(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-234001
(P2007-234001A)
(43)公開日　平成19年9月13日(2007.9.13)

(51)Int.Cl.		F I		テーマコード（参考）
G06K 19/073	(2006.01)	G06K 19/00	P	5B017
G06K 19/07	(2006.01)	G06K 19/00	H	5B035
G06F 21/06	(2006.01)	G06K 19/00	N	
		G06F 12/14	560E	

審査請求 未請求　請求項の数 8　ＯＬ　（全 33 頁）

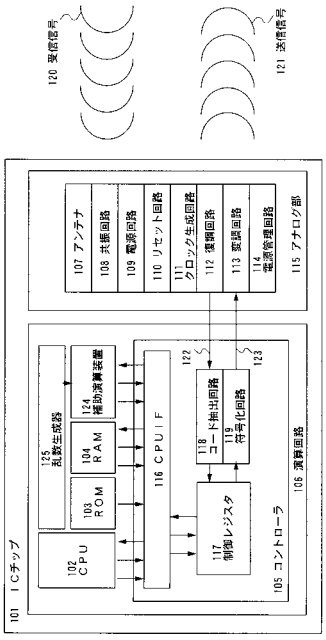
(21)出願番号　特願2007-20267(P2007-20267)
(22)出願日　平成19年1月31日(2007.1.31)
(31)優先権主張番号　特願2006-23675(P2006-23675)
(32)優先日　平成18年1月31日(2006.1.31)
(33)優先権主張国　日本国(JP)

(71)出願人　000153878
株式会社半導体エネルギー研究所
神奈川県厚木市長谷３９８番地
(72)発明者　傳保　洋樹
神奈川県厚木市長谷３９８番地　株式会社半導体エネルギー研究所内

Ｆターム(参考)　5B017 AA03　CA14
5B035 AA13　BB09　CA23　CA38

(54)【発明の名称】半導体装置

(57)【要約】
【課題】ＩＣカードが電力解析攻撃や電磁波解析攻撃を受けた際に、傍受された電力変化およびＥＭ放射から秘密鍵をとりだすことを困難にすることを目的とする。
【解決手段】演算回路及び外部との信号の送受信を行うための回路を有し、演算回路は中央処理装置１０２、補助演算装置１２４、乱数生成器１２５、読み出し専用メモリ１０３が含まれている。読み出し専用メモリ１０３には、外部との信号の送受信におけるサイドチャネル攻撃を阻止する処理をおこなうためのプログラムが記録されている。乱数生成器１２５と補助演算装置１２４を加えることにより、ＩＣチップから漏れる物理的情報の時間変化をより複雑にすることができる。この動作は前記プログラムが実行する。そのため、第３者が傍受した物理的情報から内部情報を取り出すことに時間がかかり、セキュリティを高めることが出来る。
【選択図】図１



【特許請求の範囲】
【請求項１】
外部との信号の送受信を行う回路と、
外部との信号の送受信におけるサイドチャネル攻撃を阻止する処理を行う演算回路と、を有し、
前記演算回路は、前記外部との信号の送受信におけるサイドチャネル攻撃を阻止する処理を行うプログラムが記憶された第１のメモリと、
前記第１のメモリより前記プログラムを読み出して当該プログラムを実行する中央処理装置と、
前記プログラムの命令に従って、前記信号に基づいたデータの逆変換処理を行う補助演算装置と、
前記逆変換処理の演算時間を設定するための乱数を生成する乱数生成器と、
前記逆変換処理されたデータを記憶する第２のメモリと、を有することを特徴とする半導体装置。
【請求項２】
外部との信号の送受信を行う回路と、
外部との信号の送受信におけるサイドチャネル攻撃を阻止する処理を行う演算回路と、を有し、
前記演算回路は、前記外部との信号の送受信におけるサイドチャネル攻撃を阻止する処理を行うプログラムが記憶された第１のメモリと、
前記第１のメモリより前記プログラムを読み出して当該プログラムを実行することにより、前記外部からの信号に基づいたデータの逆変換処理を行う中央処理装置と、
前記逆変換処理の演算時間を設定するための乱数を生成する乱数生成器と、
前記逆変換処理されたデータを記憶する第２のメモリと、を有することを特徴とする半導体装置。
【請求項３】
請求項１または請求項２において、
前記外部より受信される信号は、フレーム開始のコード、フラグのコード、コマンドのコード、データのコード、巡回冗長検査のコード、及びフレーム終了のコードにより構成される信号であることを特徴とする半導体装置。
【請求項４】
請求項１乃至請求項３のいずれか１項において、
前記プログラムは、前記外部より受信される信号の種類を判断する第１のルーチンと、前記逆変換処理の演算回数を判断する第２のルーチンにより構成されることを特徴とする半導体装置。
【請求項５】
請求項１乃至請求項４のいずれか１項において、
前記演算回路は、インターフェース、制御レジスタ、コード抽出回路、及び符号化回路を含むコントローラを有することを特徴とする半導体装置。
【請求項６】
請求項１乃至請求項５のいずれか１項において、
前記外部との信号の送受信を行う回路は、アンテナ、共振回路、電源回路、リセット回路、クロック生成回路、復調回路、変調回路、及び電源管理回路を有することを特徴する半導体装置。
【請求項７】
請求項１乃至請求項６のいずれか１項において、
前記乱数生成器は、第１のメモリセルを有する読み出し回路とデコーダにより制御されるメモリセルアレイを有し、
前記乱数の値は、前記第１のメモリセルの閾値電圧と前記メモリセルアレイより選択された第２のメモリセルの閾値電圧の差により決定されることを特徴とする半導体装置。

【請求項８】
請求項１乃至請求項７のいずれか１項に記載の半導体装置を備えたことを特徴とするＲＦＩＤ用ＩＣチップ、ＩＤチップ、ＩＣタグ、ＩＤタグ、ＲＦタグ、無線タグ、電子タグ、またはトランスポンダ。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は半導体装置に関する。特に外部器機との信号の送受信を無線通信で行う半導体装置に関する。なお、ここでいう半導体装置とは、半導体特性を利用することで機能しうる装置全般を指すものとする。例えば、ＲＦＩＤ（Ｒａｄｉｏ Ｆｒｅｑｕｅｎｃｙ Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）用ＩＣチップ（ＩＤチップ、ＩＣタグ、ＩＤタグ、ＲＦタグ、無線タグ、電子タグ、トランスポンダともいう）も本発明の範疇に属する。
【背景技術】
【０００２】
コンピュータ技術の発展や、画像認識技術の向上によって、バーコードなどの媒体を用いた情報認識が広く普及し、商品データの認識などに用いられている。今後はさらに多量の情報認識が実施されると予想される。その一方、バーコードによる情報読み取りなどでは、バーコードリーダーがバーコードとの接触を必要とすることや、バーコードに記録される情報量があまり多くできないという欠点があり、非接触の情報認識および媒体の記憶容量増大が望まれている。
【０００３】
このような要望から、非接触型のＲＦＩＤ用ＩＣチップ（以下、ＩＣチップという）、及びリーダ／ライタ装置（質問器ともいう；以下、リーダライタという）が開発されている。ＩＣチップとはＩＣチップ内のメモリ回路に必要な情報を記憶し、非接触手段、一般的には無線手段を用い、リーダライタにより内部の情報を読み取るものである。このようなＩＣチップに記憶された情報を読み取る情報処理装置の実用化によって、商品流通などの簡素化、低コスト化、高いセキュリティの確保が可能になるものと期待されている。
【０００４】
近年、クレジットカード、キャッシュカードなど、高いセキュリティが必要とされる分野を対象に、非接触でデータの授受が行えるＩＣチップを搭載したカードの普及が始まっている。このようなＩＣチップを搭載したカードは、データの授受を行う際に使用する周波数帯に適応した形状のアンテナを介して、外部の機器と非接触でデータの読み書きをするようになされる。また、データの授受を第３者に傍受された際に解読を困難にするため、外部の機器とデータの読み書きする際にデータを暗号にして読み書きするようになされる。
【０００５】
このようなＩＣチップを搭載したカードは、ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）の暗号アルゴリズムに対応した暗号計算を行うための専用のハードウェアとソフトウェアを合わせて搭載することで、暗号を処理している。例えば、ＤＥＳの暗号アルゴリズムを高速に処理するための方法について文献に開示されている（特許文献１参照）。
【０００６】
この文献によれば、ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）を解読するために、ＩＣチップに記録されている秘密鍵を使用している。しかし、秘密鍵を解読できる方法として、サイドチャネル攻撃が挙げられる。サイドチャネル攻撃（ｓｉｄｅ－ｃｈａｎｎｅｌ ａｔｔａｃｋ）とは、暗号装置の動作状況を様々な物理的手段で観察することにより、装置内部の重要な情報を取得しようとする攻撃方法である。具体的な攻撃方法としては、電力解析攻撃と電磁波解析攻撃がある。電力解析攻撃とは、ＩＣカードの消費電力と処理内容と相関があることを利用し、消費電力を測定して統計処理することで処理内容に関する情報（秘密鍵）を取り出すという攻撃方法である。具体的には、攻

撃者がＩＣカードに測定プローブを当て、消費電力の変化を測定することで秘密鍵を取り出す。

【０００７】

電力解析攻撃を利用することで、秘密鍵を解読した例として、複数の報告がされている（例えば、非特許文献１～３参照）。

【０００８】

電磁波解析攻撃とは、ＩＣカードが暗号演算中に周囲に発するＥＭ（Ｅｌｅｃｔｒｏｍａｇｎｅｔｉｃ）放射とデバイスの処理内容と相関があることを利用し、ＥＭ放射の時間変化を測定して統計処理することで処理内容に関する通信情報を取り出すという攻撃方法である。具体的には、攻撃者がＩＣカードのＥＭ放射を測定器によって傍受することで秘密鍵を取り出す。

【０００９】

電磁波解析攻撃を利用することで、秘密鍵を解読した例としては以下の報告がある（例えば、非特許文献４参照）。このような、電力解析攻撃や電磁波解析攻撃を利用すると、秘密鍵が短時間でわかってしまうため、クレジットカードやキャッシュカードとして要求される高いセキュリティが確保できない。

【特許文献１】特開平１１－２１２４５１号公報

【非特許文献１】Ｐａｕｌ Ｋｏｃｈｅｒ, Ｊｏｓｈｕａ Ｊａｆｆｅ, Ｂｅｎｊａｍｉｎ Ｊｕｎ, ”Ｉｎｔｒｏｄｕｃｔｉｏｎ ｔｏ Ｄｉｆｆｅｒｅｎｔｉａｌ Ｐｏｗｅｒ Ａｎａｌｙｓｉｓ ａｎｄ Ｒｅｌａｔｅｄ Ａｔｔａｃｋｓ”, １９９８.

