えながら他の7つの部分鍵について繰り返し、全体の秘密鍵 56bit 中の 48bit を得る。残りの 8bit については高々256 通りであるから全探索によって求められる。

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

一般のLSIに使われている標準1線式CMOS回路において差分電磁界解析シミュレーションを行い、その有効性を確かめる。

2.3.1 差分電磁界解析シミュレータの目的・利点

標準的なLSI回路である1線式標準CMOS回路に対して差分電磁界解析シミュレーションを行う前に、差分電磁界解析シミュレーションを行う目的や利点を説明する。

サイドチャネル攻撃についての解析や防御手法についての提案は数多く論文などで発表されており、その数は近年増え続けている。その中でも電力解析に対しての研究はもっとも進んでおり、解析手法の提案にとどまらず、ソフトウェア・ハードウェア両面に対しての対策手法も数多く提案され、さらに電力解析のシミュレータも数多く提案されている。

これらの研究成果の中で解析シミュレータの持つ利点を説明する。解析シミュレータの最も大きな利点としては耐タンパーLSI の耐タンパー性に対して手軽に評価が行えるということである。このことは実際に解析装置を必要としないという意味でも言えるが、実際の LSI の製造には多額の費用と数ヶ月にわたる期間が必要であるからこれらのコストがか

からずに耐タンパーLSIを評価できるという意味でも非常に有益である。さらに、LSI製造前の段階でシミュレーションを行っているのでシミュレーション結果に応じて手軽に修正を行い、よりタンパー性の高い耐タンパーLSIを設計できることになり、数多くの修正を行えることができることと相成って、耐タンパー性のさらなる向上自体にもつながることになる。

電力解析についてのシミュレータは数多く提案され、実際に様々な手法に基づいた電力解析シミュレータが存在している。これは、消費電力についてはSPICEシミュレーションや論理シミュレーションを元にして計算することが比較的容易であるからである。しかしながら、電磁界解析についてのシミュレータは現在においても一般的に提案されているものは存在していない。これは、LSIから放射される電磁界の評価についてはシミュレーションが難しいとされることが大きな理由だと考えられる。ところが、電磁界解析の報告例では同じLSIチップに対して行った解析において差分電磁界解析の方が差分電力解析よりも解析に有利であったという報告[7]があったり、電磁界解析ではチップ電源線などにアクセスしなくても解析が可能であるという解析に有利とされる特長もある。さらに、電力解析は、今後の電源電圧の低下や駆動周波数の増加などにより、測定時の負荷容量の影響を考慮した上でも消費電力の観測は非常に難しくなると考えられる。このような背景から、電磁界解析に対しての対策やシミュレータの要求は電力解析と同様に高まっている状況である。

以上のような背景から電磁界解析に対してのシミュレーションを行うことの重要性が説明でき、本章では一般的なLSIに対しての差分電磁界解析シミュレーションを行い、有効性を評価する。

2.3.2 差分電磁界解析シミュレーション手順の流れ

差分電磁界解析シミュレーションの流れ図を図2.8に示す。本提案シミュレーションはDESのLSIレイアウトに対して差分電磁界解析を行うものである。本論文のシミュレーションではDES暗号をverilogで設計し、LSIレイアウトを自動合成したものを差分電磁界解析シミュレーションしてシミュレータの妥当性を評価しているが、実際の利用法としては、設計済みのLSIレイアウトの差分電磁界解析耐性を評価したり、自動合成手法の差分電磁界解析耐性を評価するなど、様々な利用法が考えられる。

