

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2015 年 8 月 6 日(06.08.2015)



(10) 国際公開番号

WO 2015/114944 A1

- (51) 国際特許分類:
H04L 9/10 (2006.01)
- (21) 国際出願番号: PCT/JP2014/082010
- (22) 国際出願日: 2014 年 12 月 3 日(03.12.2014)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2014-018033 2014 年 1 月 31 日(31.01.2014) JP
- (71) 出願人: 国立大学法人東北大学(TOHOKU UNIVERSITY) [JP/JP]; 〒9808577 宮城県仙台市青葉区片平二丁目 1 番 1 号 Miyagi (JP). 国立大学法人神戸大学(NATIONAL UNIVERSITY CORPORATION KOBE UNIVERSITY) [JP/JP]; 〒6578501 兵庫県神戸市灘区六甲台町 1 番 1 号 Hyogo (JP).
- (72) 発明者: 三浦 典之(MIURA Noriyuki); 〒6578501 兵庫県神戸市灘区六甲台町 1 番 1 号 国立大学法人神戸大学内 Hyogo (JP). 本間 尚文(HOMMA

Naofumi); 〒9808577 宮城県仙台市青葉区片平二丁目 1 番 1 号 国立大学法人東北大学内 Miyagi (JP). 林 優一(HAYASHI Yuichi); 〒9808577 宮城県仙台市青葉区片平二丁目 1 番 1 号 国立大学法人東北大学内 Miyagi (JP). 青木 孝文(AOKI Takafumi); 〒9808577 宮城県仙台市青葉区片平二丁目 1 番 1 号 国立大学法人東北大学内 Miyagi (JP). 永田 真(NAGATA Makoto); 〒6578501 兵庫県神戸市灘区六甲台町 1 番 1 号 国立大学法人神戸大学内 Hyogo (JP).

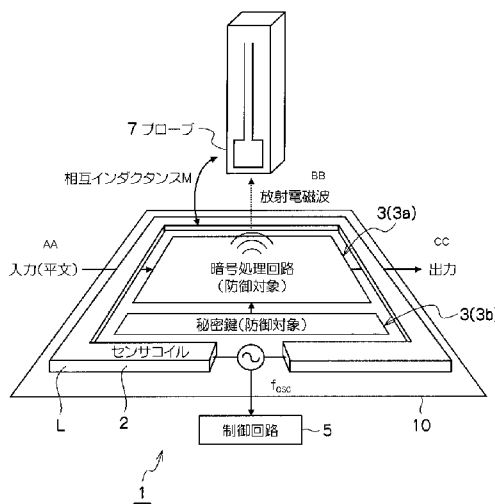
(74) 代理人: 特許業務法人 英知国際特許事務所(EI-CHI PATENT & TRADEMARK CORP.); 〒1120011 東京都文京区千石 4 丁目 4 5 番 1 3 号 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR,

[続葉有]

(54) Title: SIDE-CHANNEL ATTACK DETECTION DEVICE AND SIDE-CHANNEL ATTACK DETECTION METHOD BY SIDE-CHANNEL ATTACK DETECTION DEVICE

(54) 発明の名称: サイドチャネル攻撃の検知装置、サイドチャネル攻撃の検知装置によるサイドチャネル攻撃の検知方法



(57) Abstract: The objective of the invention is to provide a detection device wherein side-channel attacks can be detected by use of a simple structure. A side-channel attack detection device (1) comprises: a detection means (2) that has a capacitor or a coil (L) serving as an inductor placed in the proximity of an information processing device (3) such as a cipher processing circuit (3a) that is a target of a side-channel attack and that detects a change in inductance of the coil (L) (inductor) or in capacitance of the capacitor; and a determination means (control circuit (5)) that determines, on the basis of an output from the detection means (2), the approach of a probe (7) or the opening of an LSI package done by the side-channel attack.

(57) 要約: 簡単な構造で、サイドチャネル攻撃を検知することができる検知装置を提供すること。サイドチャネル攻撃の検知装置 1 は、サイドチャネル攻撃の対象となる暗号処理回路 3 a などの情報処理装置 3 に近接して配置されたインダクタとしてのコイル L またはキャパシタを有し、コイル L (インダクタ) のインダクタンスまたはキャパシタのキャパシタンスの変化を検知する検知手段 2 と、検知手段 2 の出力に基づいてサイドチャネル攻撃によるプローブ 7 の接近または L S I パッケージの開封を判定する判定手段 (制御回路 5) と、を有する。

- 2 Sensor coil
3(3a) Cipher processing circuit (target to be protected)
3(3b) Secret key (target to be protected)
5 Control circuit
7 Probe
M Mutual inductance
AA Input (plain text)
BB Radiated electromagnetic waves
CC Output



LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,

規則 4.17 に規定する申立て:

- 出願し及び特許を与えられる出願人の資格に関する申立て (規則 4.17(ii))

添付公開書類:

- 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称：

サイドチャネル攻撃の検知装置、サイドチャネル攻撃の検知装置によるサイドチャネル攻撃の検知方法

技術分野

[0001] 本発明は、サイドチャネル攻撃の検知装置、サイドチャネル攻撃の検知装置によるサイドチャネル攻撃の検知方法に関し、特に、暗号工学分野のうち、暗号ＬＳＩなどの情報処理装置に対するサイドチャネル攻撃の対策技術に関する。

背景技術

[0002] 情報通信機器の携帯が一般的となり、ネットワーク上でのプライバシー保護や高信頼な電子商取引の重要性がますます高まっている。暗号はそのような社会システムを構築する上で欠かすことのできない基盤技術であり、暗号アルゴリズムを実現したソフトウェアやハードウェアが動作する大規模集積回路（以下、暗号ＬＳＩと呼ぶ）は多くの民生品に搭載されている。暗号ＬＳＩには、通常、専門家により十分に安全性評価を行った暗号アルゴリズムが利用される。そのため、アルゴリズムの欠陥から暗号化前のデータ（平文）や秘密鍵などの漏洩の心配は（現在の計算機能力や知られている解読法の観点から）ほとんどない。

[0003] 一方、暗号ＬＳＩの実装上の脆弱性から現実的な時間で秘密情報を奪う実装攻撃の脅威が指摘されている。特に注目を集めているのが、暗号ＬＳＩの演算中の消費電力や放射電磁波、実行時間等といった本来の入出力以外の情報（サイドチャネル情報）を観察することで秘密情報を奪うサイドチャネル攻撃である。

[0004] サイドチャネル攻撃の中でも最もよく知られる攻撃が電力・電磁波解析攻撃である。１９９０年代後半にKocherらによって単純電力解析と差分電力解析が発表されたのを機に、その拡張が盛んに研究され始めた。その後、電力

の代わりに漏洩電磁波の波形を用いた電磁波解析攻撃が可能であることが示された。

電力解析攻撃や電磁波解析攻撃では、測定用プローブとデジタルオシロスコープを用いて暗号ＬＳＩから漏洩する電流・電圧の時間変化を計測する。計測した波形を計算機で加工・処理して暗号処理の内容や秘密鍵の値を推定する。

[0005] 特に、電磁波解析攻撃は、機器に直接プロービングしてＬＳＩ全体の過渡的な電圧変化を測定する電力解析と比べ、非接触な攻撃が可能となる。また、暗号ＬＳＩの局所的な特性を取得できることが報告されており、これまで電力解析の適用は難しいとされてきた機器に対しても脅威となる可能性が指摘されている。とりわけ、近年、一般的な暗号ＬＳＩの最小構成素子（ＡＮＤやＸＯＲ等の基本ゲート）の非対称性により、秘密情報を処理する部分の局所的な電磁波放射から原理的に秘密情報を取得できることが報告されている（例えば、非特許文献１参照）。

[0006] 従来のサイドチャネル攻撃への対策は、秘密情報と相関のある中間値をサイドチャネル情報として漏洩させないことを目的とし、主に乱数によって中間値を遮蔽するマスキングもしくは中間値を隠ぺいするハイディングという概念で実現されてきた。これまでアルゴリズムレベルやロジックレベル（デジタル回路レベル）で数多くのサイドチャネル攻撃への対策が提案されている（例えば、非特許文献２参照）。

先行技術文献

非特許文献

- [0007] 非特許文献１：T. Sugawara, et al., “On Measurable Side-Channel Leaks Inside ASIC Design Primitives,” Proc. CHES, pp.159-178, Aug. 2013.
- 非特許文献２：K. Tiri and et al., “Prototype IC with WDDL and differential routing - DPA resistance assessment,” CHES 2005, Lecture Notes in Computer Science, vol. 3659, pp. 354-365, May 2005.
- 非特許文献３：S. Mangard, E. Oswald, and T. Popp, “Power Analysis Att

acks - Revealing the Secrets of Smart Cards," Springer, 2007.

発明の概要

発明が解決しようとする課題

- [0008] しかしながら、上述した従来のアルゴリズムレベルやロジックレベル（デジタル回路レベル）でのサイドチャネル攻撃への対策では、ANDやXOR演算中の情報は漏洩しないことを前提としているため、その前提を覆す非特許文献1に記載されている攻撃に対しては原理的に対処できない。その前提を実現するためには基本演算素子の設計まで考慮したトランジスタレベルの対策が必要となるが、仮にそうした対策が実現できても、それは従来よりも設計難易度・コストを大幅に高める上に、暗号LSIの実行速度や消費電力、実装面積などを大きく増加させてしまう。
- [0009] 例えば、ロジックレベルのハイディング対策として知られるWDDL（Wave Dynamic Differential Logic）（非特許文献2参照）では、非特許文献1に記載されている攻撃に対処できない。さらに、同対策は少なくとも回路規模を数倍程度増加させることが知られている。
- [0010] アナログ回路レベルの対策として、暗号LSIの消費電力を内部動作状態に関わらず均一化する電源電流イコライザ（例えば、非特許文献3参照）も提案されており、それらは比較的lowオーバーヘッド（回路規模2倍程度の増加）で実現でき、電力解析攻撃には有効であるが、やはり非特許文献1に記載されているサイドチャネル攻撃には対処できない。
- [0011] 本発明は、このような問題に対処することを課題の一例とするものである。すなわち、簡単な構成で、サイドチャネル攻撃を検知可能な検知装置を提供すること、サイドチャネル攻撃の検知方法を提供すること、などを目的とする。

課題を解決するための手段

- [0012] このような目的を達成するために、本発明によるサイドチャネル攻撃の検知装置は、サイドチャネル攻撃の対象となる情報処理装置に近接して配置されたインダクタを有し、前記インダクタのインダクタンスの変化を検知する

検知手段と、前記検知手段の出力に基づいて前記サイドチャネル攻撃によるプローブの接近またはＬＳＩパッケージの開封を判定する判定手段と、を有することを特徴とする。

[0013] また、本発明に係るサイドチャネル攻撃の検知装置は、サイドチャネル攻撃の対象となる情報処理装置に近接して配置されたキャパシタを有し、前記キャパシタのキャパシタンスの変化を検知する検知手段と、前記検知手段の出力に基づいて前記サイドチャネル攻撃によるプローブの接近またはＬＳＩパッケージの開封を判定する判定手段と、を有することを特徴とする。

[0014] また、本発明のサイドチャネル攻撃の検知方法は、上記本発明に係るサイドチャネル攻撃の検知装置を用いて行われる。

発明の効果

[0015] 本発明によれば、簡単な構造で、サイドチャネル攻撃を検知可能な検知装置を提供することができる。また、本発明によれば、検知装置を用いることで簡単にサイドチャネル攻撃を検知することが可能なサイドチャネル攻撃の検知方法を提供することができる。

図面の簡単な説明

[0016] [図1]本発明の実施形態に係るサイドチャネル攻撃の検知装置を用いたサイドチャネル攻撃の検知方法の一例を示すフローチャート。

[図2]本発明の実施形態に係るサイドチャネル攻撃の検知装置の一例を示す図。

[図3]検知手段の発振器の発振周波数のシフトからサイドチャネル攻撃を検知する一例を示す図。

[図4]本発明の実施形態に係る検知装置の一例を示す図、（a）は検知装置の概念図、（b）は（a）に示した検知装置の一具体例を示す回路図。

[図5]2つのＬＣ発振器の周波数差によるサイドチャネル攻撃の検知の一例を説明する図。

[図6]検知装置と情報処理装置（暗号処理回路）の動作の一例を示すタイミングチャート、（a）は暗号処理回路の動作の一例を示す図、（b）はＬＣ発

振回路に関する信号の一例を示す図、（c）はリング発振回路に関する信号の一例を示す図。

[図7] LC発振器の発振周波数のばらつきを低減する較正回路の一例を示す図。

[図8]各発振器の発振周波数の各特性の一例を示す図、（a）はリング発振器の場合、（b）はLC発振器の場合。

[図9]較正動作の一例を説明するための図。

[図10]変換テーブル（ルックアップテーブル）の一例を示す図。

[図11]較正回路を用いたLC発振回路の発振周波数の較正動作の一例を示すフローチャート。

[図12]実測した各発振器の発振周波数の電源電圧と温度依存性の一例を示す図、（a）はリング発振器の場合、（b）はLC発振器（3巻き）の場合、（c）はLC発振器（4巻き）の場合。