【非特許文献２】Ｂｒｕｃｅ Ｓｃｈｎｅｉｅｒ, ”Ｓｉｄｅ－Ｃｈａｎｎｅｌ Ａｔｔａｃｋｓ Ａｇａｉｎｓｔ Ｃｒｙｐｔｏｓｙｓｔｅｍｓ”, Ｃｒｙｐｔｏ－Ｇｒａｍ Ｎｅｗｓｌｅｔｔｅｒ, １５ Ｊｕｎｅ １９９８.

【非特許文献３】Ｐａｕｌ Ｋｏｃｈｅｒ, Ｊｏｓｈｕａ Ｊａｆｆｅ, Ｂｅｎｊａｍｉｎ Ｊｕｎ, ”Ｄｉｆｆｅｒｅｎｔｉａｌ Ｐｏｗｅｒ Ａｎａｌｙｓｉｓ”, ＣＲＹＰＴＯ’９９, ｐｐ. ３８８－３９７, １９９９.

【非特許文献４】Ｋ. Ｇａｎｄｏｌｆｉ, Ｃ. Ｍｏｕｒｔｅｌ, Ｆ. Ｏｌｉｖｉｅｒ, ”Ｅｌｅｃｔｒｏｍａｇｎｅｔｉｃ ａｎａｌｙｓｉｓ: ｃｏｎｃｒｅｔｅ ｒｅｓｕｌｔｓ”, ＣＨＥＳ２００１, ｐｐ. ２５１－２６１, １３－１６ Ｍａｙ ２００１.

【発明の開示】

【発明が解決しようとする課題】

【００１０】

そこで、本発明はＩＣカードが電力解析攻撃や電磁波解析攻撃を受けた際に、傍受された電力変化およびＥＭ放射から秘密鍵をとりだすことに、より時間がかかる半導体装置を提供することを課題とする。

【課題を解決するための手段】

【００１１】

本発明の一は、外部との信号の送受信を行う回路と、外部との信号の送受信におけるサイドチャネル攻撃を阻止する処理を行う演算回路と、を有し、演算回路は、外部との信号の送受信におけるサイドチャネル攻撃を阻止する処理を行うプログラムが記憶された第１のメモリと、第１のメモリよりプログラムを読み出して当該プログラムを実行する中央処理装置と、プログラムの命令に従って、信号に基づいたデータの逆変換処理を行う補助演算装置と、逆変換処理の演算時間を設定するための乱数を生成する乱数生成器と、逆変換処理されたデータを記憶する第２のメモリと、を有することを特徴とする半導体装置である。

【００１２】

本発明の一は、外部との信号の送受信を行う回路と、外部との信号の送受信におけるサイドチャネル攻撃を阻止する処理を行う演算回路と、を有し、演算回路は、外部との信号

の送受信におけるサイドチャネル攻撃を阻止する処理を行うプログラムが記憶された第１のメモリと、第１のメモリよりプログラムを読み出して当該プログラムを実行することにより、外部からの信号に基づいたデータの逆変換処理を行う中央処理装置と、逆変換処理の演算時間を設定するための乱数を生成する乱数生成器と、逆変換処理されたデータを記憶する第２のメモリと、を有することを特徴とする半導体装置である。

【００１３】

本発明において、外部より受信される信号は、フレーム開始のコード、フラグのコード、コマンドのコード、データのコード、巡回冗長検査のコード、及びフレーム終了のコードにより構成される信号であってもよい。

【００１４】

本発明において、プログラムは、外部より受信される信号の種類を判断する第１のルーチンと、逆変換処理の演算回数を判断する第２のルーチンにより構成されていてもよい。

【００１５】

本発明において、演算回路は、インターフェース、制御レジスタ、コード抽出回路、及び符号化回路を含むコントローラを有する構成であってもよい。

【００１６】

本発明において、外部との信号の送受信を行う回路は、アンテナ、共振回路、電源回路、リセット回路、クロック生成回路、復調回路、変調回路、及び電源管理回路を有する構成であってもよい。

【００１７】

本発明において、乱数生成器は、第１のメモリセルを有する読み出し回路とデコーダにより制御されるメモリセルアレイを有し、乱数の値は、第１のメモリセルの閾値電圧とメモリセルアレイより選択された第２のメモリセルの閾値電圧の差により決定される構成であってもよい。

【００１８】

本発明の一は、上記本発明の半導体装置を備えたことを特徴とするＲＦＩＤ用ＩＣチップ、ＩＤチップ、ＩＣタグ、ＩＤタグ、ＲＦタグ、無線タグ、電子タグ、またはトランスポンダである。

【発明の効果】

【００１９】

サイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、乱数生成器と補助演算装置を加えることにより、ＩＣチップから漏れる物理的情報の時間変化をより複雑にすることができる。そのため、第３者が傍受した物理的情報から内部情報を取り出すことに時間がかかり、セキュリティを高めることが出来る。また、サイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、サイドチャネル攻撃を阻止する方法が変更になることに伴う仕様の変更により、ＩＣチップのマスク設計の段階から作り直す必要ない。そのため、製造コストの削減及び製造時間の短縮ができる。また、マスク設計の変更によって再度作り直したＩＣチップに不具合が生じているといった懸念もない。

【００２０】

また従来においては、サイドチャネル攻撃を阻止する機能を有するＩＣチップを製造する際においては、サイドチャネル攻撃を阻止する回路を搭載することもあった。しかしながら、本発明を採用することで、サイドチャネル攻撃を阻止する機能を読み出し専用メモリにプログラムとして格納することにより、別途サイドチャネル攻撃を阻止する機能を備えた回路を設ける場合より、ＩＣチップを小型化することができる。そのため、ＩＣチップの軽量化、１枚の基板から作製できるＩＣチップの数の増加に伴うコストの削減、またサイドチャネル攻撃を阻止する機能を備えた回路の分だけ、トランジスタ数が減少することによる歩留まりの向上に貢献することができる。

【発明を実施するための最良の形態】

【００２１】

以下、本発明の実施の形態を図面に基づいて説明する。但し、本発明は多くの異なる態

様で実施することが可能であり、本発明の趣旨及びその範囲から逸脱することなくその形態及び詳細を様々に変更し得ることは当業者であれば容易に理解される。従って、本実施の形態の記載内容に限定して解釈されるものではない。なお、実施の形態を説明するための全図において、同一部分又は同様な機能を有する部分には同一の符号を付し、その繰り返しの説明は省略する。

【００２２】

（実施の形態１）

本実施の形態では、本発明におけるサイドチャネル攻撃を阻止する機能を実現するための装置構成及び、フローチャートについて説明する。

【００２３】

図１に本発明におけるサイドチャネル攻撃を阻止する機能を搭載する対象であるＩＣチップのブロック図を示す。

【００２４】

図１において、ＩＣチップ１０１は、演算回路１０６、アナログ部１１５を有する。演算回路１０６は、ＣＰＵ１０２（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ；中央処理装置ともいう。またＭＰＵ（ｍｉｃｒｏｐｒｏｃｅｓｓｏｒ）ともいう。）、ＲＯＭ１０３（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ；読み出し専用メモリともいう）、ＲＡＭ１０４（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ；ランダムアクセスメモリともいう）、補助演算装置１２４、乱数生成器１２５、コントローラ１０５を有する。また、アナログ部１１５は、アンテナ１０７、共振回路１０８、電源回路１０９、リセット回路１１０、クロック生成回路１１１、復調回路１１２、変調回路１１３、電源管理回路１１４を有する。また、コントローラ１０５は、ＣＰＵインターフェース１１６（ＣＰＵＩＦ）、制御レジスタ１１７、コード抽出回路１１８、符号化回路１１９より構成される。なお、図１では、説明の簡略化のため通信信号として、受信信号１２０と送信信号１２１とに分けて示したが、実際には両者は重ね合わされており、ＩＣチップ１０１及びリーダライタ装置の間で同時に送受信される。受信信号１２０は、アンテナ１０７と共振回路１０８とで受信された後、復調回路１１２により復調される。また、送信信号１２１は、変調回路１１３により変調された後、アンテナ１０７より送信される。なお、受信信号及び送信信号とは、ＩＣチップ側を主体とした表現であり、ＩＣチップが外部からの信号を受信、外部に信号を送信するものであることを付記する。本明細書においては、リーダライタよりＩＣチップが受信する信号、換言すればリーダライタが送信する信号のことを外部からの信号といい、外部からの信号をＩＣチップが受信及びリーダライタが送信することを外部からの信号の送受信という。

【００２５】

なお、ＲＯＭは、リーダライタから受信した受信データを処理する際に機能するプログラム（以下、サイドチャネル攻撃阻止プログラムという）のデータが格納され、ＲＡＭにはプログラムが機能した際の処理データが格納される。ＲＯＭにはマスクＲＯＭ等があり、ＲＡＭにはスタティック型メモリ（ＳＲＡＭ）やダイナミック型メモリ（ＤＲＡＭ）等がある。具体的には、サイドチャネル攻撃阻止プログラムのデータにはＩＣチップの消費電力の変化を測定するサイドチャネル攻撃の複数のサイドチャネル攻撃阻止のためのルーチン（以下、サイドチャネル攻撃阻止ルーチン）が含まれる。

【００２６】

また図２には、ＲＯＭ１０３、ＲＡＭ１０４のアドレス空間を示す。ＲＯＭ１０３には、サイドチャネル攻撃阻止プログラム２０１、秘密鍵２０２が格納されている。サイドチャネル攻撃阻止プログラム２０１は、コマンド判断ルーチン２０１Ａ、ラウンド判断ルーチン２０１Ｂを有する。コマンド判断ルーチン２０１Ａとは、特定のコマンドの判断の処理を実行する機能をもったプログラムコードのことをいう。ラウンド判断ルーチン２０１Ｂとは、暗号解読処理におけるラウンド数を判断するための処理を実行する機能をもったプログラムコードのことをいう。これらの複数のルーチンについては、後述することでさらに詳細に説明することにする。