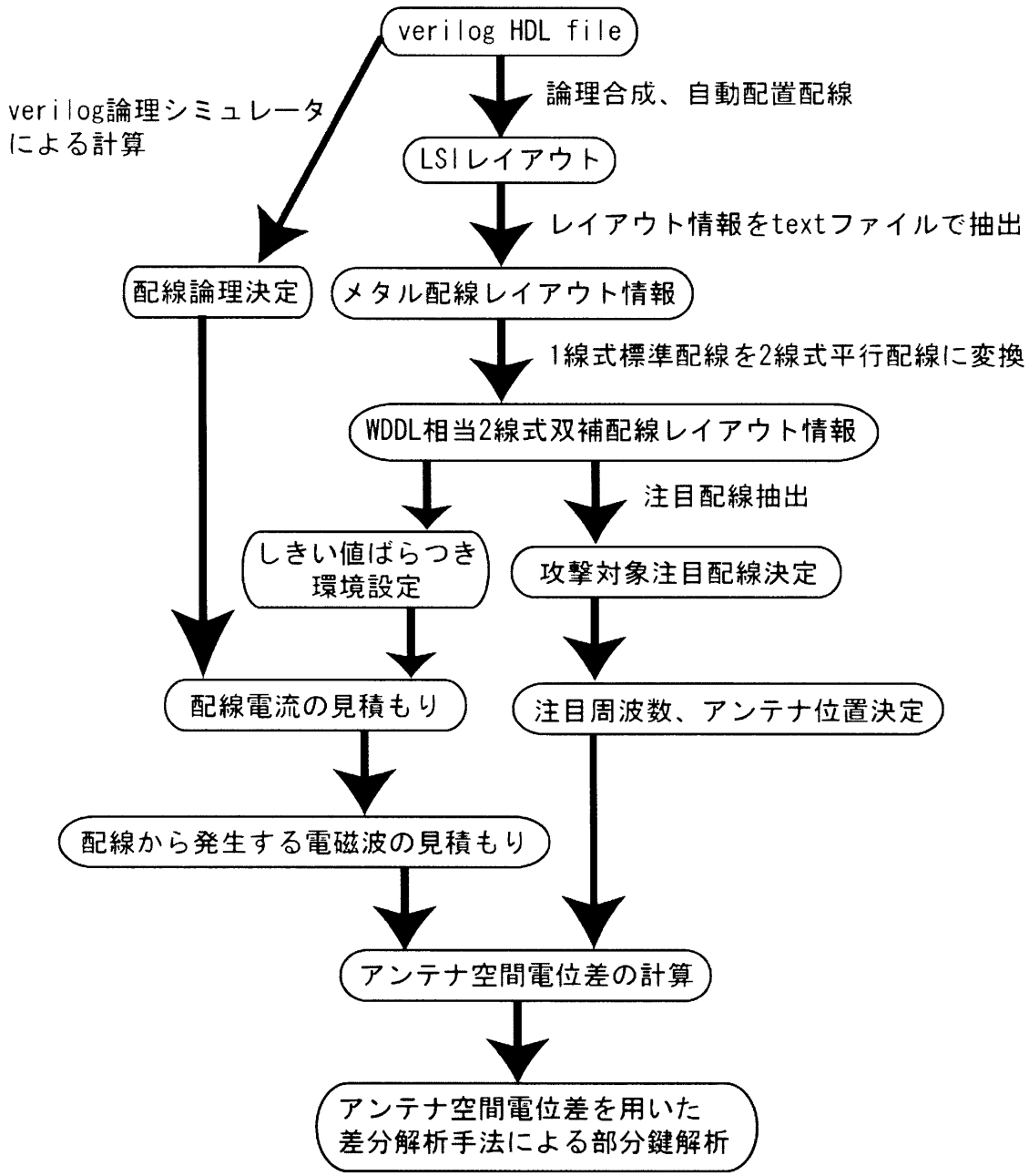


図 2.8 標準 1 線式 CMOS 回路に対しての差分電磁界解析シミュレーションの手順

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。

2.3.3 DES の LSI レイアウト生成

DES 暗号は、秘密鍵 56bit（パリティ付きで 64bit）と入力データ 64bit の 2 つを入力として、F 関数と呼ばれる非線形関数（ラウンド関数）を 16 回繰り返して実行することで入力データをスクランブル化する Feistel 構造の 64bit ブロック暗号である[10]。

今回生成する DES 暗号はラウンド関数を 1 つのみ持ち 1 回の DES オペレーションに対して 16 回同じラウンド関数を使い回すことで小面積化を図るアルゴリズムのものを用いた。

入出力情報（図 2.9）とタイミング情報を図 2.10 に示す。この DES 回路では入力信号がクロック信号の clk と平文の pt (64bit)、鍵情報の key (64bit)、処理開始信号の pin (1bit) となっており、出力信号は暗号文 ct（64bit）と処理終了信号 cout（1bit）をとっている。具体的なタイミングの説明としては、pin を'1'にし、鍵情報の key と平文の pt を入力すると 17 サイクル後に、終了信号 cout が'1'となり、暗号文出力 ct が得られることになる。

このような 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 2.11)。このときのプロセスは 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。

ここで、レイアウトを生成する際に用いた 350nm プロセスというのは現在主流となっている 130nm や 90nm プロセスに比べるとかなり古いプロセスであるが、実際にスマートカードにおいては駆動電圧 3.3V～1.8V 程度で駆動周波数数 MHz～数十 MHz という比較的古い仕様の LSI が使われているので、スマートカードに使われている LSI を対象とした解析においては適当な環境であると考えられる。