[図13]周波数スペクトラムの一例を示す図、（a）は3巻コイルL2の場合（プローブ接近なし）、（b）は4巻コイルL1の場合（プローブ接近なし）、（c）は3巻コイルL2の場合（L1にプローブ接近あり）、（d）は4巻コイルL1の場合（L1にプローブ接近あり）。

[図14]サイドチャネル攻撃の検知による動作の一例を説明するための図、（a）、（b）は攻撃検知による動作切り替えなしの場合の電磁波の波形の一例、相関係数の一例をそれぞれ示す図、（c）、（d）は攻撃検知による動作切り替えありの場合の電磁波波形の一例、相関係数の一例をそれぞれ示す図。

[図15]本発明の他の実施形態に係るサイドチャネル攻撃の検知装置の一例を説明するための概念図。

[図16]伝達関数の一例を示す図、（a）はプローブが検知手段に接近していない場合の伝達関数の一例を示す図、（b）はプローブが検知手段に接近している場合の伝達関数の一例を示す図。

[図17]入力信号の電圧の周波数特性の一例を示す図。

発明を実施するための形態

- [0017] 本発明に係る検知装置は、サイドチャネル攻撃そのものを検知する。詳細には、本発明に係るサイドチャネル攻撃の検知装置は、サイドチャネル攻撃の対象となる情報処理装置に近接して配置されたインダクタまたはキャパシタを有し、インダクタ（コイル）のインダクタンスまたはキャパシタのキャパシタンスの変化を検知する検知手段を備え、その検知手段の出力に基づいてサイドチャネル攻撃によるプローブ（導電体などにより構成される）の接近またはLSIパッケージの開封などを判定する判定手段と、を有する。本発明に係る検知装置は、プローブの接近やLSIパッケージの開封時など、インダクタンスやキャパシタンスの変化を検知手段で検知し、判定手段にてサイドチャネル攻撃を容易に判定することができる。
- [0018] 従来のサイドチャネル攻撃への対策は、攻撃されていることを検知できないことが前提となっており、有意なサイドチャネル情報を漏洩させないことが目的となっていた。本発明に係る検知装置は、電磁気の物理法則に基づいてサイドチャネル攻撃を検知することができ、その攻撃を検知した場合、以降の暗号処理を停止・変更するなどの処理を行うことで、秘密情報の漏洩を防ぐ。
- [0019] また、検知装置は、例えば、情報処理装置としての暗号LSI（暗号アルゴリズムを実現したソフトウェアやハードウェアが動作する大規模集積回路）に対するサイドチャネル攻撃（暗号LSIの動作中に生じる副次的な情報（サイドチャネル情報）を観察することで秘密情報を奪う攻撃）を検知する。本発明に係る検知装置などの技術の実現にあたっては、集積回路工学と環境電磁工学の理論と技術などを応用している。
- [0020] また、サイドチャネル攻撃の手段としてのプローブが情報処理装置としての暗号LSI（暗号処理回路）などに接近している場合、本発明の実施形態に係る検知装置は、それをプローブによって生じるインダクタンスの変化として、電磁界の乱れ（それに伴う情報処理装置の近傍電磁界や回路内部の特性インピーダンスの変化、回路内部を流れる信号損失の発生などの電氣的パ

ラメータの変化)から検知可能であり、局所電磁波解析攻撃を含むプロービングによる電氣的情報を用いるサイドチャネル攻撃全般を防ぐ。上記電氣的パラメータの変化は、プローブと暗号LSIとの電界結合、磁界結合、もしくはその両方により生ずるため、これらを避けてプロービングを伴う攻撃を実行することは原理的に困難である。

[0021] 本発明の実施形態に係る検知装置の攻撃検知センサ部分(検知手段)は、後述するように、インダクタ(コイル)を含むLC発振器などの簡便な回路で実現可能であり、センシング後段の処理回路を含めても対策対象となる暗号LSI(情報処理装置)に対して僅か数パーセントという面積オーバーヘッドで実現できる。

[0022] 環境電磁工学の分野では、集積回路内部やプリント基板上の配線パターン近傍から放射される電磁界に測定用プローブを接近配置すると、電磁界分布に変化が生じる物理現象がよく知られている。検知装置は、この物理現象を応用して、攻撃時にプローブが暗号LSIに接近する際に生じる電磁界の乱れをサイドチャネル攻撃の検知に用いる。攻撃検知後に秘密情報を保護する処理(例えば暗号処理の停止やダミー演算の挿入など動作モードを切り替える処理)で秘密情報の漏洩を防ぐことができる。

[0023] 図1は本発明の実施形態に係るサイドチャネル攻撃の検知装置を用いたサイドチャネル攻撃の検知方法の一例を示すフローチャートである。図2は本発明の実施形態に係るサイドチャネル攻撃の検知装置1の一例を示す図である。

[0024] 図2に示した例では、集積回路チップ10に、サイドチャネル攻撃の対象であり、防御対象の情報処理装置3である暗号処理回路3aや防御対象としての秘密鍵を記憶する記憶回路3bなどが形成されている。

検知装置1は、サイドチャネル攻撃を検知する検知手段2を有する。検知手段2としては、例えば、コイルL(インダクタ)を含むLC発振器などを採用することができ、集積回路チップ10などに形成されている。つまり、情報処理装置3と検知手段2は、同一の集積回路チップ10に設けられてい

る。本実施形態では、LC発振器のコイルL（インダクタ）は、情報処理装置3と一体もしくは情報処理装置3の近傍に配置されている。図2に示した例では、防御対象の情報処理装置3である暗号処理回路3aの周囲を囲むように、検知手段2であるLC発振器のコイルLが形成されている。

[0025] また、検知装置1は、検知手段2の出力に基づいて、サイドチャネル攻撃によるプローブの接近やLSIパッケージの開封を判定する判定手段としての制御回路5などを有し、制御回路5は、サイドチャネル攻撃を検知した場合に情報漏洩を防止する所定の処理などを行う。この判定手段としての制御回路5は、集積回路チップ10に形成されている。尚、制御回路5は、別の集積回路チップに形成されていてもよい。

[0026] 図3は、検知手段としてのLC発振器の発振周波数のシフトからサイドチャネル攻撃を検知する一例を示す図である。詳細には、図3は検知手段としてのLC発振器の周波数スペクトラムの一例を示し、横軸に発振周波数を示し、縦軸に各周波数成分の大きさを示す。

[0027] 電磁プローブ（プローブ）の接近により、コイルLの等価インダクタンスが変化する。このインダクタンスの変化に伴うLC発振器の発振周波数 f_{osc} のシフトに基づいて、サイドチャネル攻撃を検知する。

詳細には、プローブ7が情報処理装置3の近傍に配置された検知手段2に接近していない場合（P1）、検知手段2としてのLC発振器の発振周波数 f_{osc} は近似的に数式（1）に示すようになり、プローブ7が検知手段2に接近した場合（P2）、LC発振器の発振周波数 f_{osc} はプローブ7とコイルLとの間の相互インダクタンスMにより、近似的に数式（2）に示すようになる。プローブ7の接近により相互インダクタンスMが大きくなり、発振周波数 f_{osc} が大きくなる。つまり、検知手段2により取得されたLC発振器の発振周波数 f_{osc} が大きくシフトするなどし、予め規定された閾値を超えたか否かに基づいて、制御回路5がプローブ7の接近を検知することが可能である。プローブ7の接近を検知した場合、制御回路5は暗号処理回路の動作モードを、例えば、暗号化停止処理やダミー鍵を用いた処理などに切り替えるこ

とで、秘密情報などの漏洩を回避する。

[0028] [数1]

$$f_{osc} \approx \frac{1}{2\pi\sqrt{LC}} \quad \dots (1)$$

$$f_{osc} \approx \frac{1}{2\pi\sqrt{(L-M)C}} \quad \dots (2)$$

[0029] 次に、サイドチャネル攻撃の検知動作の一例について説明する。

ステップS T 1において、攻撃検知センサであるコイルLを含むLC発振器などの検知手段2を起動する。ここで、起動する検知手段2は、防御対象となる暗号処理回路3 aなどと一体もしくはその近傍に設置され、任意の方向から暗号処理回路3 aなどに接近するもしくはあらかじめ接近しているプローブ7によって生じるコイルL（インダクタ）のインダクタンスの変化、詳細には、電磁界の乱れ（それに伴う近傍電磁界や回路内部の特性インピーダンスの変化、回路内部を流れる信号損失の発生など）を観測可能とする。例えば、情報処理装置3として暗号処理回路3 aなどを採用した場合、検知手段2としてのセンサは当該回路の内部に実装されるように構成してもよい。

[0030] ステップS T 2において、検知手段2としてのセンサを用いて、コイルL（インダクタ）のインダクタンスの変化、詳細には、電磁界の乱れなど、センサと周囲との電磁界結合度の変化（もしくはそれに伴う物理量）を取得する。例えば、検知手段2を、コイルL（インダクタ）を含むLC発振器で実現した場合、センサと周囲との電磁界結合度の変化はLC発振器の発振周波数の変化として得られる。つまり、検知手段2は、コイルL（インダクタ）のインダクタンスの変化を、LC発振器の発振周波数の変化により検知している。さらに、センサを複数の形状・巻き数の異なるコイルにより構成すれば、電磁界結合度の変化は各コイルの発振周波数の相対的な変化として得られる。このとき、絶対的な周波数基準が不要となり、相対的に大きな基準周波数発生回路を省略できるだけでなく、周波数基準を悪用する攻撃の危険性を排除できる。

[0031] ステップS T 3において、検知手段2により、プローブの接近やパッケージの開封によるコイルのインダクタンスの変化を検知したか否かを、詳細には、電磁界の乱れなど、電磁界結合度の変化を観測したか否かを判定手段としての制御回路5（制御部）などが判定する。詳細には、制御回路5は、例えば、検知手段2をコイルLを含むLC発振器（コイル）で実現した場合、コイルLの発振周波数の変化、つまりコイルLのインダクタンスの変化により判定する。これが変化している場合にはステップS T 4の処理に進み、変化していない場合にはステップS T 5の処理に進む。

[0032] ステップS T 4において、検知手段2により上記変化が観測された場合、制御回路5は攻撃検知信号を出力する。ここでは、制御回路5が暗号処理回路3 aなどに攻撃検知信号を出力した場合、暗号処理回路3 aは秘密情報を保護する動作モード（停止やダミー演算の実行、ハイディング処理、マスキング処理）などに切り替える処理を行う。

尚、制御回路5は、秘密情報を保護する動作モードに切り替える処理として、少なくとも、偽の鍵を用いた暗号処理、鍵の変更処理、暗号処理に関わる情報（例えば、少なくとも、鍵、データ、回路情報のいずれかを含む）を消去する処理、検知したことを外部に通知する処理、のいずれかを行ってもよい。

[0033] ステップS T 5において、検知手段2としてのセンサにより上記変化が観測されなかった場合、防御対象となる暗号処理回路などの暗号化処理が終了するまでステップS T 2，S T 3の処理を適宜繰り返す。

[0034] 図1に示した処理の頻度は防御する対象に応じて変更する。例えば、単純解析の対象となる公開鍵暗号処理の場合、各鍵ビットの演算が行われる間隔で処理（ステップS T 2，S T 3）を繰り返す。差分解析の対象となる共通鍵暗号処理の場合、暗号処理の直前に一度だけ処理（ステップS T 2，S T 3）を行う。

[0035] <複数のLC発振器を攻撃検知センサとして用いた検知装置>

図4は本発明の実施形態に係る検知装置1の一例を示す図である。詳細に

は、図4（a）は複数のLC発振器を有する検知装置1の概念図、図4（b）は図4（a）に示した検知装置1の一具体例を示す回路図である。検知手段2は、複数のLC発振器（発振回路）を備えていてもよい。以下、検知手段2として2つのLC発振器を備えた検知装置1を説明する。

[0036] 詳細には、検知装置1は、情報処理装置3としての暗号処理回路3a上またはその近傍に配置されたコイルL1、コイルL2を有する。また、検知装置1は、コイルL1、L2をそれぞれ備えた発振器51（LC発振器を含む）、発振器52（LC発振器を含む）、およびセンサコア回路50を有する。例えば、暗号処理回路3aの秘密情報処理部3c、3dなどの秘密情報を処理する機能ブロック（S-BOXやレジスタ等）は、それぞれコイルL1、L2の直下に配置し、それ以外の鍵情報を含まない機能ブロック（I/Oインタフェース等）をコイルL1、L2間に配置する。