【００２７】
ＲＡＭ１０４は、送信データレジスタ２０３、受信データレジスタ２０４を有する。送信データレジスタ２０３は、ＩＣチップが送信するデータを格納する機能を有する。受信データレジスタ２０４は、ＩＣチップが受信したデータを格納する機能を有する。ＲＡＭ１０４は、ＲＯＭ１０３に比べて情報量が少ないため、その面積は小さい。
【００２８】
また図３には、リーダライタからＩＣチップに送信される信号、換言するとＩＣチップが受信する信号の構成について示す。受信信号は、ＳＯＦ３０１（Ｓｔａｒｔ Ｏｆ Ｆｒａｍｅ；フレームの開始）、フラグ３０２、コマンド３０３、データ３０４、ＣＲＣ（ｃｙｃｌｉｃ ｒｅｄｕｎｄａｎｃｙ ｃｈｅｃｋ、巡回冗長検査ともいう）３０５、ＥＯＦ３０６（Ｅｎｄ Ｏｆ Ｆｒａｍｅ；フレームの終了）を有する信号である。ＳＯＦ３０１，ＥＯＦ３０６は単に信号の開始と終了を示すものである。フラグ３０２はＡＳＫ、ＦＳＫ等の変調の種類の情報を有する。コマンド３０３は、リーダライタがＩＣチップを読み取るか否かを規定する信号であり、信号が読み取られる場合には「インベントリー（Ｉｎｖｅｎｔｏｒｙ）＝１」、それ以外の状態（読み取りを休止する等の命令）では、「インベントリー（Ｉｎｖｅｎｔｏｒｙ）≠１」との情報を有する。データ３０４には、暗号解読するデータが含まれる。ＣＲＣ３０５はデータの誤認を防止するためにデータより生成される固有のコードの情報を有する。
【００２９】
乱数生成器１２５は、乱数を生成する機能を有する。具体的には、製造する半導体装置の特性ばらつきを利用することでそのような機能を実現する。なお、半導体装置の特性ばらつきとしては、製造プロセスに起因する種々のばらつき（膜の厚さ、膜の性質、不純物濃度など）を利用する。乱数生成器によるデータは、電気的な読み出し以外の方法で解読することが困難であることから、高いセキュリティを確保する。
【００３０】
また図１０には、補助演算装置１２４の構成を示す。補助演算装置１２４は複数のスイッチマトリクスによって構成され、入力データ１１０１を鍵１１０２を使って演算し、出力データ１１０３として出力する機能を有する。補助演算装置１２４が演算する時間は、スイッチパラメータ１１０４の値を元に決まる。具体的には、スイッチパラメータ１１０４の値を元に複数のスイッチマトリクスを切り替えることでそのような機能を実現する。
【００３１】
次に、図１におけるＩＣチップでのサイドチャネル攻撃を阻止する機能をもつプログラムの動作を、図４のフローチャートと対応させながら説明する。
【００３２】
まず、ＩＣチップが有するリセット回路１１０は、受信信号１２０を受けて演算回路１０６にリセットをかける（初期リセット４０１）。復調回路１１２はリセットがかかると受信信号１２０の復調を開始し、コード抽出回路１１８へ復調された受信データ１２２を出力する。コード抽出回路１１８は復調された受信データ１２２から制御コードを抽出し制御レジスタ１１７へ書き込む。
【００３３】
ＩＣチップが有するＣＰＵ１０２は、制御レジスタ１１７にコード抽出回路からの信号の書き込みがあると動作を開始する（開始４０２）。ＣＰＵ１０２は、制御レジスタ１１７内の制御コードにＳＯＦ（Ｓｔａｒｔ Ｏｆ Ｆｒａｍｅ）が含まれていれば（制御レジスタ判断４０３）、ＲＯＭ１０３からサイドチャネル攻撃阻止プログラムを読み込み（プログラム読み込み４０４）、サイドチャネル攻撃阻止プログラム内のサイドチャネル攻撃阻止ルーチンを実行する（ルーチン実行４０９）。一方、制御レジスタ１１７の制御コードにＳＯＦが含まれていなければ初期リセット４０１後の状態に戻る。なお、ＣＰＵ１０２は、サイドチャネル攻撃阻止ルーチンの実行終了後、初期リセット４０１後の状態に戻る。
【００３４】

次に、図１におけるＩＣチップでのサイドチャネル攻撃を阻止する機能を実現するためのサイドチャネル攻撃阻止プログラム内のサイドチャネル攻撃阻止ルーチンを図５～図９を用いて説明する。

【００３５】

まず、図５に示すフローチャートと対応させながらサイドチャネル攻撃阻止ルーチンの動作を説明する。ＣＰＵ１０２は、ＲＯＭ１０３からサイドチャネル攻撃阻止プログラムを読み込み、サイドチャネル攻撃阻止ルーチンを開始する（ルーチン開始５０１）。ＣＰＵ１０２は、制御レジスタ１１７のコマンドコードを読み込み、ＲＡＭ１０４へ書き込む（コマンド取得５０３）。ＣＰＵ１０２は、コマンドコードの種類によって処理を暗号解読と暗号解読以外に分岐させ（コマンド判断５０９）、さらに複数のルーチンを実行させることができる。最後に、ＣＰＵ１０２はサイドチャネル攻撃を阻止するための複数のルーチンを終了する（終了５０４）。

【００３６】

次に図６のフローチャートと対応させながら図１におけるＩＣチップでのコマンドコード別処理の詳細を説明する。

【００３７】

図６に暗号解読コマンドのフローチャートを示す（図５における（Ａ））。ＣＰＵ１０２は、制御レジスタ１１７のデータコードを読み込み、受信データレジスタ２０４へ書き込む（データ取得６０１）。ＣＰＵ１０２は、第一の逆変換処理（図６における（Ｄ））を実行する。

【００３８】

次に図７にラウンド判断のフローチャートを示す（図６における（Ｂ））。ＣＰＵ１０２は、ラウンド（ＲＯＵＮＤ）フラグ値をＮ（本実施形態では８）にする。ＣＰＵ１０２は、ラウンドフラグ値によって処理を分岐させる（ラウンド判断６１２）。ＣＰＵ１０２は、ラウンドフラグ値が０以外の時には、ラウンド処理（図７における（Ｃ））を実行する。ＣＰＵ１０２は、ラウンドフラグ値が０の時には、サイドチャネル攻撃阻止ルーチンを終了させる（終了５０４）。

【００３９】

図８にラウンド処理のフローチャートを示す（図７における（Ｃ））。ＣＰＵ１０２は、受信データレジスタ２０４の値を読み出し、第二の逆変換（本実施の形態ではＰｓｅｕｄｏ－Ｈａｄａｍａｒｄ変換の逆変換）を施し、再び受信データレジスタ２０４に格納する（第二の逆変換６１３）。ＣＰＵ１０２は、受信データレジスタ２０４の値を読み出し、逆転置を施し、再び受信データレジスタ２０４に格納する（逆転置６１４）。ＣＰＵ１０２は、第二の逆変換６１５を第二の逆変換６１３、と同じ方法で行う。ＣＰＵ１０２は、逆転置６１６を逆転置６１４と同じ方法で行う。ＣＰＵ１０２は、第二の逆変換６１７を第二の逆変換６１３、と同じ方法で行う。ＣＰＵ１０２は、第一の逆変換処理（図８における（Ｄ））を実行する。ＣＰＵ１０２は、ラウンドフラグ値を１減らす。

【００４０】

図９に第一の逆変換処理のフローチャートを示す（図６、図８における（Ｄ））。ＣＰＵ１０２は、補助演算装置１２４へ受信データレジスタ２０４の値を逆変換前データとして送信する（逆変換前データ送信６２１）。補助演算装置１２４は、ＣＰＵ１０２から逆変換前データを受信すると動作を開始する（開始６２２）。補助演算装置１２４は、乱数生成器１２５から乱数値をスイッチパラメータ１１０４として読み込む（乱数値読み込み６２３）。補助演算装置１２４は、スイッチパラメータ１１０４の値を元に補助演算装置内のスイッチマトリクスを切り替える（スイッチマトリクス切り替え６２４）。補助演算装置１２４は、秘密鍵２０２を鍵１１０２として読み込む（鍵読み込み６２５）。補助演算装置１２４は、逆変換前データを入力データ１１０１として入力する（データ入力６２６）。補助演算装置１２４は、鍵を用いて入力データに逆変換（本実施の形態では４５を底とする指数・対数演算と２５７を基数とする剰余処理の逆変換）を施し（逆変換６２８）、出力データ１１０３として出力する（データ出力６２９）。補助演算装置１２４は、

出力データ１１０３を逆変換後データとしてＣＰＵ１０２へ送信し動作を終了する（終了６３０）。ＣＰＵ１０２は、補助演算装置１２４が動作を終了すると逆変換後データを受信し、受信データレジスタ２０４に格納する（逆変換後データ受信６３１）。データ入力６２６からデータ出力６２９までの時間を補助演算時間Ｔとする。補助演算装置１２４では、乱数生成器１２５から読み込んだ乱数値を元に補助演算時間Ｔが変化する。

【００４１】

以上のような形態とすることで、サイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、乱数生成器と補助演算装置を加えることにより、ＩＣチップから漏れる物理的情報の時間変化をより複雑にする。そのため、第３者が傍受した物理的情報から内部情報を取り出すことに時間がかかり、セキュリティを高めることが出来る。また、サイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、サイドチャネル攻撃を阻止する方法が変更になることに伴う仕様の変更により、ＩＣチップのマスク設計の段階から作り直す必要がない。そのため、製造コストの削減及び製造時間の短縮ができる。また、マスク設計の変更によって再度作り直したＩＣチップに不具合が生じているといった懸念もない。