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。

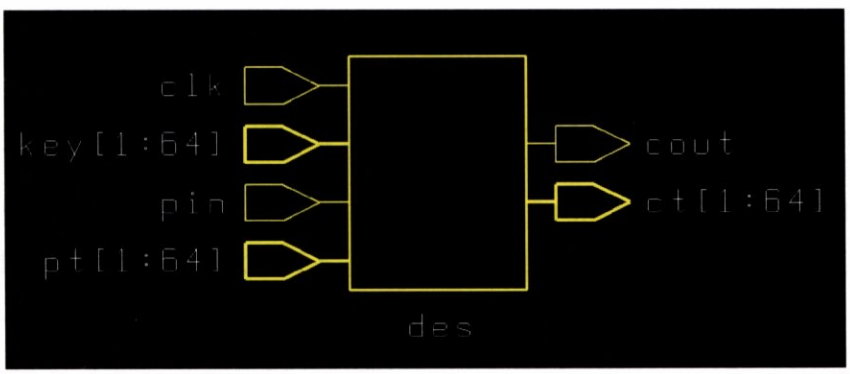


図 2.9 DES 暗号回路の入出力図

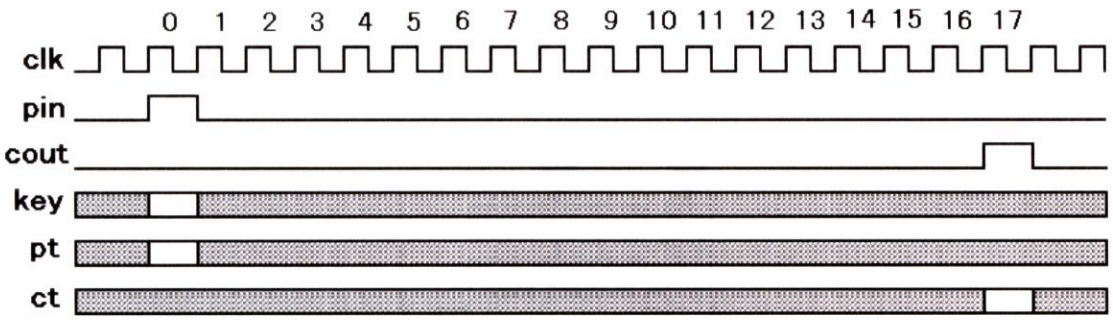


図 2.10 DES 暗号回路のタイミング図

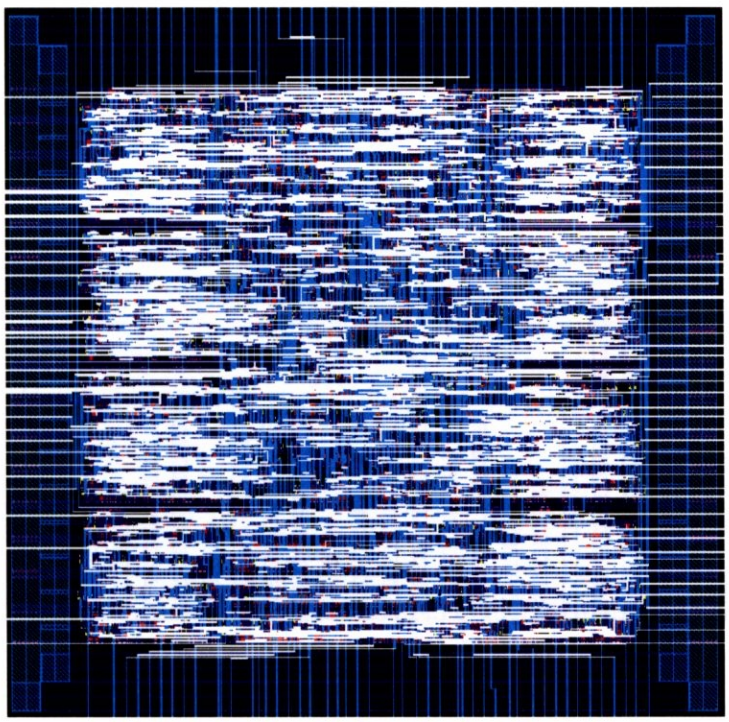


図 2.11 自動合成された DES の LSI レイアウト(600um×600um)

2.3.4 攻撃対象となる注目配線の抽出

攻撃対象となる配線を設定する。LSI 中の大量にある内部配線のうち、選択関数が設定でき、差分解析手法に用いることができる論理を含む配線を「注目配線」と設定する。この場合、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(図 2.12)この配線の論理は平文または暗号文と推測鍵から一意的に求まり、選択関数となる条件を満たしている。他にも注目配線となりうる配線はあるが、レジスタからの直接出力であることと、DES の回路構造からこの部分の配線が比較的長くなると考えられるのでこれらの配線を攻撃対象にした。

32 本ある注目配線（図 2.13）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 2.14：821.68um)に注目し、攻撃対象とした。