[0037] センサコア回路50は、例えば、制御回路5（制御部）と、コイルL1用の発振器51（発振回路）、コイルL2用の発振器52（発振回路）を有する。各発振器51、52のコイルL1、L2は上述したように、秘密情報処理部3c、3dの近傍に配置されている。詳細には、検知手段は、少なくともコイルL1（センサコイル）、コイルL2（センサコイル）などのコイルを有する。本実施形態では、検知手段は、コイルL1、L2などのコイル、センサコア回路50（制御回路5（制御部）、発振器51、52などの発振器、校正回路、リング発振器等）、などを有する。

[0038] コイルL1、L2は、例えば、直交する辺を異なる配線層でレイアウトすることで、各コイル下に配置される暗号処理回路3aのデジタル信号配線を妨害しないように構成されている（例えば、非特許文献参照：M. Saito, et al., “An Extended XY Coil for Noise Reduction in Inductive-coupling Link,” A-SSCC Dig. Tech. Papers, pp.305-308, Nov. 2009.）。

[0039] コイルL1、L2に必要なリソースは、数10トラック程度の配線リソースのみである。

検知手段2としての2つのコイルL1、L2は、巻き数や直径等の形状が

同じであってもよいし、異なるものを用いてもよい。

本実施形態では、検知手段2としての2つのコイルL1, L2は、巻き数や直径等の形状の異なるものを用いる。例えば、サイドチャネル攻撃時にプローブを用いて秘密情報を取得するためには、2つのコイルL1, L2のいずれか一方もしくは両方に接近させる必要がある。プローブが接近した場合、2つの発振器51, 52 (LC発振器) の発振周波数に差が生じる。ここで、2つのコイルL1, L2の巻き数・形状が異なるため、コイルL1, L2にまたがったプローブの接近 (一般的な電磁波解析攻撃) や個々のコイルL1, L2に対して同一のプローブが同時に接近 (複数のプローブによる電磁波解析攻撃) した場合であっても、各発振器51, 52 (LC発振器) の発振周波数に差が生じることに注意されたい。

[0040] コイルL1, L2以外のセンサコア回路50は、完全デジタル回路で構成されている。LC発振器のコアは、電源スイッチ付きのCMOSインバータなどで構成されている。詳細には、発振器51 (LC発振回路) は、コイルL1 (インダクタ) を除きロジック回路で構成されている。

発振器51が形成された集積回路は、複数のトランジスタT1~T3, T11~T1a, T1b~T1n, T21~T2a, T2b~Tbn、インバータN1~N8, N11~N14、NANDゲートD1, D11などを有し、図4 (b) に示したように各構成要素が接続されている。

本実施形態では、例えば、MOS型電界トランジスタのキャパシタとコイルL1を用いて発振器51 (8L) を構成している。発振器51 (LC発振器) の発振周波数は、予め規定された周波数となるように設定されており、各トランジスタT11~T1a, T1b~T1n, T21~T2a, T2b~Tbnの接続を切り替えることにより、発振周波数の微調整を行うことができるように構成されている。

[0041] リング発振器8Rは、図4 (b) に示したように、インバータN11~N14、NANDゲートD11により構成されている。このリング発振器8Rは、発振器51のLC発振器8Lの発振周波数を較正する際に用いられる。

[0042] 発振器 5 2 (LC 発振器を含む) は、上述した発振器 5 1 と略同様な構造であり、コイル L 1 をコイル L 2 と読み替えた構造であるので、説明を省略する。つまり、発振器 5 2 は、LC 発振器、リング発振器などを有する。

[0043] 図 5 は 2 つの LC 発振器の周波数差によるサイドチャネル攻撃の検知の一例を説明する図である。詳細には、コイル L 1 を有する LC 発振器の発振周波数と、コイル L 2 を有する LC 発振器の発振周波数を図 5 に示す。図 5 において、横軸に検知手段 (センサ) としてのコイル L 1, L 2 とプローブとの距離を示し、縦軸に発振周波数を示す。

[0044] 図 5 に示した例では、サイドチャネル攻撃によるプローブがコイル L 1, L 2 から離れている場合、各 LC 発振器の発振周波数は、閾値 f_{th} より小さい同じ値を示すとする。尚、各 LC 発振器の発振周波数は異なる値を示していてもよい。

[0045] 例えば、プローブがコイル L 2 に近づいた場合、コイル L 1 を有する LC 発振器の発振周波数は僅かに上昇し、コイル L 2 を有する LC 発振器の発振周波数は閾値 f_{th} より大きい値を示す。また、プローブがコイル L 1 に近づいた場合、コイル L 1 を有する LC 発振器の発振周波数が閾値 f_{th} より大きい値を示すことになる。

上述したように、検知手段としてコイル L 1, L 2 を用いた場合、コイル L 1, L 2 の一方または両方に近づいたことを、各 LC 発振器の発振周波数に基づいて容易に検知することができる。

[0046] 尚、各発振器 5 1, 5 2 (LC 発振器) の発振周波数差は制御回路内のカウンタで計測される。本発明の実施形態に係る検知装置は、検知手段として発振器 5 1, 5 2 (LC 発振器) の発振周波数差を利用しており、クロックを周波数基準として使用しないため、システムクロックを含む外部入力のクロック源が攻撃者によって任意に変更される攻撃に対して耐性を有する。また、面積と電力の大きいオンチップの高精度な周波数基準発生回路 (バンドギャップリファレンスなどのアナログ回路) も不要となる。物理サイズを考慮すると困難ではあるが、万が一、2 つの電磁プローブで 2 つのコイルを同

時に攻撃しても、コイル形状が異なるため、両コイルの周波数シフト量を長時間一定に保つのは極めて困難である（攻撃には数時間かかる）。

[0047] 図6は検知装置と情報処理装置（暗号処理回路）の動作の一例を示すタイミングチャートである。詳細には、図6（a）は暗号処理回路の動作の一例を示す図、図6（b）はLC発振回路に関する信号LOenの一例を示す図、図6（c）はリング発振回路に関する信号ROenの一例を示す図である。

[0048] 本実施形態に係る検知装置は、検知手段としてのLC発振回路を、図6に示すように、暗号処理の動作前後に間欠起動することで、プローブの接近をモニタする。動作間隔は守るべき暗号アルゴリズムに応じて適宜設定することができる。

図6に示した例では、トリガ信号LOenによってLC発振器は、起動時に即座にフルスイング（設定振幅）の安定発振を行うことができる。トリガ信号ROenによりリング発振器は所定の発振周波数で発振を行う。後述するように、本発明の実施形態に係る検知装置は、リング発振器による発振周波数とLC発振器による発振周波数に基づいて、LC発振器の周波数を較正する。

サイドチャネル攻撃の検知に必要な時間は、 $1\mu\text{s}$ 以下であり、I/Oを含む暗号処理時間（ $\sim 100\mu\text{s}$ ）の1%以下の動作時間に抑えることができるため、消費電力のオーバーヘッドを著しく低減できる。

LC発振器は、暗号処理動作の停止中に起動するように制御回路により制御されるので、コイルからの放射電磁界により暗号情報が漏洩することはない。また、LC発振器と暗号処理回路の間の干渉は非常に小さい。

[0049] <較正>

図7はLC発振器の発振周波数のばらつきを低減する較正回路の一例を示す図である。

本発明の実施形態に係るサイドチャネル攻撃の検知装置は、検知手段による検知精度を向上させるために、LC発振器の発振周波数のPVT（プロセ

ス、電圧、温度)ばらつきを低減する機構を有する。詳細には、ローカルにリング発振器を搭載し、PVTばらつきに応じてLC発振周波数を適応的に較正する。詳細には、集積回路チップに形成されたセンサコア回路内にリング発振器8Rが設けられている。例えば、較正回路55は、制御回路5(制御部)などに形成されている。

較正回路55には、LC発振器8L、リング発振器8Rがそれぞれカウンタ57a(57)、57b(57)を介して接続されている。カウンタ57a(57)はLC発振器8Lによる発振周波数を計測し、信号Loclk(#Loclk)を較正回路55に出力する。カウンタ57b(57)はリング発振器8Rによる発振周波数を計測し、デジタル信号Rock(#Rock)を較正回路55に出力する。

[0050] 図8は各発振器の発振周波数の各特性の一例を示す図である。詳細には、図8(a)はリング発振器の場合、図8(b)はLC発振器の場合をそれぞれ示す。図9は、較正動作の一例を説明するための図である。図8(a)、図8(b)、図9において、横軸に供給電圧 V_{DD} [V]を示し、縦軸に発振周波数のシフト割合[%]を示す。図8において、FF、TT、SSの各左側はNMOSの特性を示し、右側はPMOSの特性を示す。F(Fast)は、トランジスタがオンしやすいことを示し、S(slow)は、トランジスタがオンし難いことを示し、T(Typical)は、設計通りであることを示す。図9において、供給電圧の増加により発振周波数のシフト割合が増加する曲線はリング発振器の特性を示し、供給電圧の増加により発振周波数のシフト割合が減少する曲線はLC発振器の特性を示し、略一定値を示す直線は較正曲線を示す。

図10は変換テーブル(ルックアップテーブル:LUT)の一例を示す図である。図10において、横軸に較正のための周波数、縦軸に容量値を示す。

[0051] 検知手段としてのセンサに使用するLC発振器には、正の温度係数を持つバラクタダイオード型のキャパシタを使用せずに較正用の小さなMOSキャ

パシタ（同様に正の温度係数を持つが、温度係数はバラクタダイオードよりも小さい）のみを接続した。このときLC発振器の発振周波数のPVTばらつきは、CMOSインバータのトランジスタの g_m に反比例する特性となり、リング発振器の周波数に対して単調な逆特性を有する（図8、図9参照）。尚、図8、図9のグラフには記載していないがSF/FSコーナーにおいても同様である。この特性を利用することで、LC発振器8L、リング発振器8Rの発振周波数をカウントするためのカウンタ57a（57）、57b（57）と小サイズのLUT（図10参照）を用いて、LC発振器の発振周波数をワンステップでデジタル較正を行うことができる。

[0052] 図11は較正回路を用いたLC発振回路の発振周波数の較正動作の一例を示すフローチャートである。次に、LC発振器の発振周波数を較正する方法の一例を、図4、図7～図11などを参照しながら説明する。

[0053] ステップST11において、較正回路55を含む制御回路5は、リング発振器8R、LC発振器8L、およびカウンタ57a、57bを起動させる。

カウンタ57aはLC発振器8Lの発振周波数を測定し、カウンタ57bはリング発振器8Rの発振周波数を測定する。詳細には、カウンタ57aはLC発振器8Lのクロック数をカウントし、カウンタ57bはリング発振器8Rのクロック数をカウントする。

[0054] 較正回路55は、カウンタ57a、57bのいずれか一方がフルカウント（設定値）になった時点で、他方のカウンタのカウント値を読み出し、それに応じて較正值を増減する。較正回路55は、予め記憶回路などに記憶されているLUT（図10）を参照して、得られた較正值に基づいてLC発振器8Lの容量値（ ΔC ）に変換し、LC発振器8Lの発振周波数を較正する。

[0055] 詳細には、ステップST12において、較正回路55は、カウンタ57a、57bによりカウントされる計測値のいずれか一方がフルカウント（設定値）になったか否かを判別し、カウンタ57b（リング発振器用）のカウント値（#Clock）がフルカウントになった場合、ステップST13の処理に進み、カウンタ57a（LC発振器8L用）のカウント値（#Locl

k) がフルカウントになった場合、ステップ S T 2 3 の処理に進む。

[0056] ステップ S T 1 3 において、較正回路 5 5 は、カウンタ 5 7 a (L C 発振器用) によるカウント値 (# L O c l k) を読み込む。このカウント値は、リング発振器の発振周波数と L O 発振器の発振周波数の差に対応する。

[0057] ステップ S T 1 4 において、カウンタ 5 7 a (L C 発振器用) によるカウント値 (# L O c l k) に基づいて、L C 発振器の発振周波数が設定値となるように、較正値を減少させる処理を行う。

[0058] ステップ S T 1 5 において、較正回路 5 5 は、L U T (図 1 0 参照) を参照して、較正値 (Δf に対応) から、L C 発振器の容量値 ΔC に変換する処理を行い、ステップ S T 1 6 の処理に進む。

[0059] ステップ S T 1 6 において、較正回路 5 5 は、容量値 ΔC に基づいて L C 発振器 8 L の容量を減少させて、発振周波数を較正する。詳細には、較正回路 5 5 は、信号 CalCode を L C 発振器 8 L に出力し、図 4 (b) に示したトランジスタ T 2 1 ~ T 2 a, T 2 b ~ T 2 n それぞれを信号 CalCode に応じてオン接続またはオフ状態とし、トランジスタ T 1 1 ~ T 1 a, T 1 b ~ T 1 n による M O S キャパシタの容量値を調整することで、L C 発振器 8 L の発振周波数を較正する。