【００４２】

また従来においては、サイドチャネル攻撃を阻止する機能を有するＩＣチップを製造する際においては、サイドチャネル攻撃を阻止する回路を搭載することもあった。しかしながら、本発明を採用することで、サイドチャネル攻撃を阻止する機能を読み出し専用メモリにプログラムとして格納することにより、別途サイドチャネル攻撃を阻止する機能を備えた回路を設ける場合より、ＩＣチップを小型化することができる。そのため、ＩＣチップの軽量化、１枚の基板から作製できるＩＣチップの数の増加に伴うコストの削減、またサイドチャネル攻撃を阻止する機能を備えた回路の分だけ、トランジスタ数が減少することによる歩留まりの向上に貢献することができる。

【００４３】

なお、本実施の形態は、本明細書中の他の実施の形態の記載とも適宜組み合わせて実施することが可能である。

【００４４】

（実施の形態２）

実施の形態１においては、複数のサイドチャネル攻撃阻止ルーチンを有するサイドチャネル攻撃阻止プログラムをＲＯＭに格納することによりＩＣチップがサイドチャネル攻撃を阻止する機能を取りうる構成について示した。本実施の形態においては、実施の形態１とは異なる形態のサイドチャネル攻撃を阻止する機能を実現するための装置構成について説明する。フローチャートについては実施の形態１と同様であるため、必要に応じて実施の形態１で述べた図を用いて説明する。

【００４５】

図１２に本発明におけるサイドチャネル攻撃を阻止する機能を搭載する対象であるＩＣチップのブロック図を示す。図１２は実施の形態１における図１のＩＣチップのブロック図から補助演算装置１２４をのぞいたものであり、図１と同様にＣＰＵ１０２と、ＲＯＭ１０３と、ＲＡＭ１０４と、乱数生成器１２５と、からなる演算回路１０６と、アンテナ１０７と、共振回路１０８と、電源回路１０９と、リセット回路１１０と、クロック生成回路１１１と、復調回路１１２と、変調回路１１３と、電源管理回路１１４とからなるアナログ部１１５と、を有する。コントローラ１０５は、ＣＰＵインターフェース（ＣＰＵＩＦ）１１６と、制御レジスタ１１７と、コード抽出回路１１８と、符号化回路１１９と、から構成される。

【００４６】

このようなＩＣチップにおけるサイドチャネル攻撃を阻止する機能の処理は、実施の形態１と同じであるが、実施の形態１における図９の第一の逆変換処理を補助演算装置１２４の代わりにＣＰＵ１０２が行う。

【００４７】

次に、図１２におけるＩＣチップでの第一の逆変換処理の動作を、図１１のフローチャートと対応させながら説明する。

【００４８】

図１１においてＣＰＵ１０２は、乱数生成器１２５の出力値を元に、後述する逆変換１００３で使用する逆変換パターンを選択する（逆変換パターン選択１００１）。ＣＰＵ１０２は、逆変換を開始する（逆変換開始１００２）。ＣＰＵ１０２は、逆変換パターン選択１００１で選択された逆変換パターンと秘密鍵２０２を用いて受信データレジスタ２０４の値に逆変換（本実施の形態では４５を底とする指数・対数演算と２５７を基数とする剰余処理の逆変換）を施す（逆変換１００３）。ＣＰＵ１０２は、逆変換を終了する（逆変換終了１００４）。逆変換開始１００２から逆変換終了１００４までの時間を演算時間Ｔとする。ＣＰＵ１０２では、乱数生成器１２５から読み込んだ乱数値を元に演算時間Ｔを変化する。

【００４９】

これら機能を有するプログラムをＲＯＭに含み、ＣＰＵ１０２の命令によって処理することで、補助演算装置１２４の必要が無くなり、補助演算装置１２４の分だけ回路を小さくすることが可能になる。

【００５０】

以上のような形態とすることで、サイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、ＩＣチップから漏れる物理的情報の時間変化をより複雑にする。そのため、第３者が傍受した物理的情報から内部情報を取り出すことに時間がかかり、セキュリティを高めることが出来る。また、サイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、サイドチャネル攻撃を阻止する方法が変更になることに伴う仕様の変更により、ＩＣチップのマスク設計の段階から作り直す必要ない。そのため、製造コストの削減及び製造時間の短縮ができる。また、マスク設計の変更によって再度作り直したＩＣチップに不具合が生じているといった懸念もない。

【００５１】

また従来においては、サイドチャネル攻撃を阻止する機能を有するＩＣチップを製造する際においては、サイドチャネル攻撃を阻止する回路を搭載することもあった。しかしながら、本発明を採用することで、サイドチャネル攻撃を阻止する機能を読み出し専用メモリにプログラムとして格納することにより、別途サイドチャネル攻撃を阻止する機能を備えた回路を設ける場合より、ＩＣチップを小型化することができる。そのため、ＩＣチップの軽量化、１枚の基板より作製できるＩＣチップの数の増加に伴うコストの削減、またサイドチャネル攻撃を阻止する機能を備えた回路の分だけ、トランジスタ数が減少することによる歩留まりの向上に貢献することができる。

【００５２】

なお、本実施の形態は、本明細書中の他の実施の形態の記載とも適宜組み合わせて実施することが可能である。

【００５３】

（実施の形態３）

本実施の形態では、絶縁基板上に形成された薄膜トランジスタによりＩＣチップを形成する形態について説明する。

【００５４】

図１３（Ａ）に示すように、絶縁基板１３００を用意する。絶縁基板１３００には、ガラス基板、石英基板、プラスチック基板等が挙げられる。また、これら基板において、その裏面を研磨する等の手法によって薄くすることができる。さらに、金属元素等の導電性基板や、シリコン等の半導体性基板上に絶縁性を有する材料を用いて層を形成した基板を用いることも可能である。ＩＣチップを、例えばプラスチック基板に形成することにより、柔軟性が高く、軽量で薄型な装置を作製することができる。

【００５５】

絶縁基板１３００上に剥離層１３０１を選択的に形成する。勿論、剥離層１３０１を絶

縁基板１３００全面に形成しても良い。剥離層１３０１はスパッタリング法やプラズマＣＶＤ法等により、タングステン（Ｗ）、モリブデン（Ｍｏ）、チタン（Ｔｉ）、タンタル（Ｔａ）、ニオブ（Ｎｂ）、ニッケル（Ｎｉ）、コバルト（Ｃｏ）、ジルコニウム（Ｚｒ）、亜鉛（Ｚｎ）、ルテニウム（Ｒｕ）、ロジウム（Ｒｈ）、パラジウム（Ｐｄ）、オスミウム（Ｏｓ）、イリジウム（Ｉｒ）、珪素（Ｓｉ）から選択された元素、又は元素を主成分とする合金材料、又は元素を主成分とする化合物材料からなる層を、単層又は積層して形成する。珪素を含む層の結晶構造は、非晶質、微結晶、多結晶のいずれの場合でもよい。

【００５６】

剥離層１３０１上に下地層１３０２を形成する。下地層１３０２は、酸化珪素、窒化珪素、または酸化窒化珪素等の絶縁性を有する材料を用い、単層構造または積層構造で形成することができる。積層構造を用いる場合、下地層１３０２の一層目として、膜厚１０ｎｍ以上２００ｎｍ以下（好ましくは５０ｎｍ以上１００ｎｍ以下）の酸化窒化珪素層を形成する。当該酸化窒化珪素層は、プラズマＣＶＤ法を用い、SiH_4、NH_3、N_2O及びH_2を反応ガスとして形成することができる。次いで下地層１３０２の二層目として、膜厚５０ｎｍ以上２００ｎｍ以下（好ましくは１００ｎｍ以上１５０ｎｍ以下）の酸化窒化珪素層を形成する。当該酸化窒化珪素層は、プラズマＣＶＤ法を用い、SiH_4及びN_2Oを反応ガスとして形成することができる。

【００５７】

下地層１３０２上に半導体層１３０４を形成する。半導体層１３０４は、シリコン材料、又はシリコンとゲルマニウムからなる材料等、シリコン半導体層を用いて形成することができる。半導体層１３０４の結晶構造は非晶質、微結晶、多結晶のいずれでもよい。

【００５８】

多結晶の半導体層を形成するには、非晶質半導体層に対して加熱処理を行う手法がある。加熱処理には、レーザ照射、加熱炉、ランプ照射等が挙げられ、これらのいずれか一又は複数を用いることができる。

【００５９】

レーザ照射には、連続発振型のレーザビーム（ＣＷレーザ）やパルス発振型のレーザビーム（パルスレーザ）を用いることができる。レーザビームとしては、Ａｒレーザ、Ｋｒレーザ、エキシマレーザ、ＹＡＧレーザ、Y_2O_3レーザ、YVO_4レーザ、ＹＬＦレーザ、YA_1O_3レーザ、ガラスレーザ、ルビーレーザ、アレキサンドライトレーザ、Ｔｉ：サファイヤレーザ、銅蒸気レーザまたは金蒸気レーザのうち一種または複数種から発振されるものを用いることができる。このようなレーザビームの基本波と、当該基本波の第２高調波から第４高調波といった高調波のレーザビームのいずれかを照射することで、粒径の大きな結晶を有するシリコン層を得ることができる。高調波には、Ｎｄ：YVO_4レーザ（基本波１０６４ｎｍ）の第２高調波（５３２ｎｍ）や第３高調波（３５５ｎｍ）を用いることができる。レーザ照射におけるエネルギー密度は０．０１～１００ＭＷ／ｃｍ^{2}程度（好ましくは０．１～１０ＭＷ／ｃｍ^2）が必要である。そして、走査速度を１０～２０００ｃｍ／ｓｅｃ程度として照射する。

【００６０】

なお、基本波のＣＷレーザと高調波のＣＷレーザとを照射するようにしてもよいし、基本波のＣＷレーザと高調波のパルスレーザとを照射するようにしてもよい。複数のレーザ光を照射することにより、広範囲のエネルギー領域を補うことができる。

【００６１】

また、パルスレーザであって、非晶質状態を有するシリコン層がレーザによって溶融してから固化するまでに、次のパルスのレーザを照射できるような発振周波数でレーザを発振させるレーザビームを用いることもできる。このような周波数でレーザを発振させることで、走査方向に向かって連続的に成長した結晶粒を有するシリコン層を得ることができる。このようなレーザの発振周波数は１０ＭＨｚ以上であり、通常用いられている数十Ｈｚ～数百Ｈｚの周波数帯よりも著しく高い。