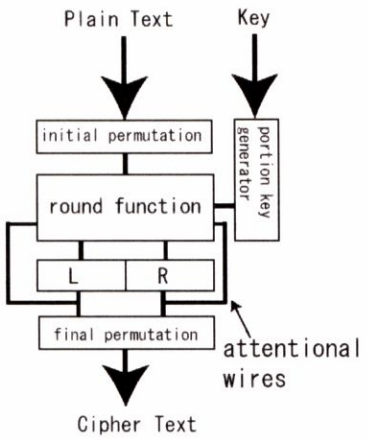


図 2.12 注目配線の設定

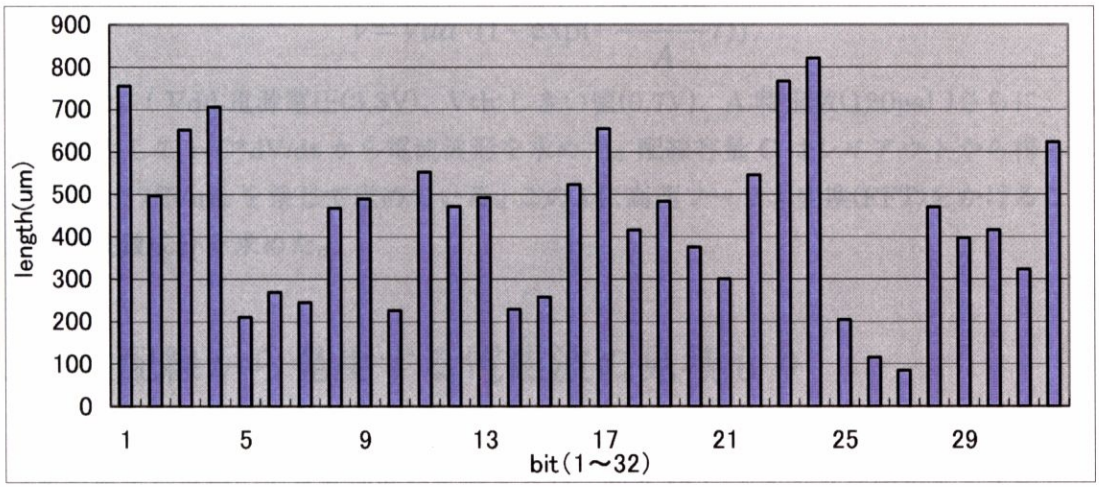


図 2.13 注目配線の長さの比較

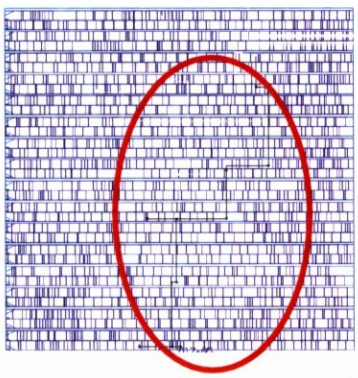


図 2.14 攻撃対象とした第 24bit 配線(821.68um)

2.3.5　配線論理の設定

verilog 論理シミュレータから全ての内部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。

2.3.6　内部配線からの配線電流の見積もり

配線の信号電圧、発生電流をレイアウトから概算した。1 線式 CMOS 回路の内部配線において、

立ち上がり('0'→'1')の電圧波形を

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

立ち下がり('1'→'0')の電圧波形を

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

で概算した。(Vdd:電源電圧(3.3V)、Vth:しきい値(0.7V)、A:時定数(120ps))さらに、配線容量を C として i=C*dV/dt から電流波形を求めた。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。

2.3.7　配線から発生する電磁波の見積もり

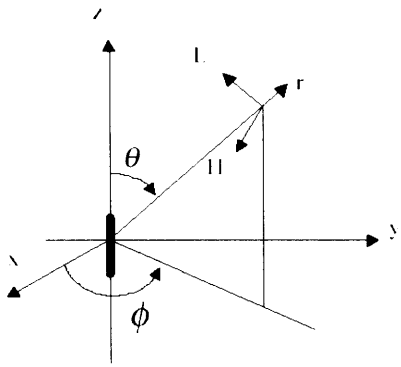
チップ上の全ての内部配線についてマクスウェルの方程式から導かれた微小ダイポールアンテナモデルを用いて電界強度を見積もった。図 2.15 に示すような微小ダイポールアンテナモデルでは長さ L のアンテナに $I_0 e^{jwt}$（周波数 $\omega/2\pi$ 、振幅 I_0）の電流を流すと図に示す 3 つの式のように周囲に電界と磁界の成分が発生する[11]。微小ダイポールアンテナ中心、微小ダイポールアンテナ中心から観測点までの距離は LSI レイアウトから計算し、各周波数成分の電流の振幅は電流式に高速フーリエ変換（FFT）をかけたものから計算した。

ここで、実際の配線だけでなく、実配線と逆方向に電流が流れるチップ基板対称の仮想配線（図 2.16）を考慮し、この配線にリターン電流が流れるとし、仮想配線からの発生する電磁波の影響も足しあわせた。

さらに、配線長が観測アンテナとの距離と比較して大きすぎる配線は微小ダイポールアンテナ中心と観測点との位置の角度差により誤差が生じる。分割単位を変化させて試行し

た結果、長い配線においては観測点と配線との距離の 20 分の 1 以下になるように配線を等長分割した（図 2.17）。これにより精度を高めている。

以上の手法を用いて全周波数成分の電界強度を計算して内部配線から発生する電界強度を見積もった。これを全内部配線に適用して、全ての内部配線からの全電界強度をデカルト座標に変換した上で足しあわせることにより全ての配線全体からの影響を考慮した測定点での電界強度を求めた。



$$E_r = \frac{I_0 L e^{j(\omega t-\beta r)}\cos\theta}{j\omega\varepsilon_0 4\pi}\left[\frac{2j\beta}{r^2}+\frac{2}{r^3}\right]$$

$$E_\theta = -\frac{I_0 L e^{j(\omega t-\beta r)}\sin\theta}{j\omega\varepsilon_0 4\pi}\left[\frac{\beta^2}{r}-\frac{j\beta}{r^2}-\frac{1}{r^3}\right]$$

$$H_\phi = \frac{I_0 L e^{j(\omega t-\beta r)}\sin\theta}{4\pi}\left[\frac{j\beta}{r}+\frac{1}{r^2}\right]$$