[0060] ステップ S T 2 3 において、カウンタ 5 7 a (L C 発振器 8 L 用) のカウント値 (# L O c l k) がフルカウントになった場合 (ステップ S T 1 2)、較正回路 5 5 は、カウンタ 5 7 b (リング発振器用) によるカウント値 (# R O c l k) を読み込む。このカウント値は、リング発振器の発振周波数と L O 発振器の発振周波数の差に対応する。

[0061] ステップ S T 2 4 において、カウンタ 5 7 b (リング発振器用) によるカウント値 (# R O c l k) に基づいて、L O 発振器の発振周波数が設定値となるように、較正値を増加させる処理を行い、ステップ S T 1 5 の処理に進む。

[0062] ステップ S T 1 5 において、較正回路 5 5 は、L U T (図 1 0 参照) を参照して、較正値 (Δf に対応) から、L C 発振器の容量値 ΔC に変換する処

理を行い、ステップS T 2 6 の処理に進む。

[0063] ステップS T 2 6 において、較正回路5 5 は、容量値 ΔC に基づいてL C 発振器8 L の容量を増加させて、発振周波数を較正する。

[0064] ここで、サイドチャネル攻撃の検知手段と同様に、較正回路5 5 はL C 発振回路とリング発振回路の周波数差を利用しているため、他の周波数基準は不要であることに注意されたい。つまり、較正回路5 5 による較正処理は、システムクロックを含む外部入力のクロック源が攻撃者によって任意に変更される攻撃に対して耐性を有する。

また、上述した較正回路5 5 を用いたL C 発振器の発振周波数の較正方法は、設計段階であらかじめ設定されたL U T（変換テーブル）に従って容量を調整して、L C 発振器の発振周波数のP V Tばらつき成分のみを補正するものであり、プローブの接近に伴うインダクタンスの変化による発振周波数の変化分については、較正後もそのまま残る。

したがって、仮に電源投入前に、プローブを接近させていたとしても、電源投入・較正後に仕様上の発振周波数（設計段階で決定される）と観測された発振周波数との差により正しく攻撃検知が可能である。

[0065] また、図8，図9に示したように、リング発振器の電圧特性と、L C 発振器の電圧特性が逆特性となっており、図9に示したように、交点を通る一定値となるように上記較正を行う。つまり、L C 発振器の発振周波数の電圧依存性を小さくするように較正を行う。

供給電圧が比較的高い場合、リング発振器の発振周波数がL C 発振器の発振周波数よりも高くなり、その周波数差に基づいて、L C 発振器の発振周波数を較正する。また、供給電圧が比較的低い場合、リング発振器の発振周波数がL C 発振器の発振周波数よりも低くなり、その周波数差に基づいて、L C 発振器の発振周波数を較正する。このように、リング発振器の発振周波数とL C 発振器の発振周波数の差により、供給電圧が基準の電圧よりも低いまたは高いことを判断することができ、そうした場合であっても、L C 発振器の発振周波数を確実に較正することができる。

[0066] また、図 8、図 9 に示したように、リング発振器の温度特性と、LC 発振器の温度特性が逆特性となっており、図 9 に示したように、交点を通る一定値となるように上記較正を行う。詳細には、リング発振器は温度が高くなると、発振周波数が低くなり、LC 発振器は温度が高くなると発振周波数が高くなる。図 9 に示したように、例えば、温度が高くなった場合であっても、交点を通る略一定値の較正用曲線が僅かに高くなる程度である。このため、温度が変化した場合であっても、較正の誤差を非常に小さくすることができる。つまり、リング発振回路と LC 発振回路の温度依存性が逆特性なので、電圧依存性を補正するときに、温度の変動によるドリフトを少なくすることができる。

[0067] また、図 8 に示したように、リング発振器および LC 発振器のプロセスばらつき特性が逆特性となっており、同様に、プロセスのばらつきがある場合であっても、較正の誤差を非常に小さくすることができる。

[0068] <実験・検証>

本願発明者は、本願発明に係る検知装置の効果を確認するために、図 4 に示したような情報処理装置 3 としての暗号処理回路 3a を有する集積回路のチップ上に、コイル L1、コイル L2、センサコア回路 50、つまり、コイル L1 を有する LC 発振器、コイル L2 を有する LC 発振器、制御回路 5 などの回路を、0.18 μm CMOS テクノロジーの LSI として作製した。

[0069] 検知手段としてのコイル L1 は 4 巻き、コイル L2 は 3 巻きである。コイル L1 は、縦 285 μm × 横 400 μm の矩形形状であり、コイル L2 は縦 285 μm × 横 480 μm の矩形形状である。

[0070] この本発明に係る検知装置を有する LSI を搭載した評価ボードをサイドチャネル攻撃標準評価基板 (SASEB0 R-II) に搭載し、マイクロマニピュレータで固定した極小電磁プローブを、検知装置を有する LSI に接近させた。

[0071] プローブからの EM 信号は、100W のパワーアンプで増幅した後、オシロスコープを介してコンピュータ (PC) に波形を取り込み、コンピュータにて相関計算を行って、局所 EM 解析攻撃を行った。

[0072] まず、LC発振器のデジタル校正を評価した。

図12は実測した各発振器の発振周波数の電源電圧と温度依存性の一例を示す図である。詳細には、図12(a)はリング発振器の場合、図12(b)はLC発振器(3巻き)の場合、図12(c)はLC発振器(4巻き)の場合をそれぞれ示す図である。

[0073] リング発振器とLC発振器(3巻き、4巻き)の間にPVTばらつきに対する逆特性を確認した。本願発明者は、上述したデジタル校正を行ったところ、±10%の電源電圧変動範囲と0~60℃の温度変化範囲において、周波数ばらつきを±1%以下に抑えることができた。

[0074] 次に、本発明に係る検知装置によるサイドチャネル攻撃の検知機能を評価した。

図13は周波数スペクトラムの一例を示す図である。詳細には、図13(a)は3巻コイルL2の場合(プローブ接近なし)、図13(b)は4巻コイルL1の場合(プローブ接近なし)、図13(c)は3巻コイルL2の場合(L1にプローブ接近あり)、図13(d)は4巻コイルL1の場合(L1にプローブ接近あり)、をそれぞれ示す。

[0075] 極小電磁プローブ(プローブ)を4巻きコイルL1(センサコイル)に接近させたところ、5.2%発振周波数がシフトし、図13に示したように、正常に攻撃検知ができることを確認した。

[0076] 図14は、サイドチャネル攻撃の検知による動作の一例を説明するための図である。詳細には図14(a)、図14(b)は攻撃検知による動作切り替えなしの場合の電磁波の波形の一例、相関係数の一例をそれぞれ示す図であり、図14(c)、図14(d)は攻撃検知による動作切り替えありの場合の電磁波波形の一例、相関係数の一例をそれぞれ示す図である。

[0077] 制御回路(制御部)は、サイドチャネル攻撃の検知装置による攻撃検知後、暗号処理回路に、停止やダミー演算の実行などの漏洩防止処理を行う動作を行わせることで、鍵情報の漏洩を防げることも実測により確認することができた。詳細には、図14に示したように、相関係数に基づいた正解鍵の検

出を防止することができた。

[0078] 表 1 に、本発明に係るサイドチャネル攻撃の検知装置の機能と、暗号処理回路（１ラウンド／１クロックのループアーキテクチャに基づくＡＥＳ暗号回路）に対する搭載時の面積、電力、性能オーバーヘッドを記載する。

本発明に係るサイドチャネル攻撃の検知装置（本対策回路）は、２．４％の面積と１％の電力と性能のわずかなオーバーヘッドで、従来の対策では防ぐことが困難な局所的な電磁波解析攻撃に対する耐性を実現できる。

[0079] また、本発明に係るサイドチャネル攻撃の検知装置は、ハイディングやマスキングなどの先行するサイドチャネル攻撃対策とも組み合わせ可能であり、相補的に組み合わせることにより、より堅牢なセキュリティを有する暗号処理回路を実現できる。

[0080] [表1]

	暗号処理回路 (AES暗号化回路)	本対策回路	全体 (対策による オーバーヘッド)
レイアウト面積	0.573mm ²	0.009mm ²	0.582mm ² (+1.6%)
性能	125μs/暗号化	0.3μs/センス	125.3μs (-0.2%)
消費電力	225μW	17μW	242μW (+7.6%)
回路プロセス	0.18μm Standard Logic CMOS		

[0081] <本発明の他の実施形態>

上記実施形態に係るサイドチャネル攻撃の検知装置は、図 2、図 4 などに示したように、検知手段としてコイル（インダクタ）を備えた LC 発振器を採用し、導電体などにより構成されるプローブなどの接近によるインダクタンス（相互インダクタンス）の変化に応じた発振周波数の変化や、暗号処理回路などの情報処理装置を含む LSI のパッケージ（導電体や樹脂などにより構成される）の開封によるインダクタンス（相互インダクタンス）の変化に応じた発振周波数の変化に基づいて判定手段としての制御回路がサイドチ

チャンネル攻撃によるプローブの接近やLSIパッケージの開封などを判定したが、この形態に限られるものではない。

[0082] 例えば、本発明に係る検知装置は、プローブなどの接近によるキャパシタンス（相互キャパシタンス）の変化に基づいて、上述したように、プローブなどを検知する検知手段と、その検知手段の出力に基づいてサイドチャンネル攻撃によるプローブの接近やLSIパッケージの開封などを判定する制御回路などの判定手段などを有してもよい。

[0083] 図15は本発明の他の実施形態に係るサイドチャンネル攻撃の検知装置の一例を説明するための概念図である。図16は伝達関数の一例を示す図である。詳細には、図16(a)はプローブが検知手段に接近していない場合の伝達関数の一例を示す図、図16(b)はプローブが検知手段に接近している場合の伝達関数の一例を示す図である。図17は入力信号の電圧の周波数特性の一例を示す図である。

例えば、図15に示した本発明に係る検知装置は、集積回路チップ10に形成された情報処理装置3の近傍に、検知手段として、導電体により細長の伝送路201を設けることによりキャパシタを形成し、その伝送路201の一方の端部から所定の信号（図17参照）を入力し、伝送路201の他方の端部で信号を受信し、その信号に基づいて判定手段としての制御回路5が伝達関数の変化によりプローブ7の接近を判定してもよい。つまり、図16に示した例では、検知手段による、プローブ7の接近による容量結合の変化（キャパシタンスの変化）を示す出力に基づいて、判定手段としての制御回路5がサイドチャンネル攻撃によるプローブの接近を判定する。

また、上述した暗号処理回路などの情報処理装置を含むLSI（集積回路チップ10）が導電体や樹脂などにより構成されるLSIパッケージに収容されている場合、上記検知装置は、パッケージの開封による容量結合の変化（キャパシタンスの変化）に基づいてサイドチャンネル攻撃を検知してもよい。詳細には、上述したように、集積回路チップ10に形成された情報処理装置3の近傍に、検知手段として、導電体などにより伝送路201を設けるこ

とによりキャパシタを形成し、その伝送路 201 の一方の端部から、所定の信号（図 17 参照）を入力し、伝送路 201 の他方の端部で信号を受信し、伝達関数の変化に基づいて判定手段としての制御回路 5 が L S I パッケージの開封を判定してもよい。つまり、検知手段により、パッケージの開封時の容量結合による容量結合の変化（キャパシタンスの変化）に基づいて、判定手段としての制御回路 5 が L S I パッケージの開封を判定する。

[0084] 以上、説明したように、本発明の実施形態に係るサイドチャネル攻撃の検知装置 1 は、サイドチャネル攻撃の対象となる情報処理装置に近接して配置されたコイル（インダクタ）またはキャパシタを有し、コイル（インダクタ）のインダクタンスまたはキャパシタのキャパシタンスの変化を検知する検知手段と、その検知手段によりサイドチャネル攻撃によるプローブの接近または L S I パッケージの開封を判定する判定手段としての制御回路 5 と、を有する。

このため、簡単な構成で、サイドチャネル攻撃を検知可能な検知装置を提供することができる。

また、制御回路は、サイドチャネル攻撃によるプローブの接近または L S I パッケージの開封を検知した場合、上述したように、暗号処理回路の秘密情報を保護する動作モードに切り替える処理を行ってもよい。

[0085] また、本発明に係る検知装置は、上記検知手段を有するので、従来対策では防ぐことが困難な局所電磁波解析攻撃も含めてプロービングによる電気的情報を用いるサイドチャネル攻撃全般を防ぐことができる。

[0086] また、本発明に係る検知装置は、集積回路内部やプリント基板上の配線パターンから放射される電磁界を測定するためにプローブを接近させると、コイルのインダクタンスの変化、詳細には、例えば、集積回路やプリント基板上の配線と（プローブを含む）周囲との電磁界結合度が変化し、不可避に電磁界分布に変化が生じるという物理法則に基づいて、サイドチャネル攻撃を検知することができ、攻撃者は原理的に検知されることなく攻撃を行うことは困難となる。