【００６２】
加熱処理として加熱炉を用いる場合には、非晶質状態を有する半導体層を４００～５５０℃で２～２０時間かけて加熱する。このとき、徐々に高温となるように温度を４００～５５０℃の範囲で多段階に設定するとよい。最初の４００℃程度の低温加熱工程により、非晶質状態を有する半導体層に含まれる水素等が出てくるため、結晶化の際に層表面が荒れるのを低減することができる。
【００６３】
上記加熱処理の工程において、半導体層の結晶化を促進させる金属、例えばニッケル（Ｎｉ）を添加する。例えば、非晶質状態を有する珪素層上にニッケルを含む溶液を塗布し、加熱処理を行うことができる。このように金属を用いて加熱処理を行うことで、加熱温度を低減することができ、さらに、結晶粒界の連続した多結晶珪素層を得ることができる。ここで結晶化を促進するための金属としてはＮｉの他に、鉄（Ｆｅ）、ルテニウム（Ｒｕ）、ロジウム（Ｒｈ）、パラジウム（Ｐｄ）、オスミウム（Ｏｓ）、イリジウム（Ｉｒ）、白金（Ｐｔ）、銅（Ｃｕ）、銀（Ａｕ）等を用いることもできる。
【００６４】
結晶化を促進させる金属はメモリセル等の汚染源となるため、半導体層を結晶化した後に、金属を除去するゲッタリング工程を行うことが望ましい。ゲッタリング工程では、半導体層を結晶化した後、半導体層上にゲッタリングシンクとなる層を形成し、加熱することで金属をゲッタリングシンクへ移動させる。ゲッタリングシンクには、多結晶半導体層や不純物が添加された半導体層を用いることができる。例えば、多結晶珪素層上にアルゴン等の不活性元素が添加された多結晶半導体層を形成し、これをゲッタリングシンクとして用いることができる。ゲッタリングシンクに不活性元素を添加することによって、ひずみを生じさせ、より効率的に金属を捕獲することができる。また新たにゲッタリングシンクを形成することなく、ＴＦＴの半導体層の一部にリン等の元素を添加することによって、金属を捕獲することもできる。
【００６５】
このように形成された半導体層を、所定の形状に加工し、島状の半導体層１３０４を形成する。加工手段には、フォトリソグラフィ法によって形成されたマスクを用いて、エッチングする。エッチングには、ウェットエッチング法又はドライエッチング法を適用することができる。
【００６６】
半導体層１３０４を覆うようにゲート絶縁層１３０５として機能する絶縁層を形成する。ゲート絶縁層１３０５は、下地層１３０２と同様の材料、方法により形成することができる。
【００６７】
図１３（Ｂ）に示すように、ゲート絶縁層１３０５を介してゲート電極層１３０６として機能する導電層を形成する。ゲート電極層１３０６はアルミニウム（Ａｌ）、チタン（Ｔｉ）、モリブデン（Ｍｏ）、タンタル（Ｔａ）、タングステン（Ｗ）もしくはシリコン（Ｓｉ）の元素からなる膜又はこれらの元素を有する合金膜を用いることができる。ゲート電極層１３０６は、単層構造又は積層構造とすることができ、積層構造として窒化タンタルとタングステンの積層構造を適用することができる。ゲート電極層１３０６の加工手段には、フォトリソグラフィ法によって形成されたマスクを用いて、エッチングする。エッチングには、ウェットエッチング法又はドライエッチング法を適用することができる。
【００６８】
ゲート電極層１３０６の側面にサイドウォール１３０７と呼ばれる絶縁物を形成する。サイドウォール１３０７は、下地層１３０２と同様の材料、方法により形成することができる。またサイドウォール１３０７の端部にテーパ形状を有するためには、等方性エッチングを用いればよい。サイドウォール１３０７により、ゲート長が狭くなるにつれて生じる短チャネル効果を防止することができる。短チャネル効果はＮチャネル型ＴＦＴに顕著であるため、少なくともＮチャネル型ＴＦＴのゲート電極側面に設けるとよい。

【００６９】
このような状態で、ゲート絶縁層１３０５をエッチングする。その結果、半導体層１３０４の一部や下地層１３０２が露出する。エッチングには、ウェットエッチング法又はドライエッチング法を適用することができる。
【００７０】
そして、ゲート電極層１３０６、及びサイドウォール１３０７を用いて、半導体層１３０４に不純物元素を添加し、高濃度不純物領域１３１０、１３１２を形成する。Ｎチャネル型ＴＦＴとする場合、不純物元素はリン（Ｐ）を用い、Ｐチャネル型ＴＦＴとする場合、不純物元素はボロン（Ｂ）を用いることができる。このとき、不純物元素の添加量によっては、サイドウォール１３０７下方に低濃度不純物領域が形成される。本実施の形態ではＮチャネル型の不純物領域にのみ低濃度不純物領域１３１１を形成する。低濃度不純物領域１３１１は、短チャネル効果を防止することができるからである。このような低濃度不純物領域を有する構造をＬＤＤ（Ｌｉｇｈｔｌｙ　Ｄｏｐｅｄ　Ｄｒａｉｎ）構造と呼ぶ。
【００７１】
その後、下地層１３０２、半導体層１３０４、ゲート電極層１３０６、サイドウォール１３０７を覆うように絶縁層１３１４を形成する。絶縁層１３１４は、ＣＶＤ法によってシリコンを有する材料から形成するとよい。
【００７２】
絶縁層１３１４を形成後、必要に応じて加熱処理を行う。加熱処理には、上記結晶化と同様な手段を用いることができる。加熱処理により、不純物領域の活性化を行うことができる。ＣＶＤ法により形成された絶縁層１３１４は、水素を多く含むため、上記加熱処理により水素が拡散し、不純物領域の膜あれを低減することができる。
【００７３】
図１３（Ｃ）に示すように、層間膜として機能する絶縁層１３１５、１３１６を形成する。絶縁層１３１５、１３１６には、無機材料又は有機材料を用いることができる。無機材料は、酸化珪素、窒化珪素、酸化窒化珪素等を用いることができる。有機材料はポリイミド、アクリル、ポリアミド、ポリイミドアミド、レジスト又はベンゾシクロブテン、シロキサン、ポリシラザンを用いることができる。なお、シロキサンとは、シリコン（Ｓｉ）と酸素（Ｏ）との結合で骨格構造が構成される。置換基として、少なくとも水素を含む有機基（例えばアルキル基、芳香族炭化水素）が用いられる。置換基として、フルオロ基を用いてもよい。または置換基として、少なくとも水素を含む有機基と、フルオロ基とを用いてもよい。ポリシラザンは、シリコン（Ｓｉ）と窒素（Ｎ）の結合を有するポリマー材料を出発原料として形成される。無機材料を用いると不純物元素の侵入を防止することができ、有機材料を用いると平坦性を高めることができる。そのため、本実施の形態では、絶縁層１３１５に無機材料を用い、絶縁層１３１６に有機材料を用いる。
【００７４】
絶縁層１３１４、１３１５、１３１６にコンタクトホールを形成して配線１３１８を形成する。配線１３１８は、アルミニウム（Ａｌ）、チタン（Ｔｉ）、モリブデン（Ｍｏ）、タンタル（Ｔａ）、タングステン（Ｗ）もしくはシリコン（Ｓｉ）の元素からなる膜又はこれらの元素を有する合金膜を用いることができる。配線１３１８は、単層構造又は積層構造を用いることができ、例えば第一層にタングステン、窒化タングステン等を用い、第二層にアルミニウムとシリコンの合金（Ａｌ－Ｓｉ）、アルミニウムとチタンの合金（Ａｌ－Ｔｉ）を用い、第三層に窒化チタン膜、チタン膜等を順次積層した構造を適用することができる。配線１３１８の加工には、フォトリソグラフィ法で形成されたマスクを用いて、エッチングする。エッチングには、ウェットエッチング法又はドライエッチング法を適用することができる。配線１３１８は、半導体層１３０４では不純物領域に接続し、このような配線をソース電極、ドレイン電極と呼ぶことができる。
【００７５】
このようにして、Ｎチャネル型ＴＦＴ１３３０、Ｐチャネル型ＴＦＴ１３３１を形成す

ることができる。

【００７６】

その後必要に応じて、配線１３１８上に保護膜１３１９を形成する。保護膜１３１９は、珪素を有する酸化物、又は珪素を有する窒化物によって形成することができる。例えば、窒化珪素を用いて保護膜１３１９を形成する。その結果、水分や酸素の侵入を防止することができる。

【００７７】

図１３（Ｄ）に示すように、ＴＦＴ間に開口部を形成し、エッチング剤１３２５を導入する。開口部はウェットエッチング法又はドライエッチング法を用いて形成することができる。なお開口部の形成位置は、ＴＦＴ間でなくともよく、半導体層１３０４が形成されない領域であればよい。エッチング剤１３２５は、ウェットエッチング法であれば、フッ酸を水やフッ化アンモニウムで希釈した混液、フッ酸と硝酸の混液、フッ酸と硝酸と酢酸の混液、過酸化水素と硫酸の混液、過酸化水素とアンモニウム水と水の混液、過酸化水素と塩酸と水の混液等を用いる。また、ドライエッチング法であれば、フッ素等のハロゲン系の原子や分子を含む気体、又は酸素を含む気体を用いる。好ましくは、エッチング剤として、フッ化ハロゲン又はハロゲン間化合物を含む気体又は液体、例えば三フッ化塩素（ClF_3）を適用することができる。

【００７８】

エッチング剤を導入することにより、剥離層１３０１が除去される。すると、絶縁基板１３００が剥離される。このようにして、薄型化、軽量化を達成したＩＣチップを形成することができる。

【００７９】

エッチング剤を導入する方法以外に、レーザ描画により剥離層１３０１を露出させたり、ＩＣチップの側面に切り込みを入れる等して、物理的に絶縁基板１３００を剥離させてもよい。