Current: $i = I_0 e^{j\omega t}$

Wave number: $\beta = 2\pi/\lambda = \omega/c$

$1/r$ radiated term
$1/r^2$ induced term
$1/r^3$ electrostatic term

図 2.15 微小ダイポールアンテナモデル

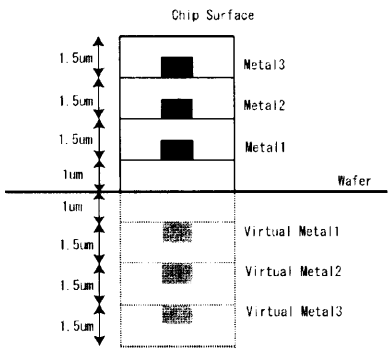


図 2.16 仮想配線からのリターン電流の考慮

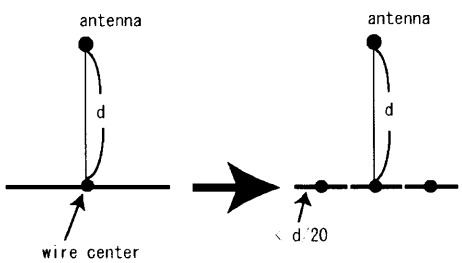


図 2.17 配線分割による精度向上

2.3.8　観測アンテナの配置と空間電位差の計算

観測アンテナでの空間電位差を見積もるために、アンテナ空間上での電界の線積分を行い、アンテナ空間の空間電位差を計算する。このアンテナ空間電位差は観測アンテナ空間を 10um ずつ微小区間分割して微小電位差を足しあわせることにより計算した。チップ上に観測アンテナを配置するにあたり、注目配線のレイアウトを把握している場合はアンテナ位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（図 2.18)。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、注目配線からの影響によるアンテナ空間電位差を示すマップを作った。この場合、注目配線は 100MHz 駆動で論理'0'と'1'を繰り返す動作を取っている。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 2 配置を考慮している。アンテナ空間電位差マップは図 2.19 と図 2.20 に示す。