[0087] また、本発明では、従来対策に対して、暗号ＬＳＩの実行速度や消費電力、実装面積などのオーバーヘッドを大きく削減している。従来対策は少なくとも回路規模を数倍程度増加する。一方、本発明では、検知手段をＬＣ発振器により構成した場合、対策対象となる暗号処理回路に対して２．４％というわずかな面積オーバーヘッドで実現できる。また、コイル以外のすべての回路は完全デジタル回路（ロジック回路）で構成できるので、集積回路製造プロセスの微細化に応じて、暗号コアと同様に面積を縮小できる。

また、コイルについても集積回路製造プロセスの微細化によるトランジスタ性能の改善により縮小可能であり、暗号コアに対するセンサ全体の面積オーバーヘッドについても一定に保つことが出来る。

[0088] また、本発明に係る検知装置は、検知手段をＬＣ発振器により構成した場合、コイル以外の回路を完全デジタル回路（ロジック回路）で構成できるため、設計容易性が高く、集積回路製造プロセスの微細化に応じて、暗号コアと同様に面積を縮小できる。

[0089] また、本発明に係る検知装置は、形状・巻き数の異なる２つ以上のコイルを用いた攻撃検知方式により、多様なプロービング方法を検知可能にするとともに、高精度な周波数基準を不要にすることで周波数基準に対する攻撃も不可能にする。

[0090] また、本発明では、２コイル以上を用いた攻撃検知方式により高精度な周波数基準を不要にし、周波数基準に対する攻撃を不可能にするだけでなく、本発明による回路面積や消費電力の増加を大きく削減することに寄与する。さらに、リング発振器を用いたセンサのワンステップデジタル校正により、ＰＶＴばらつきにも対応可能である。

[0091] さらに、リング発振器を用いたＬＣ発振器の発振周波数のワンステップデジタル校正により、様々な動作環境にも対応可能である。

本発明は、上記機能を実現した場合でも、対策対象となる暗号処理回路（情報処理装置）に対して、例えば、２．４％程度という僅かな面積オーバーヘッドで実現できる。

[0092] また、本発明によれば、上記サイドチャネル攻撃の検知装置を有する半導体装置を提供することができる。

また、本発明によれば、上記サイドチャネル攻撃の検知装置によるサイドチャネル攻撃の検知方法を提供することができる。

符号の説明

- [0093] 1…検知装置
2…検知手段
3…情報処理装置
3 a…暗号処理回路
5…制御回路（判定手段：制御部）
7…プローブ
8 L…LC発振器
8 R…リング発振器
10…集積回路チップ
50…センサコア回路
55…較正回路
57, 57 a, 57 b…カウンタ
L, L1, L2…コイル。

請求の範囲

- [請求項1] サイドチャネル攻撃の対象となる情報処理装置に近接して配置されたインダクタを有し、前記インダクタのインダクタンスの変化を検知する検知手段と、
- 前記検知手段の出力に基づいて前記サイドチャネル攻撃によるプロブの接近またはLSIパッケージの開封を判定する判定手段と、を有することを特徴とする
- サイドチャネル攻撃の検知装置。
- [請求項2] 前記検知手段は、前記インダクタを含む発振回路を有し、前記発振回路の発振周波数の変化を検知することを特徴とする請求項1に記載のサイドチャネル攻撃の検知装置。
- [請求項3] 前記検知手段の前記インダクタは複数であることを特徴とする請求項1または請求項2に記載のサイドチャネル攻撃の検知装置。
- [請求項4] 前記複数のインダクタは、それぞれ形状が異なることを特徴とする請求項3に記載のサイドチャネル攻撃の検知装置。
- [請求項5] 前記複数のインダクタは、それぞれ巻き数が異なることを特徴とする請求項3または請求項4に記載のサイドチャネル攻撃の検知装置。
- [請求項6] 前記検知手段は、前記インダクタを除きロジック回路で構成されていることを特徴とする請求項1から請求項5の何れかに記載のサイドチャネル攻撃の検知装置。
- [請求項7] リング発振回路を備え、該リング発振回路の発振周波数に基づいて、前記検知手段の前記発振回路のキャパシタンスを調整することで該発振回路の発振周波数を較正する手段を有することを特徴とする請求項2から請求項6の何れかに記載のサイドチャネル攻撃の検知装置。
- [請求項8] サイドチャネル攻撃の対象となる情報処理装置に近接して配置されたキャパシタを有し、前記キャパシタのキャパシタンスの変化を検知する検知手段と、
- 前記検知手段の出力に基づいて前記サイドチャネル攻撃によるプロ

ープの接近またはLSIパッケージの開封を判定する判定手段と、を有することを特徴とする

サイドチャネル攻撃の検知装置。

[請求項9] 前記サイドチャネル攻撃によるプローブの接近またはLSIパッケージの開封を検知した場合、暗号処理回路の秘密情報を保護する動作モードに切り替える制御回路を有することを特徴とする請求項1から請求項8の何れかに記載のサイドチャネル攻撃の検知装置。

[請求項10] 前記制御回路は、少なくとも、暗号処理回路の暗号処理を停止させる処理、ダミー演算処理、ハイディング処理、マスキング処理のいずれかを含むことを特徴とする請求項9に記載のサイドチャネル攻撃の検知装置。

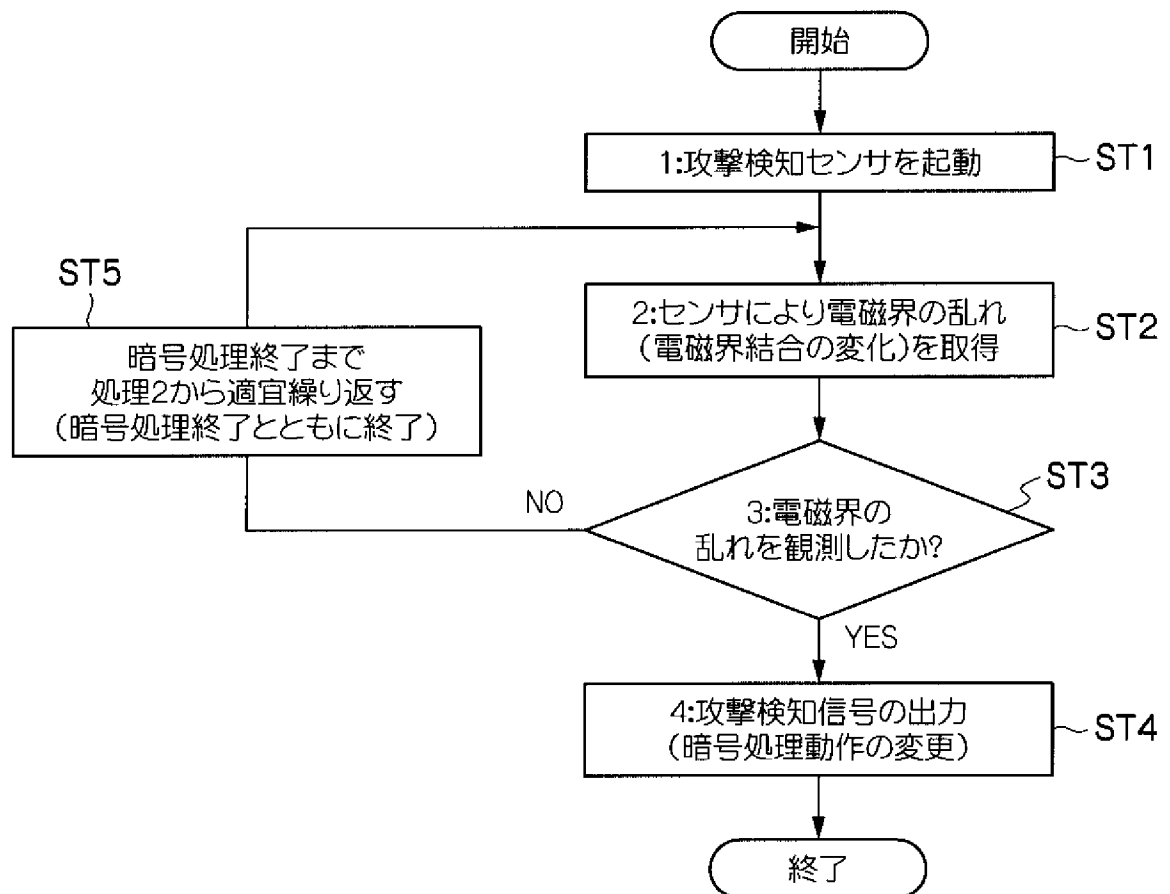
[請求項11] 前記制御回路は、少なくとも、偽の鍵を用いた暗号処理、鍵の変更処理、暗号処理に関わる情報を消去する処理、検知したことを外部に通知する処理、のいずれかを含むことを特徴とする請求項9に記載のサイドチャネル攻撃の検知装置。

[請求項12] 前記情報処理装置および前記検知手段は、同一の集積回路チップに設けられていることを特徴とする請求項1から請求項11の何れかに記載のサイドチャネル攻撃の検知装置。

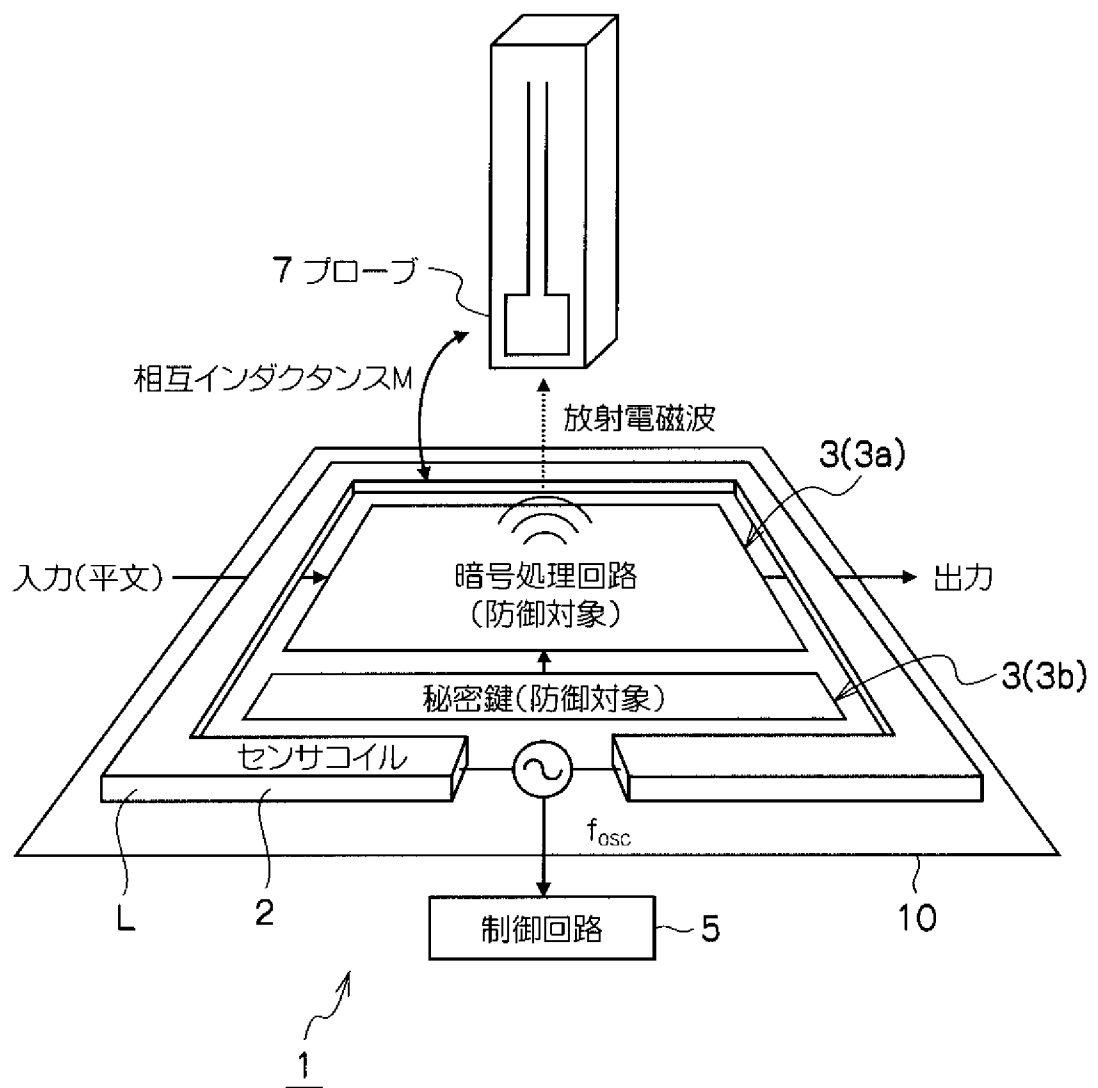
[請求項13] 請求項1から請求項12の何れかに記載のサイドチャネル攻撃の検知装置を有する半導体装置。