【００８０】

図１３（Ｅ）に示すように、フィルム１３２７、１３２８によって覆い、ＩＣチップを完成させることができる。このとき、接着層１３２９を用いて、フィルム１３２７や１３２８と貼り合わせてもよい。フィルム１３２７、１３２８には、水分や酸素等の侵入を防ぐために、保護膜を形成しても良い。また配線１３１８上には保護膜１３１９が形成されているため、下地層１３０２又は接着層１３２９の下方に保護膜を形成してもよい。保護膜は、珪素を有する酸化物、又は珪素を有する窒化物によって形成することができる。

【００８１】

このように絶縁基板上、さらに絶縁基板を剥離したＩＣチップは、より軽量で安価に提供することができる。またこのようなＩＣチップは柔軟性に富むため、曲面に貼り付けることも可能である。

【００８２】

また、本実施の形態は、本明細書中の他の実施の形態の記載とも適宜組み合わせて実施することが可能である。そのため、本発明の半導体装置のサイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、ＩＣチップから漏れる物理的情報の時間変化をより複雑にする。そのため、第３者が傍受した物理的情報から内部情報を取り出すことに時間がかかり、セキュリティを高めることが出来る。また、サイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、サイドチャネル攻撃を阻止する方法が変更になることに伴う仕様の変更により、ＩＣチップのマスク設計の段階から作り直す必要がなくなる。そのため、製造コストの削減及び製造時間の短縮ができる。また、マスク設計の変更によって再度作り直したＩＣチップに不具合が生じているといった懸念もない。

【００８３】

また従来においては、サイドチャネル攻撃を阻止する機能を有するＩＣチップを製造する際においては、サイドチャネル攻撃を阻止する回路を搭載することもあった。しかしながら、本発明を採用することで、サイドチャネル攻撃を阻止する機能を読み出し専用メモ

リにプログラムとして格納することにより、別途サイドチャネル攻撃を阻止する機能を備えた回路を設ける場合より、ＩＣチップを小型化することができる。そのため、ＩＣチップの軽量化、１枚の基板より作製できるＩＣチップの数の増加に伴うコストの削減、またサイドチャネル攻撃を阻止する機能を備えた回路の分だけ、トランジスタ数が減少することによる歩留まりの向上などに貢献することができる。

【００８４】

（実施の形態４）

本実施の形態では、単結晶シリコンに形成されたトランジスタによりＩＣチップを形成する形態について図１４を用いて説明する。

【００８５】

まず、図１４（Ａ）を用いて、トランジスタの作製工程について説明する。単結晶のシリコン基板１９０１を用意する。そして、シリコン基板１９０１の主面（素子形成面または回路形成面）の第１の素子形成領域にｎ型ウェル１９０２を、第２の素子形成領域にｐ型ウェル１９０３をそれぞれ選択的に形成する。また、シリコン基板１９０１の裏面を研磨する等の手法によって薄くすることも可能である。予め、シリコン基板１９０１を薄膜化することによって、軽量で薄型な半導体装置を作製することができる。

【００８６】

次いで、第１の素子形成領域と第２の素子形成領域とを区画するための素子分離領域となるフィールド酸化膜１９０４を形成する。フィールド酸化膜１９０４は厚い熱酸化膜であり、ＬＯＣＯＳ（ｌｏｃａｌ　ｏｘｉｄａｔｉｏｎ　ｏｆ　ｓｉｌｉｃｏｎ）法を用いて形成すればよい。なお、素子分離法は、ＬＯＣＯＳ法に限定されず、例えば素子分離領域はトレンチ分離法を用いてトレンチ構造を有していてもよいし、ＬＯＣＯＳ構造とトレンチ構造の組み合わせであってもよい。

【００８７】

次いで、シリコン基板の表面を、例えば熱酸化させることによってゲート絶縁膜を形成する。ゲート絶縁膜は、ＣＶＤ法を用いて形成してもよく、酸化窒化珪素膜や酸化珪素膜や窒化珪素膜やそれらの積層膜を用いることができる。

【００８８】

次いで、ポリシリコン層１９０５ｂ、１９０６ｂとシリサイド層１９０５ａ、１９０６ａとの積層膜を全面に形成し、リソグラフィ技術およびドライエッチング技術に基づき積層膜を形成することによってゲート絶縁膜上にポリサイド構造を有するゲート電極１９０５、１９０６を形成する。ポリシリコン層１９０５ｂ、１９０６ｂは低抵抗化するために予め、10^{21}／cm^3程度の濃度でリン（Ｐ）をドープしておいても良いし、ポリシリコン膜を形成した後で濃いｎ型不純物を拡散させても良い。また、シリサイド層１９０５ａ、１９０６ａを形成する材料はモリブデンシリサイド（ＭｏＳｉｘ）、タングステンシリサイド（ＷＳｉｘ）、タンタルシリサイド（ＴａＳｉｘ）、チタンシリサイド（ＴｉＳｉｘ）などを適用することが可能である。

【００８９】

次いで、エクステンション領域を形成するために、ゲート絶縁膜を介してシリコン半導体基板にイオン注入を行う。本実施例においては、各ソース領域およびドレイン領域とチャネル形成領域との間に形成された不純物領域をエクステンション領域と呼ぶ。エクステンション領域１９０７、１９０８の不純物濃度は、ソース領域およびドレイン領域の不純物濃度よりも低い場合もあるし、同等の場合もあるし、高い場合もある。即ち、エクステンション領域の不純物濃度は、半導体装置に要求される特性に基づいて決定すればよい。

【００９０】

本実施例は、本発明に適用されるＣＭＯＳ回路を製造する場合であるので、ｐチャネル型ＦＥＴを形成すべき第１の素子形成領域をレジスト材料で被覆し、ｎ型不純物であるヒ素（Ａｓ）やリン（Ｐ）をシリコン基板に注入する。また、ｎチャネル型ＦＥＴを形成すべき第２の素子形成領域をレジスト材料で被覆し、ｐ型不純物であるボロン（Ｂ）をシリコン基板に注入する。

【００９１】
次いで、イオン注入された不純物の活性化および、イオン注入によって発生したシリコン基板における結晶欠陥を回復するために、第１回目の活性化処理を行う。Ｓｉの融点程度の温度まで半導体基板を加熱して活性化する。
【００９２】
次いで、ゲート電極の側壁にサイドウォール１９０９、１９１０を形成する。例えば酸化珪素からなる絶縁材料層を全面にＣＶＤ法にて堆積させ、かかる絶縁材料層をエッチバックすることによってサイドウォールを形成すればよい。エッチバックの際に自己整合的にゲート絶縁膜を選択的に除去してもよい。また、エッチバック後にゲート絶縁膜のエッチングを行ってもよい。こうして、ゲート電極の幅と、そのゲート電極の側壁の両側に設けられたサイドウォールの幅とを合計した幅を有するゲート絶縁膜１９１１、１９１２が形成される。
【００９３】
次いで、ソース領域およびドレイン領域を形成するために、露出したシリコン基板にイオン注入を行う。ｐチャネル型ＦＥＴを形成すべき第１の素子形成領域をレジスト材料で被覆し、ｎ型不純物であるヒ素（Ａｓ）やリン（Ｐ）をシリコン基板に注入してソース領域１９１３及びドレイン領域１９１４を形成する。また、ｎチャネル型ＦＥＴを形成すべき第２の素子形成領域をレジスト材料で被覆し、ｐ型不純物であるボロン（Ｂ）をシリコン基板に注入してソース領域１９１５及びドレイン領域１９１６を形成する。
【００９４】
次いで、イオン注入された不純物の活性化および、イオン注入によって発生したシリコン基板における結晶欠陥を回復するために、第２回目の活性化処理を行う。
【００９５】
そして、活性化後に層間絶縁膜やプラグ電極やメタル配線等を形成する。第１の層間絶縁膜１９１７は、プラズマＣＶＤ法や減圧ＣＶＤ法を用いて酸化シリコン膜や酸化窒化シリコン膜などを形成する。さらにその上にリンガラス（ＰＳＧ）、あるいはボロンガラス（ＢＳＧ）、もしくはリンボロンガラス（ＰＢＳＧ）の第２の層間絶縁膜１９１８が形成する。第２の層間絶縁膜１９１８は、平坦性を上げるため、スピンコート法や常圧ＣＶＤ法で作製する。なお、層間絶縁膜は単層であってもよいし、３層以上の多層構造であってもよい。
【００９６】
ソース電極１９１９、１９２１、及びドレイン電極１９２０、１９２２は、第１の層間絶縁膜１９１７および第２の層間絶縁膜１９１８にそれぞれのＦＥＴのソース領域及びドレイン領域に達するコンタクトホールを形成した後に形成するもので、低抵抗材料として通常良く用いられるアルミニウム（Ａｌ）を用いると良い。また、ＡｌとチタンＴｉ）の積層構造としても良い。
【００９７】
なお、コンタクト穴は、電子線直接描画技術によって形成してもよい。電子線直接描画は、ポジ型の電子線描画用レジストを第１の層間絶縁膜１９１７及び第２の層間絶縁膜１９１８上の全面に形成し、電子線が照射された部分を現像液によって溶解させる。そして、コンタクト穴が形成される箇所のレジストに穴が空き、レジストをマスクとしてドライエッチングを行なうことにより、所定の位置の第１の層間絶縁膜１９１７及び第２の層間絶縁膜１９１８がエッチングされてコンタクト穴を形成することができる。
【００９８】
最後に、パッシベーション膜１９２３を形成する。図１４（Ａ）において向かって左側がｐチャネル型トランジスタ１９２５であり、右側がｎチャネル型トランジスタ１９２６である。
【００９９】
パッシベーション膜１９２３は、プラズマＣＶＤ法で窒化シリコン膜、または酸化シリコン膜、あるいは窒化酸化シリコン膜で形成されている。また、窒化シリコン膜等の代わ

りに有機樹脂膜、若しくはパッシベーション膜の上に有機樹脂膜を積層してもよい。有機樹脂材料として、ポリイミド、ポリアミド、アクリル、ベンゾシクロブテン（ＢＣＢ）などを用いることができる。有機樹脂膜を用いる利点は、膜の形成方法が簡単である点や、比誘電率が低いので寄生容量を低減できる点、平坦化するのに適している点などがある。勿論、上述した以外の有機樹脂膜を用いても良い。