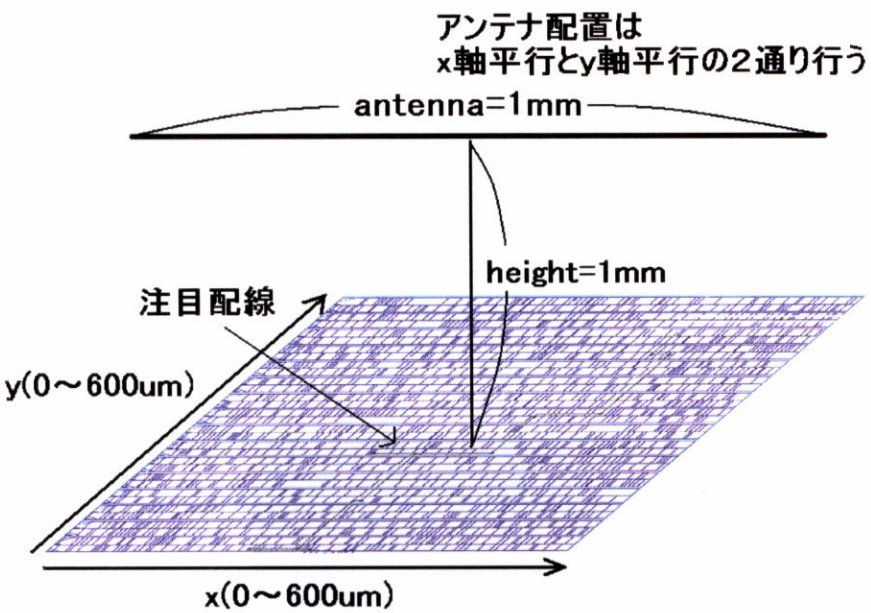


図 2.18 チップ上のアンテナ配置

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。

以上の手法を用いて 50000 回の各サンプルにおけるアンテナ空間電位差を取得した。