[請求項14] 請求項1から請求項12の何れかに記載のサイドチャネル攻撃の検知装置によるサイドチャネル攻撃の検知方法。

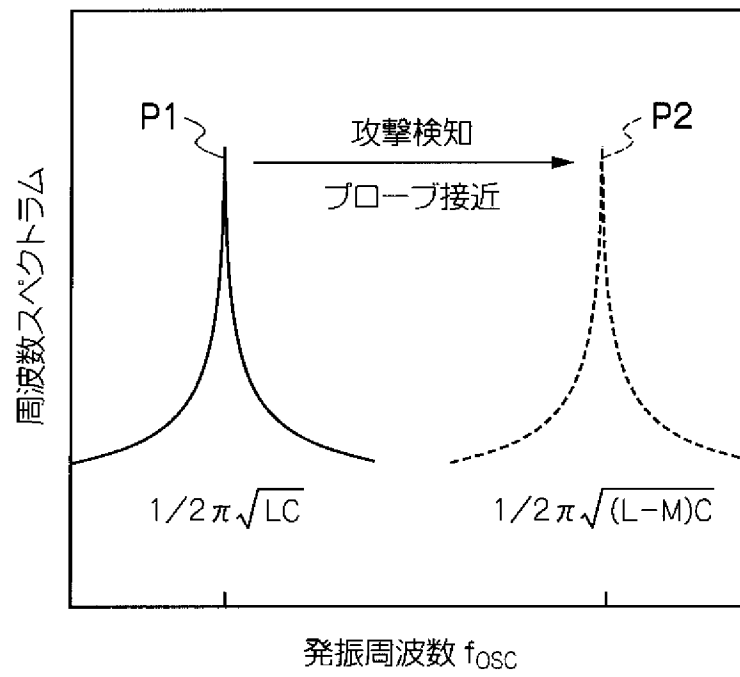
[図1]



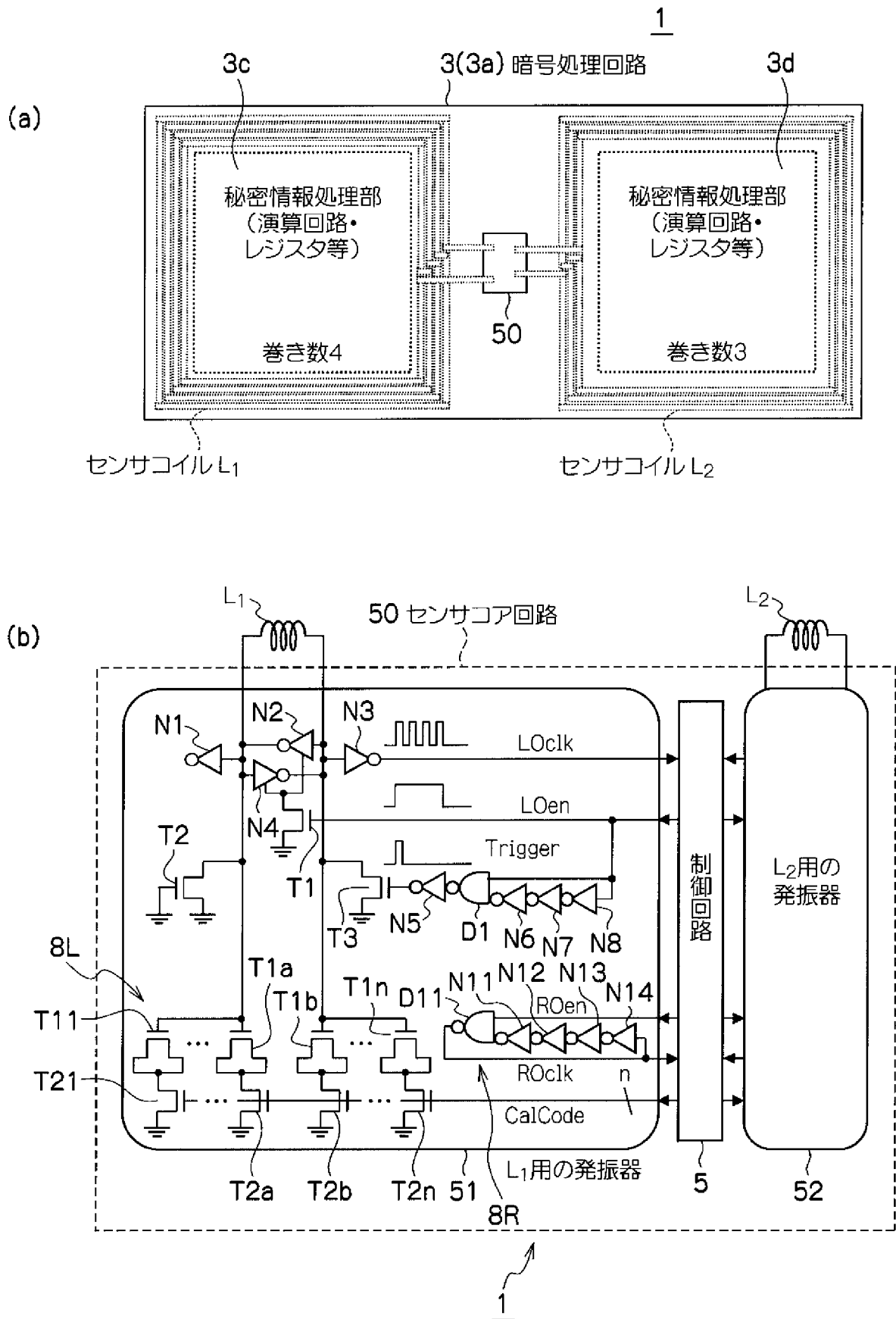
[図2]



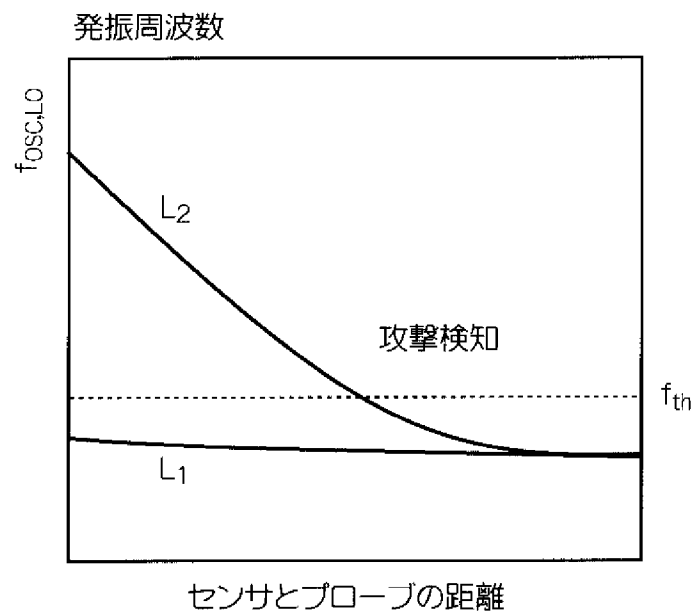
[図3]



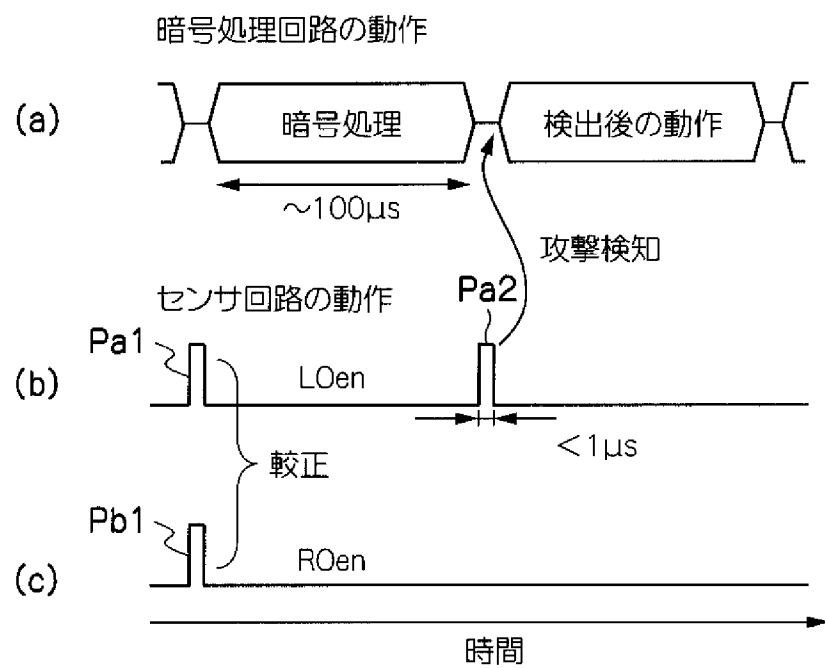
[図4]



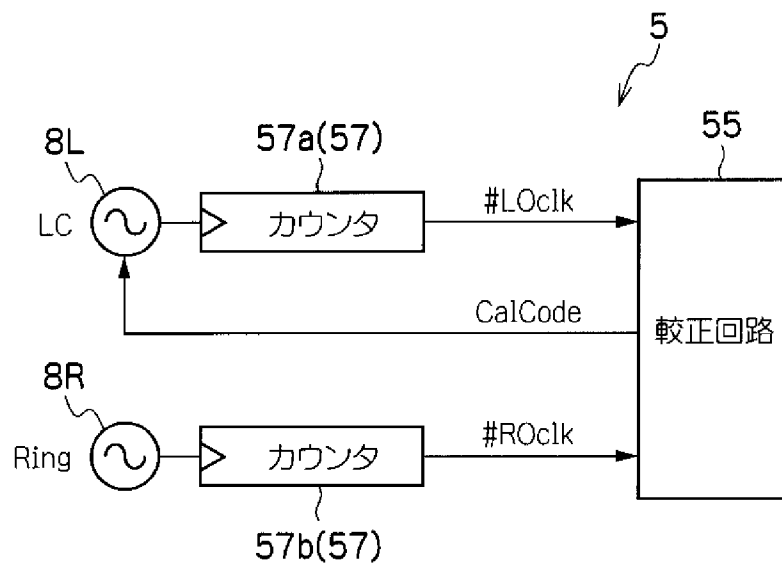
[図5]



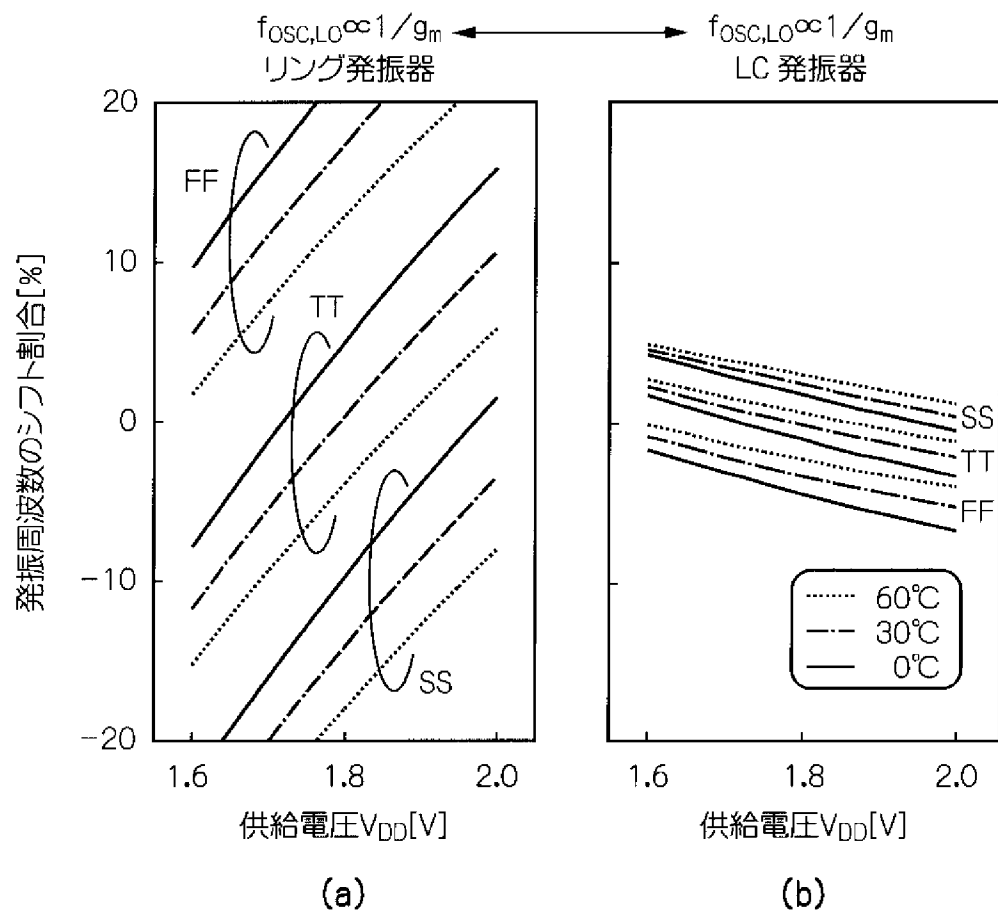
[図6]