【０１００】

このようにして、単結晶基板上にｐチャネル型トランジスタ１９２５とｎチャネル型トランジスタ１９２６を形成することができる。

【０１０１】

なお、ｐチャネル型トランジスタ１９２５とｎチャネル型トランジスタ１９２６の作製された基板において、その裏面を研磨する等の手法によってさらに半導体装置を薄くしてもよい。シリコン基板をさらに薄膜化することによって、軽量で薄型な半導体装置を作製することができる。

【０１０２】

そして、図１４（Ｂ）に示すように、フィルム１９２７、１９２８によって覆い、ＩＣチップを完成させることができる。フィルム１９２７、１９２８には、水分や酸素等の侵入を防ぐために、保護膜を形成しても良い。保護膜は、珪素を有する酸化物、又は珪素を有する窒化物によって形成することができる。また、フィルムにはＩＣチップのアンテナとなるパターンが形成されていてもよい。

【０１０３】

このように単結晶基板上に形成されたＩＣチップは、軽量でより小型化された製品を提供することができる。またこのようなＩＣチップは小型化された半導体装置を作成することができ、トランジスタのばらつきも小さいため、好適である。

【０１０４】

また、本実施の形態は、本明細書中の他の実施の形態の記載とも適宜組み合わせて実施することが可能である。そのため、本発明の半導体装置のサイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、ＩＣチップから漏れる物理的情報の時間変化をより複雑にする。そのため、第３者が傍受した物理的情報から内部情報を取り出すことに時間がかかり、セキュリティを高めることが出来る。また、サイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、サイドチャネル攻撃を阻止する方法が変更になることに伴う仕様の変更により、ＩＣチップのマスク設計の段階から作り直す必要がなくなる。そのため、製造コストの削減及び製造時間の短縮ができる。また、マスク設計の変更によって再度作り直したＩＣチップに不具合が生じているといった懸念もない。

【０１０５】

また従来においては、サイドチャネル攻撃を阻止する機能を有するＩＣチップを製造する際においては、サイドチャネル攻撃を阻止する回路を搭載することもあった。しかしながら、本発明を採用することで、サイドチャネル攻撃を阻止する機能を読み出し専用メモリにプログラムとして格納することにより、サイドチャネル攻撃を阻止する機能を備えた回路の分だけ、ＩＣチップを小型化することができる。そのため、ＩＣチップの軽量化、１枚の基板から作製できるＩＣチップの数の増加に伴うコストの削減、またサイドチャネル攻撃を阻止する機能を備えた回路の分だけ、トランジスタ数が減少することによる歩留まりの向上に貢献することができる。

【０１０６】

（実施の形態５）

本実施の形態では、本発明における半導体装置の例として、暗号処理機能を有するＩＣチップについて図１５を用いて説明する。

【０１０７】

まず、図１５を用いてＩＣチップのブロック構成を説明する。図１５において、ＩＣチップ１０１は、ＣＰＵ１０２と、ＲＯＭ１０３と、ＲＡＭ１０４と、コントローラ１０５と、からなる演算回路１０６と、アンテナ１０７と、共振回路１０８と、電源回路１０９

と、リセット回路１１０と、クロック生成回路１１１と、復調回路１１２と、変調回路１１３と、電源管理回路１１４と、からなるアナログ部１１５と、を有する。コントローラ１０５は、ＣＰＵインターフェース（ＣＰＵＩＦ）１１６と、制御レジスタ１１７と、コード抽出回路１１８と、符号化回路１１９と、から構成される。なお、図１５では、説明の簡単化のため、通信信号を受信信号１２０と、送信信号１２１とに分けて示したが、実際には、両者は重ね合わされており、ＩＣチップ１０１及びリーダライタの間で同時に送受信される。受信信号１２０は、アンテナ１０７と共振回路１０８とで受信された後、復調回路１１２により復調される。また、送信信号１２１は、変調回路１１３により変調された後、アンテナ１０７より送信される。

【０１０８】

図１５において、通信信号により形成される磁界中にＩＣチップ１０１を置くと、アンテナ１０７と共振回路１０８により、誘導起電力を生じる。誘導起電力は、電源回路１０９における電気容量により保持され、また電気容量によって電位が安定化され、ＩＣチップ１０１の各回路に電源電圧として供給される。リセット回路１１０は、ＩＣチップ１０１全体の初期リセット信号を生成する。例えば、電源電圧の上昇に遅延して立ち上がる信号をリセット信号として生成する。クロック生成回路１１１は、電源管理回路１１４より生成される制御信号に応じて、クロック信号の周波数とデューティー比を変更する。復調回路１１２は、ＡＳＫ方式の受信信号１２０の振幅の変動を”０”／”１”の受信データ１２２として検出する。復調回路１１２は、例えばローパスフィルターとする。さらに、変調回路１１３は、送信データをＡＳＫ方式の送信信号１２１の振幅を変動させて送信する。例えば、送信データ１２３が”０”の場合、共振回路１０８の共振点を変化させ、通信信号の振幅を変化させる。電源管理回路１１４は、電源回路１０９より演算回路１０６に供給される電源電圧または演算回路１０６における消費電流を監視し、クロック生成回路１１１において、クロック信号の周波数とデューティー比を変更するための制御信号を生成する。

【０１０９】

本実施の形態におけるＩＣチップの動作を説明する。まず、ＩＣチップ１０１は、リーダライタより送信された暗号文データを含む受信信号１２０を受信する。受信信号１２０は、復調回路１１２で復調された後、コード抽出回路１１８で制御コマンドや暗号文のデータなどに分解され、制御レジスタ１１７に格納される。ここで、制御コマンドは、ＩＣチップ１０１の応答を指定するデータである。例えば、固有ＩＤ番号の送信、動作停止、暗号解読などを指定する。ここでは、暗号解読に指定した制御コマンドを受信したとする。

【０１１０】

続いて、演算回路１０６において、ＣＰＵ１０２が、ＲＯＭ１０３に格納された暗号解読プログラムにしたがって、ＲＯＭ１０３にあらかじめ格納された秘密鍵３００１を用いて暗号文を解読（復号）する。復号された暗号文（復号文）は、制御レジスタ１１７に格納される。この際、ＲＡＭ１０４をデータ格納領域として用いる。なお、ＣＰＵ１０２は、ＣＰＵＩＦ１１６を介してＲＯＭ１０３、ＲＡＭ１０４、制御レジスタ１１７にアクセスする。ＣＰＵＩＦ１１６は、ＣＰＵ１０２が要求するアドレスより、ＲＯＭ１０３、ＲＡＭ１０４、制御レジスタ１１７のいずれかに対するアクセス信号を生成する機能を有している。

【０１１１】

最後に、符号化回路１１９において、復号文から送信データ１２３を生成し、変調回路１１３で変調し、アンテナ１０７より送信信号１２１をリーダライタに送信する。

【０１１２】

なお、本実施の形態では、演算方式として、ソフトウェア的に処理する方式、すなわち、ＣＰＵと大規模メモリとで演算回路を構成し、プログラムをＣＰＵで実行する方式について説明したが、目的に応じて最適な演算方式を選び、当該方式に基づいて構成することも可能である。例えば、演算方式として、他にも、演算をハードウェア的に処理する方式

と、ハードウェア及びソフトウェアを併用する方式と、が考えられる。ハードウェア的に処理する方式では、専用回路で演算回路を構成すれば良い。ハードウェア及びソフトウェアを併用する方式では、専用回路と、ＣＰＵと、メモリと、で演算回路を構成し、専用回路で演算処理の一部分を行い、残りの演算処理のプログラムをＣＰＵで実行すれば良い。

【０１１３】

また、本実施の形態は、本明細書中の他の実施の形態の記載とも適宜組み合わせて実施することが可能である。そのため、本発明の半導体装置のサイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、ＩＣチップから漏れる物理的情報の時間変化をより複雑にする。そのため、第３者が傍受した物理的情報から内部情報を取り出すことに時間がかかり、セキュリティを高めることが出来る。また、サイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、サイドチャネル攻撃を阻止する方法が変更になることに伴う仕様の変更により、ＩＣチップのマスク設計の段階から作り直す必要ない。そのため、製造コストの削減及び製造時間の短縮ができる。また、マスク設計の変更によって再度作り直したＩＣチップに不具合が生じているといった懸念もない。

【０１１４】

また従来においては、サイドチャネル攻撃を阻止する機能を有するＩＣチップを製造する際においては、サイドチャネル攻撃を阻止する回路を搭載することもあった。しかしながら、本発明を採用することで、サイドチャネル攻撃を阻止する機能を読み出し専用メモリにプログラムとして格納することにより、別途サイドチャネル攻撃を阻止する機能を備えた回路を設ける場合より、ＩＣチップを小型化することができる。そのため、ＩＣチップの軽量化、１枚の基板から作製できるＩＣチップの数の増加に伴うコストの削減、またサイドチャネル攻撃を阻止する機能を備えた回路の分だけ、トランジスタ数が減少することによる歩留まりの向上に貢献することができる。

【０１１５】

（実施の形態６）

アンテナは、電波法に定められた範囲内で目的に見合った大きさ、形状であればよい。送受信される信号は、１２５ｋＨｚ、１３．５６ＭＨｚ、９１５ＭＨｚ、２．４５ＧＨｚなどがあり、それぞれＩＳＯ規格などが設定される。具体的なアンテナとしては、ダイポールアンテナ、パッチアンテナ、ループアンテナ、八木アンテナなどを用いればよい。本実施の形態では、ＩＣチップに接続されるアンテナ形状について説明する。

【０１１６】

図１６（Ａ）にＩＣチップ１６０１に接続されるアンテナ１６０２を示す。図１６（Ａ）において、ＩＣチップ１６０１が中心部に設けられ、アンテナ１６０２はＩＣチップ１６０１の接続端子に接続されている。アンテナの長さを確保するため、アンテナ１６０２は矩形状に折れ曲がっている。

【０１１７】

図１６（Ｂ）には、ＩＣチップ１６０１が一端側に設けられ、アンテナ１６０３はＩＣチップ１６０１の接続端子に接続されている。アンテナの長さを確保するため、アンテナ１６０３は矩形状に折れ曲がっている。