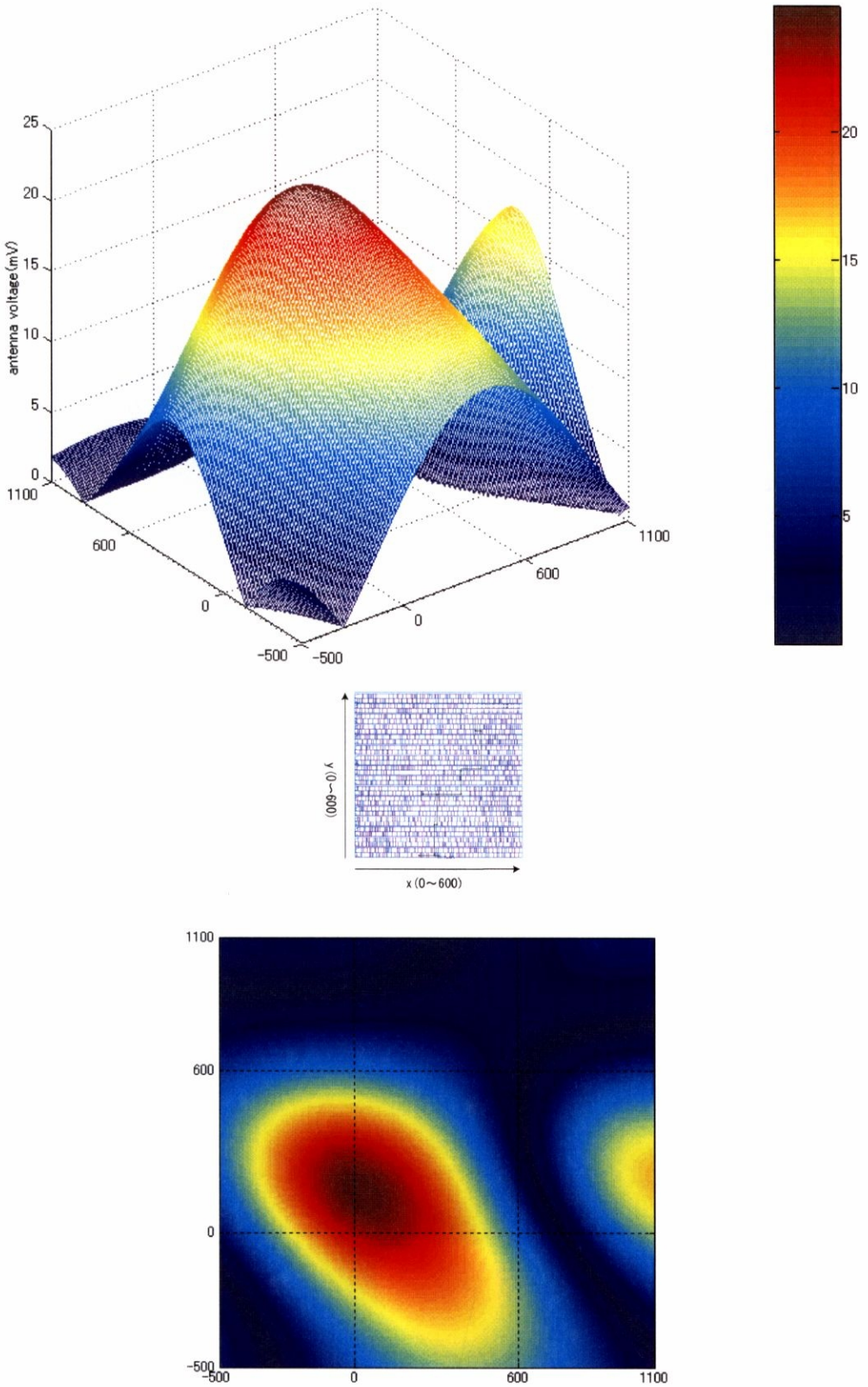


図 2.19 x 軸平行にアンテナを配置した場合のアンテナ空間電位差マップ

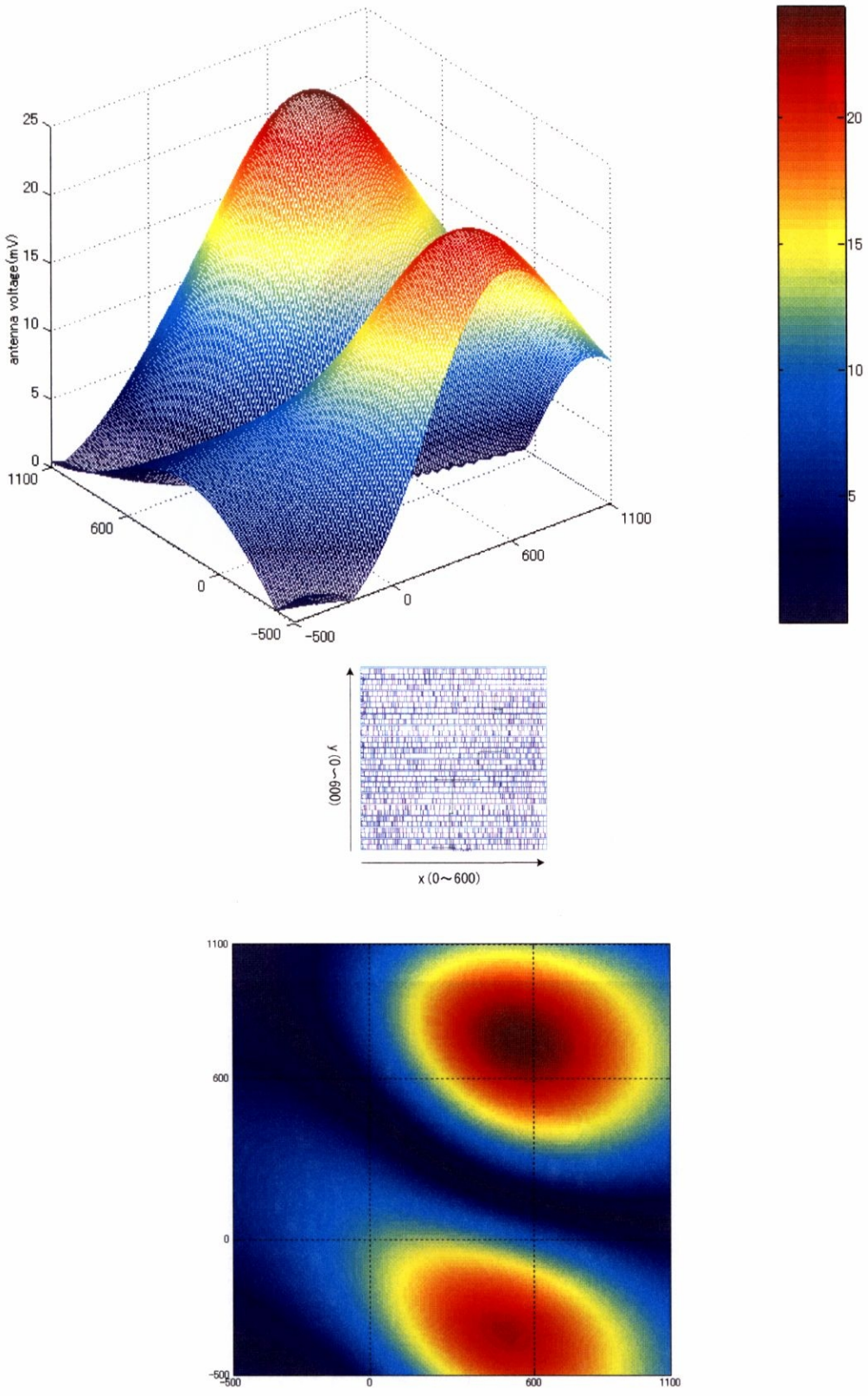


図 2.20 y 軸平行にアンテナを配置した場合のアンテナ空間電位差マップ