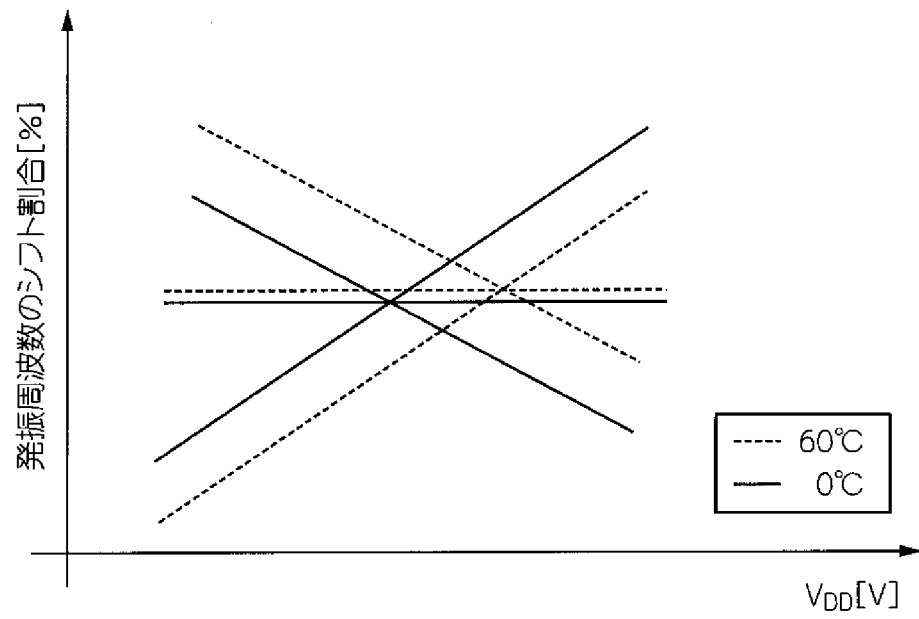
[図7]



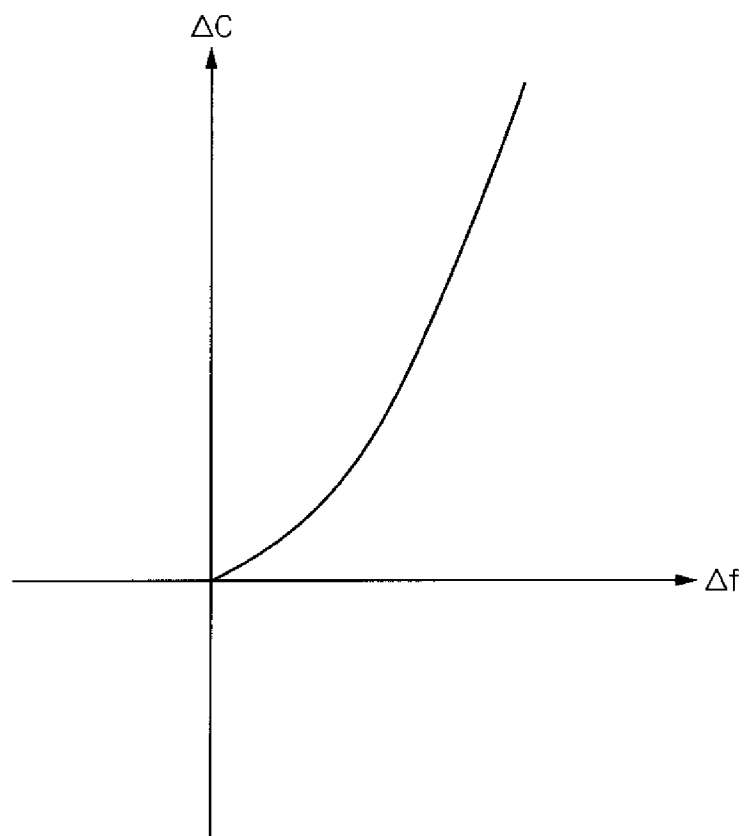
[図8]



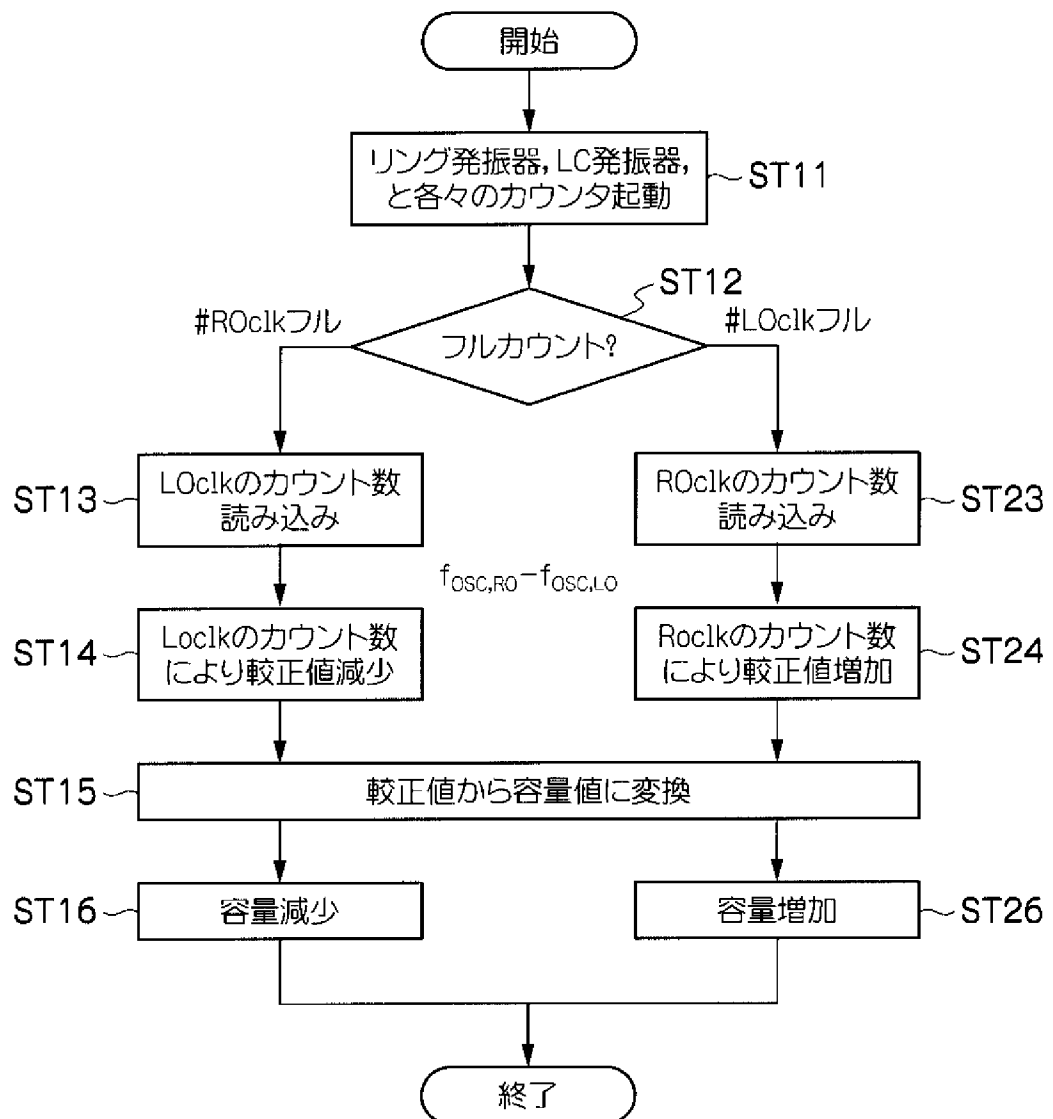
[図9]



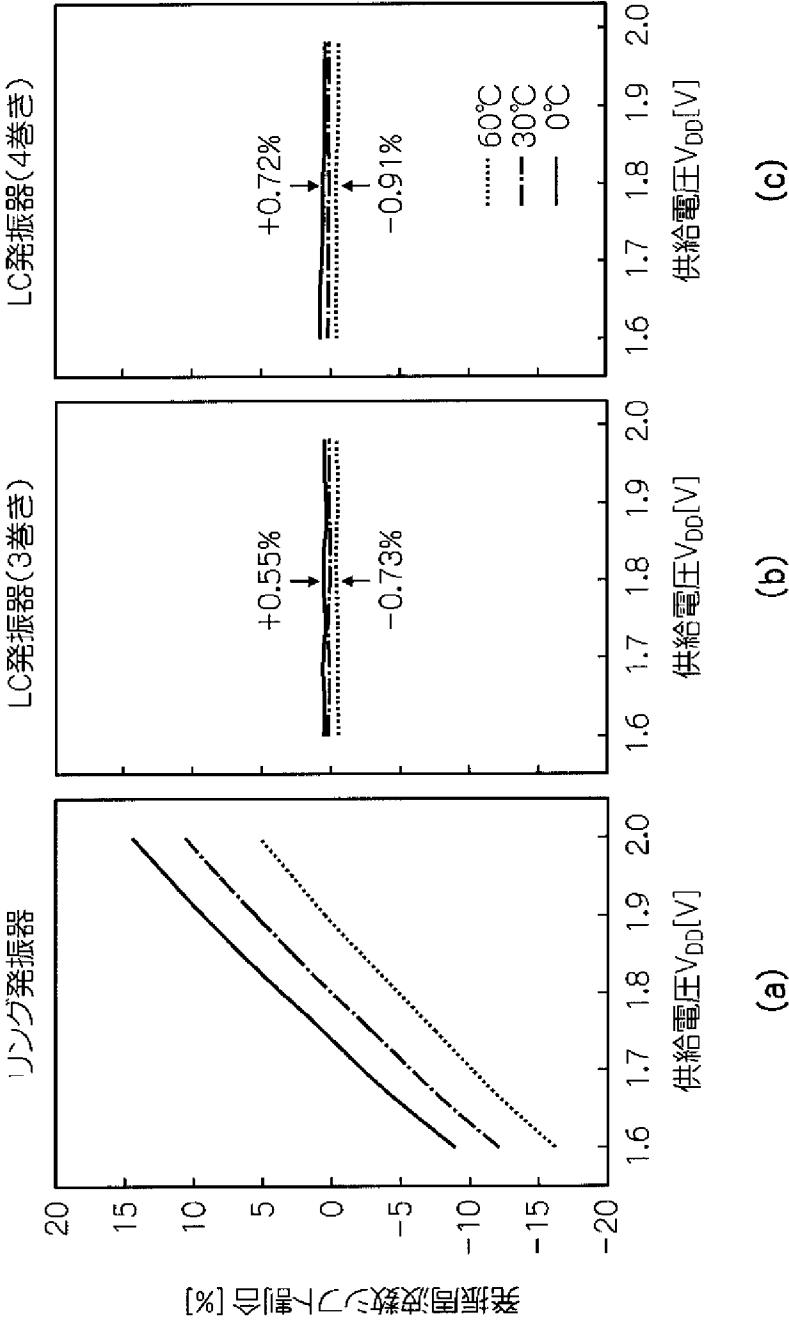
[図10]