また、参考として注目配線からの電界・磁界強度は図 2.21、図 2.22 のようになっている。

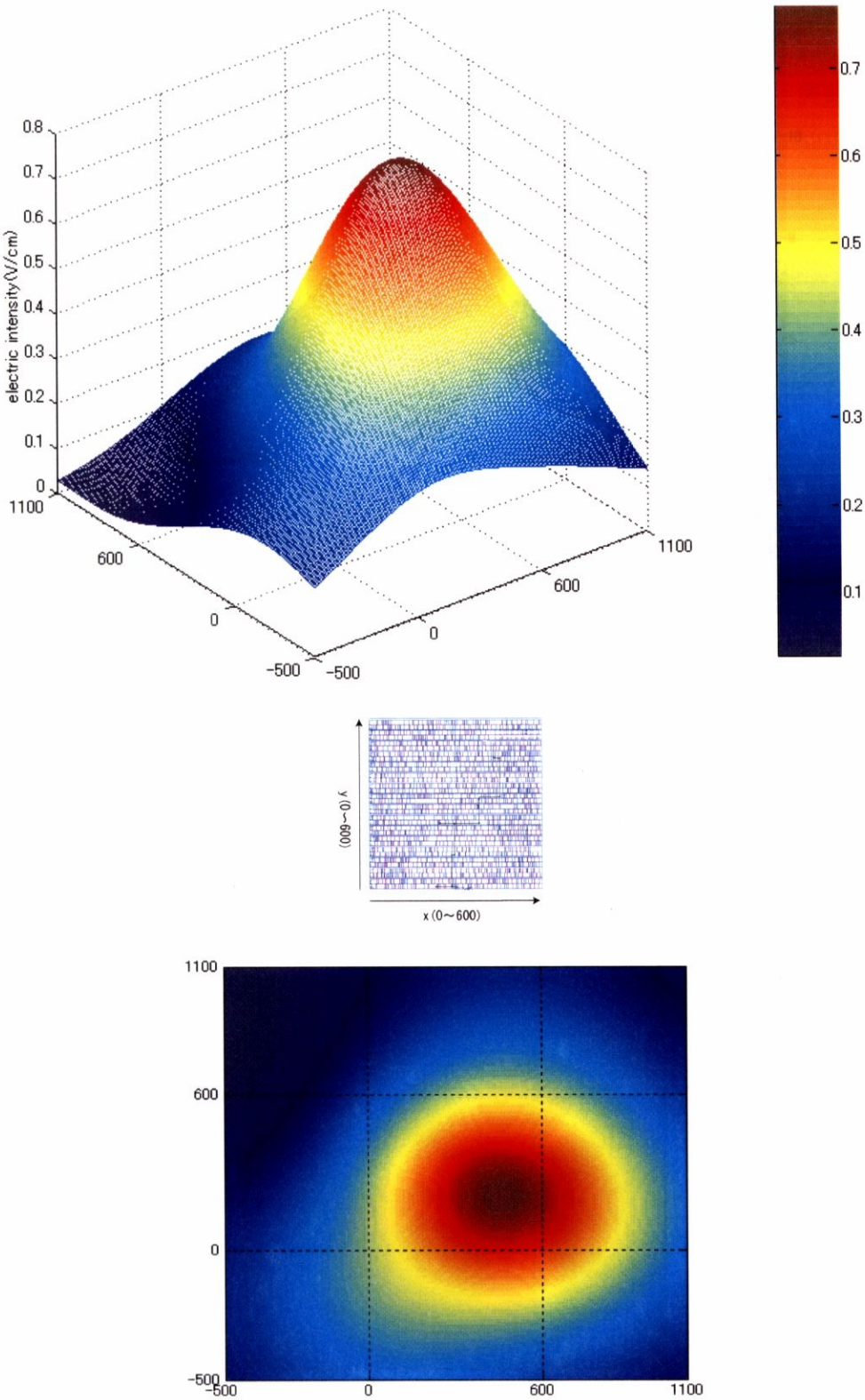


図 2.21 注目配線からの電界強度マップ

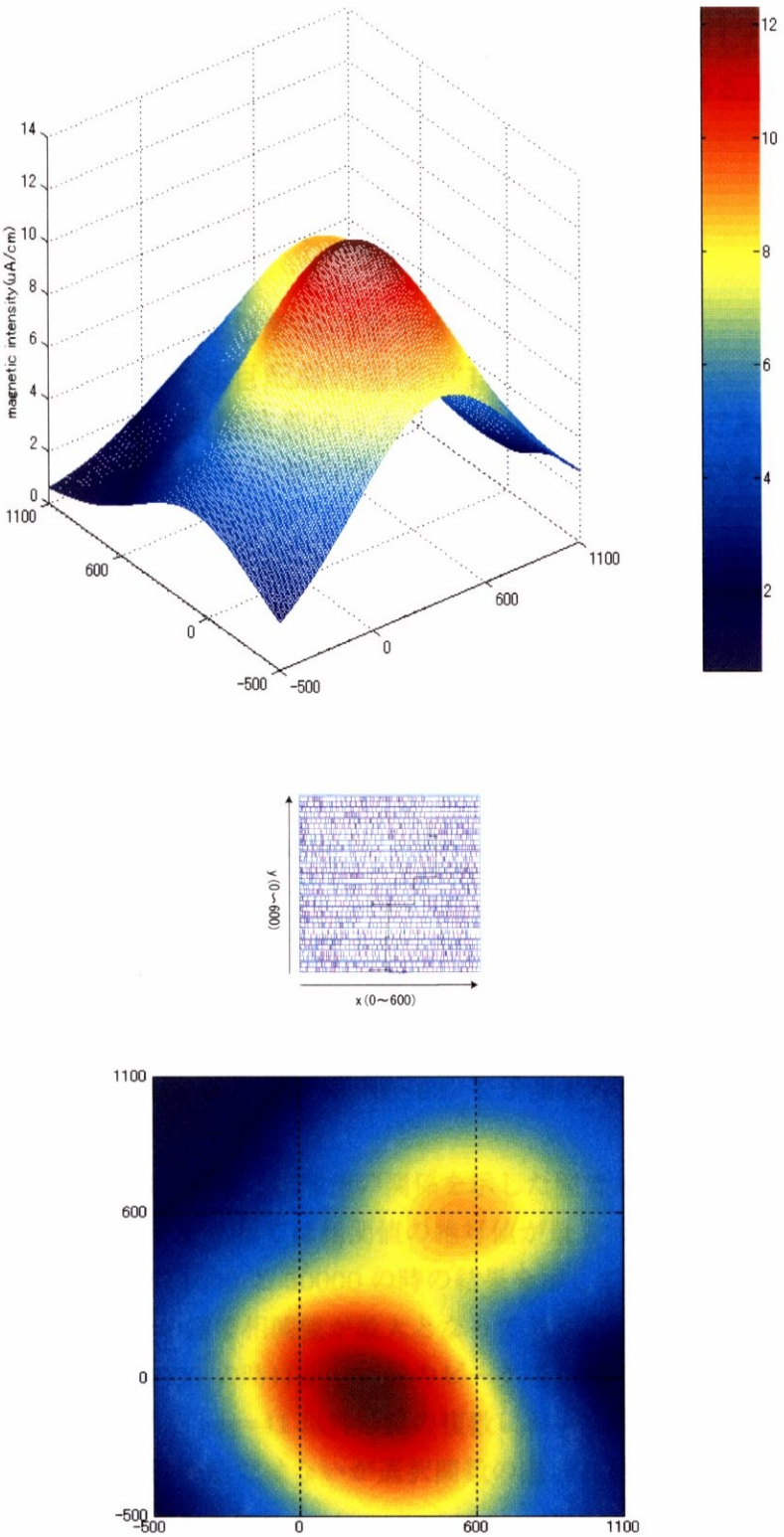


図 2.22 注目配線からの磁界強度マップ