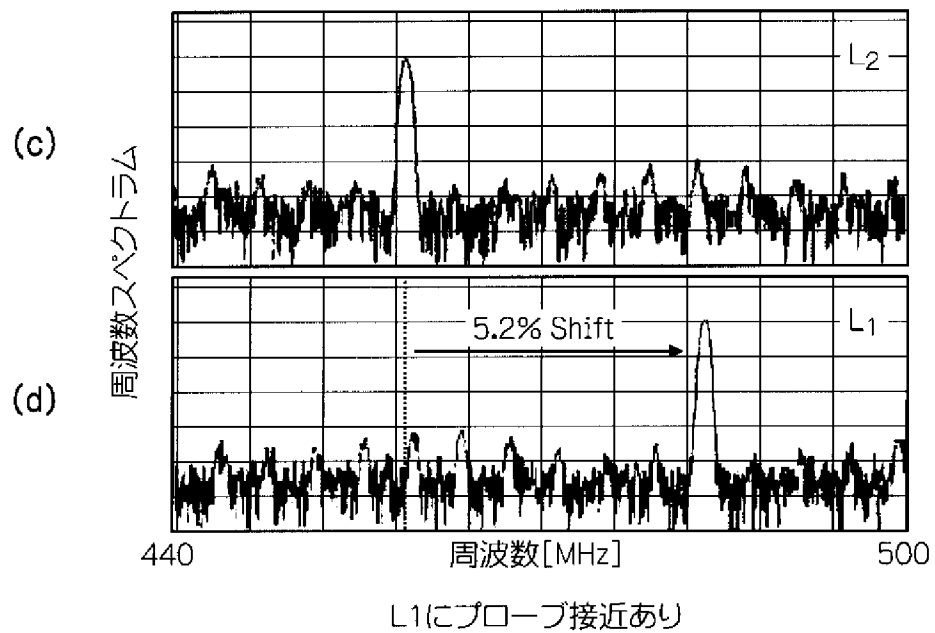
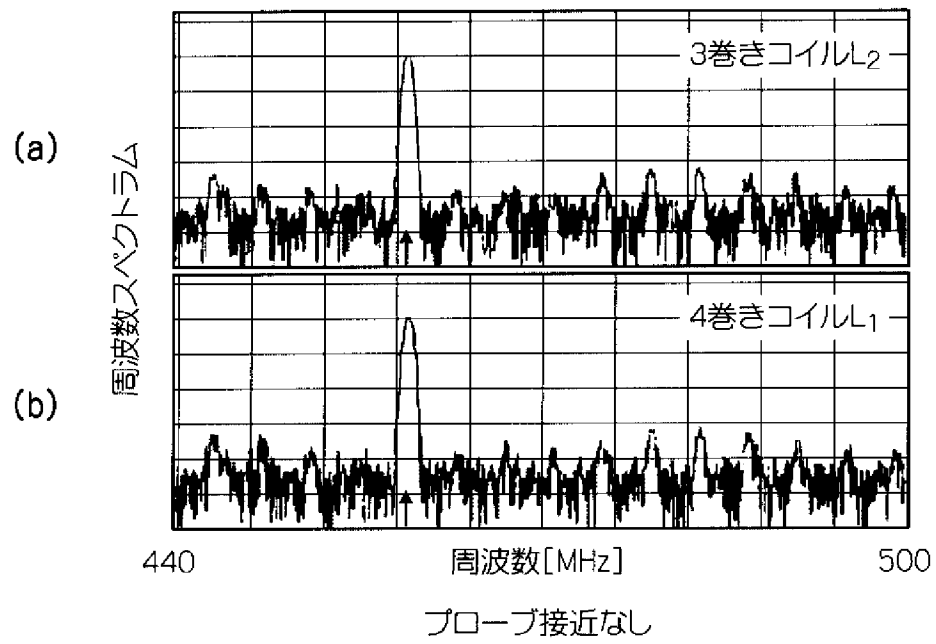
[図11]



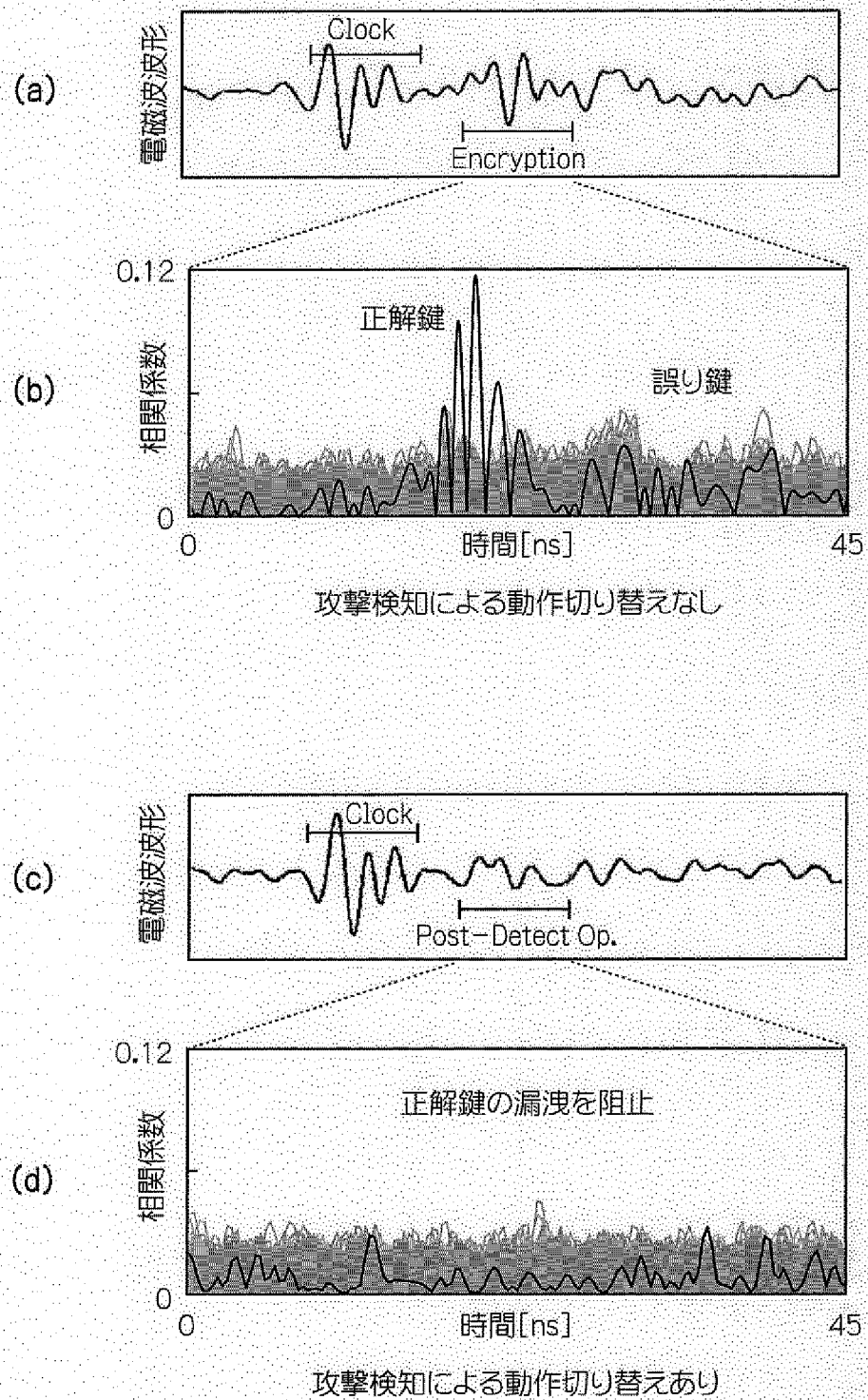
[図12]



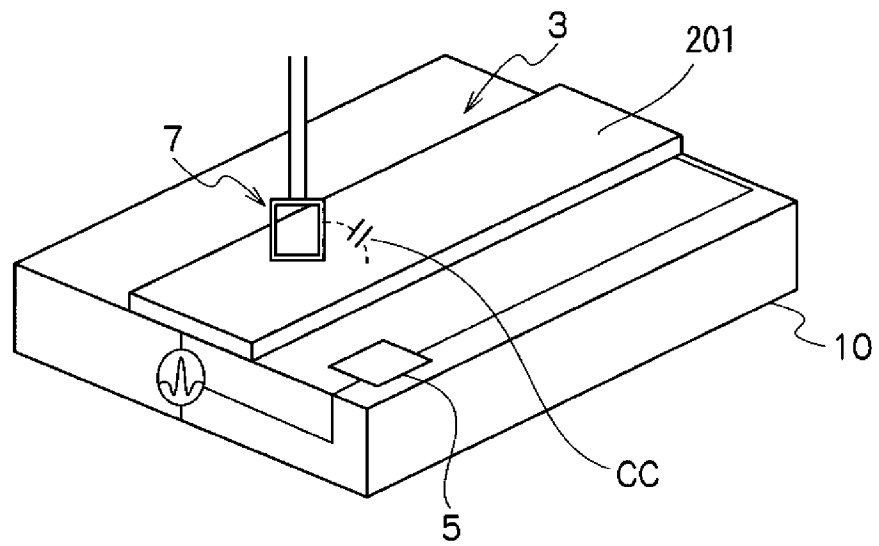
[図13]



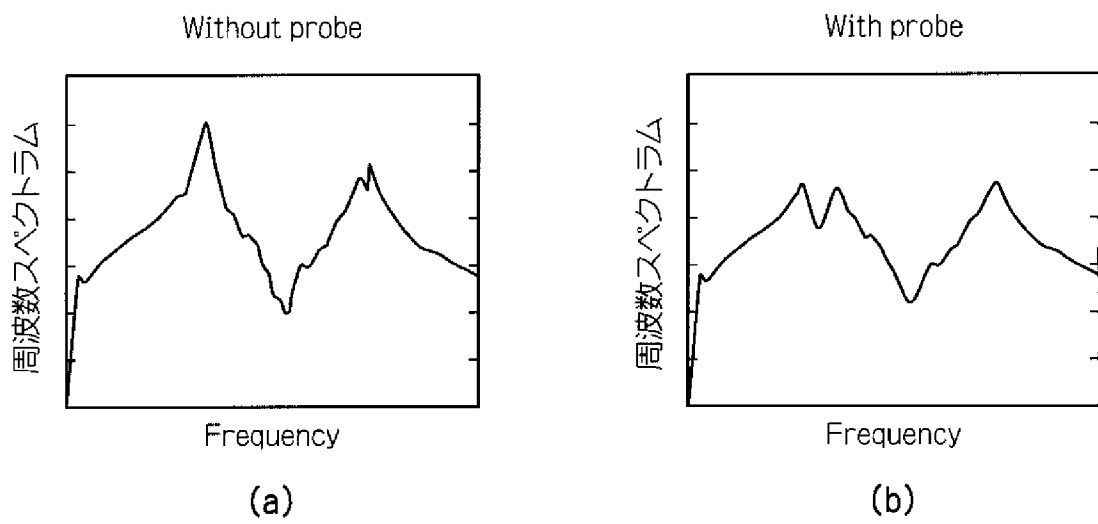
[図14]



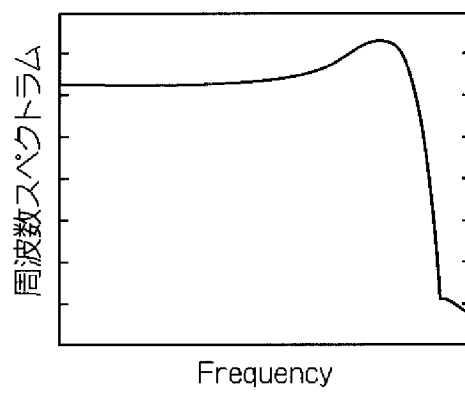
[図15]



[図16]



[図17]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/082010

A. CLASSIFICATION OF SUBJECT MATTER H04L9/10(2006.01) i		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) H04L9/10		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2015 Kokai Jitsuyo Shinan Koho 1971-2015 Toroku Jitsuyo Shinan Koho 1994-2015		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	JP 2007-535022 A (Commissariat A L'energie Atomique), 29 November 2007 (29.11.2007), paragraphs [0006], [0068] to [0098]; fig. 4, 5 & US 2007/0121575 A1 & EP 1700256 A1 & WO 2005/069210 A1 & DE 602004008339 T2 & FR 2864667 A1 & AT 370464 T	1-4, 6, 8-14 5, 7
A	JP 6-60234 A (The United States of America), 04 March 1994 (04.03.1994), entire text; all drawings & US 5237307 A & GB 2262015 A & DE 4239993 A1 & FR 2684220 A1 & CA 2083070 A1	1-14
☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 27 January 2015 (27.01.15)		Date of mailing of the international search report 03 February 2015 (03.02.15)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan		Authorized officer Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C）） Int.Cl. H04L9/10(2006.01)i			
B. 調査を行った分野 調査を行った最小限資料（国際特許分類（I P C）） Int.Cl. H04L9/10			
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2015年 日本国実用新案登録公報 1996-2015年 日本国登録実用新案公報 1994-2015年			
国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）			
C. 関連すると認められる文献			
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号	
X A	JP 2007-535022 A（コミツサリア タ レネルジー アトミック） 2007.11.29, 段落【0006】、【0068】－【0098】、図4, 5 & US 2007/0121575 A1 & EP 1700256 A1 & WO 2005/069210 A1 & DE 602004008339 T2 & FR 2864667 A1 & AT 370464 T	1-4, 6, 8-14 5, 7	
A	JP 6-60234 A（アメリカ合衆国）1994.03.04, 全文, 全図 & US 5237307 A & GB 2262015 A & DE 4239993 A1 & FR 2684220 A1 & CA 2083070 A1	1-14	
☐ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。			
* 引用文献のカテゴリー 「A」特に関連のある文献ではなく、一般的技術水準を示すもの 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す） 「O」口頭による開示、使用、展示等に言及する文献 「P」国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」同一パテントファミリー文献			
国際調査を完了した日 27.01.2015		国際調査報告の発送日 03.02.2015	
国際調査機関の名称及びあて先 日本国特許庁（I S A / J P） 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官（権限のある職員） 打出 義尚 電話番号 03-3581-1101 内線 3546	5 S 4440