【０１１８】

図１６（Ｃ）には、ＩＣチップ１６０１の両端に矩形状に折れ曲がったアンテナ１６０４が設けられている。

【０１１９】

図１６（Ｄ）には、ＩＣチップ１６０１の両端に直線上のアンテナ１６０５が設けられている。

【０１２０】

このようにアンテナの形状はＩＣチップの構造若しくは偏波、又は用途に見合ったものを選択すればよい。そのため、ダイポールアンテナであれば折り返しダイポールアンテナであってもよい。ループアンテナであれば、円形ループアンテナ、方形ループアンテナであってもよい。パッチアンテナであれば円形パッチアンテナ、方形アンテナであってもよ

い。

【０１２１】

パッチアンテナの場合、セラミック等の誘電材料を用いたアンテナを用いればよい。パッチアンテナの基板として用いる誘電材料の誘電率を高くすることによってアンテナを小型化することができる。また、パッチアンテナの場合、機械強度が高いため、繰り返し使用することが可能である。

【０１２２】

パッチアンテナの誘電材料は、セラミック、有機樹脂、又はセラミックと有機樹脂の混合物等で形成することができる。セラミックの代表例としては、アルミナ、ガラス、フォルステライト等が挙げられる。さらには、複数のセラミックを混合して用いてもよい。また、高い誘電率を得るためには、誘電体層を、強誘電体材料で形成することが好ましい。強誘電体材料の代表例としては、チタン酸バリウム（$BaTiO_3$）、チタン酸鉛（$PbTiO_3$）、チタン酸ストロンチウム（$SrTiO_3$）、ジルコン酸鉛（$PbZrO_3$）、ニオブ酸リチウム（$LiNbO_3$）、チタン酸ジルコン鉛（ＰＺＴ）等が挙げられる。さらには、複数の強誘電体材料を混合して用いてもよい。

【０１２３】

また、本実施の形態は、本明細書中の他の実施の形態の記載とも適宜組み合わせて実施することが可能である。そのため、本発明の半導体装置のサイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、ＩＣチップから漏れる物理的情報の時間変化をより複雑にする。そのため、第３者が傍受した物理的情報から内部情報を取り出すことに時間がかかり、セキュリティを高めることが出来る。また、サイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、サイドチャネル攻撃を阻止する方法が変更になることに伴う仕様の変更により、ＩＣチップのマスク設計の段階から作り直す必要ない。そのため、製造コストの削減及び製造時間の短縮ができる。また、マスク設計の変更によって再度作り直したＩＣチップに不具合が生じているといった懸念もない。

【０１２４】

また従来においては、サイドチャネル攻撃を阻止する機能を有するＩＣチップを製造する際においては、サイドチャネル攻撃を阻止する回路を搭載することもあった。しかしながら、本発明を採用することで、サイドチャネル攻撃を阻止する機能を読み出し専用メモリにプログラムとして格納することにより、別途サイドチャネル攻撃を阻止する機能を備えた回路を設ける場合より、ＩＣチップを小型化することができる。そのため、ＩＣチップの軽量化、１枚の基板から作製できるＩＣチップの数の増加に伴うコストの削減、サイドチャネル攻撃を阻止する機能を備えた回路の分だけ、トランジスタ数が減少することによる歩留まりの向上に貢献することができる。

【０１２５】

（実施の形態７）

アンテナについて、実施の形態６で説明した形態とは異なる構成を、図１７を用いて説明する。図１７は、無線チップと、第１のアンテナと、第２のアンテナと、第３のアンテナと、電気容量と、から構成される半導体装置の回路図及びレイアウトである。

【０１２６】

図１７（Ａ）は、本実施形態における半導体装置の回路図である。ここで、無線チップ１７０１に搭載された第１のアンテナ（内側アンテナ）１７０２、第２のアンテナ１７０３、第３のアンテナ１７０４、電気容量１７０５である。第２のアンテナ１７０３と、第３のアンテナ１７０４と、電気容量１７０５と、から外側アンテナ１７０６が構成される。

【０１２７】

リーダ／ライタからの通信信号を、第３のアンテナ１７０４で受信すると、第３のアンテナ１７０４では電磁誘導による誘導起電力が生じる。この誘導起電力により、第２のアンテナ１７０３から、誘導電磁界が発生する。この誘導電磁界を、第１のアンテナ１７０２で受信することで、第１のアンテナ１７０２では、電磁誘導による誘導起電力が生じる

ことになる。

【０１２８】

ここで、第３のアンテナ１７０４のインダクタンスを大きくすることで、第１のアンテナ１７０２が受信する誘導電磁界を大きくすることができる。すなわち、第１のアンテナ１７０２のインダクタンスが小さくても、無線チップ１７０１を動作させるのに十分な誘導電磁界を供給することができる。第１のアンテナ１７０２をオンチップアンテナとした場合、無線チップ１７０１は面積が小さいため、インダクタンスはあまり大きくできない。したがって、第１のアンテナ１７０２のみ用いた場合は、無線チップ１７０１の通信距離を伸長することは困難である。ところが、本実施形態に示した構成により、オンチップアンテナの無線チップでも、通信距離を伸長することが可能である。

【０１２９】

図１７（Ｂ）は、本実施形態における半導体装置のアンテナレイアウトの第１の形態である。図１７（Ｂ）は、第３のアンテナ１７０４の外部に第２のアンテナ１７０３を形成した形態である。第１のスルーホール１７０７と、第２のスルーホール１７０８と、は電気的に接続されており、第２のアンテナ１７０３と、第３のアンテナ１７０４と、電気容量１７０５と、から外側アンテナを形成する。電気容量１７０５には、チップコンデンサ、フィルムコンデンサなどを用いることができる。図１７（Ｂ）のようなレイアウトは、幅の狭いアンテナを形成することができるので、幅の狭い形状の半導体装置を提供するときに有効である。

【０１３０】

図１７（Ｃ）は、本実施形態における半導体装置のアンテナレイアウトの第２の例である。図１７（Ｃ）は、第３のアンテナ１７０４の内部に第２のアンテナ１７０３を形成した例である。第１のスルーホール１７０９と、第２のスルーホール１７１０と、は電気的に接続されており、第２のアンテナ１７０３と、第３のアンテナ１７０４と、電気容量１７０５と、から外側アンテナを形成する。電気容量１７０５には、チップコンデンサ、フィルムコンデンサなどを用いることができる。図１７（Ｃ）のようなレイアウトは、幅の狭いアンテナを形成することができるので、幅の狭い形状の半導体装置を提供するときに有効である。

【０１３１】

以上のような形態とすることで、通信距離を伸長した高性能な半導体装置を提供することができる。

【０１３２】

また、本実施の形態は、本明細書中の他の実施の形態の記載とも適宜組み合わせて実施することが可能である。そのため、本発明の半導体装置のサイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、ＩＣチップから漏れる物理的情報の時間変化をより複雑にする。そのため、第３者が傍受した物理的情報から内部情報を取り出すことに時間がかかり、セキュリティを高めることが出来る。また、サイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、サイドチャネル攻撃を阻止する方法が変更になることに伴う仕様の変更により、ＩＣチップのマスク設計の段階から作り直す必要ない。そのため、製造コストの削減及び製造時間の短縮ができる。また、マスク設計の変更によって再度作り直したＩＣチップに不具合が生じているといった懸念もない。

【０１３３】

また従来においては、サイドチャネル攻撃を阻止する機能を有するＩＣチップを製造する際においては、サイドチャネル攻撃を阻止する回路を搭載することもあった。しかしながら、本発明を採用することで、サイドチャネル攻撃を阻止する機能を読み出し専用メモリにプログラムとして格納することにより、別途サイドチャネル攻撃を阻止する機能を備えた回路を設ける場合より、ＩＣチップを小型化することができる。そのため、ＩＣチップの軽量化、１枚の基板から作製できるＩＣチップの数の増加に伴うコストの削減、サイドチャネル攻撃を阻止する機能を備えた回路の分だけ、トランジスタ数が減少することによる歩留まりの向上に貢献することができる。

【０１３４】
（実施の形態８）
乱数生成器は、回路構成やレイアウトが共通であって、かつ同じ製造工程を用いても製造するたびにランダムなデータが生成されるメモリ回路であり、ＩＤチップごとに異なる乱数を生成する乱数生成器として使用することができる。以下、図１８、図１９を用いて乱数生成器の形態について説明する。
【０１３５】
図１８（Ａ）に示すのは乱数生成器の代表的な形態である。同図において、乱数生成器は、デコーダ１８０１、メモリセルアレイ１８０２、及び読み出し回路１８０３からなる。デコーダ１８０１はアドレス信号を受け取って対応するアドレスのワード線を選択する。メモリセルアレイ１８０２は、メモリセル１８０４がマトリクス状に配置されてなり、同じ行のメモリセルは同一のワード線に接続され、同じ列のメモリセルは同一のビット線に接続される。メモリセルはワード線を介して選択され、ビット線を介してデータ読み出しが行われる。読み出し回路１８０３はビット線を選択し、ビット線電位を増幅してデータの読み出しを行う。
【０１３６】
図１８（Ｂ）に示すのは、乱数メモリを構成するメモリセルの例である。メモリセルは１つのＴＦＴ１８０５から構成され、ＴＦＴのソース電極およびドレイン電極の一方はビット線に、残る一方とゲート電極はワード線に接続されている。このメモリセルは、ワード線にＴＦＴ１８０５のしきい値電圧Ｖｔｈよりも高い電圧Ｖｗｏｒｄが印加されると、ビット線に（Ｖｗｏｒｄ－Ｖｔｈ）の電位を充電する。ＴＦＴのしきい値電圧はグレインパタンやプロセスばらつきに起因するばらつきを有するため、そのばらつきをδＶｔｈとすると、図１８（Ｃ）に示すような分布に従ったアナログ電位がビット線に充電されることになる。その結果、本メモリセルはＴＦＴのしきい値電圧のばらつきに基づいたランダムな電位を出力する。
【０１３７】
図１９に示すのは読み出し回路の構成例であり、メモリセル一列分に対応する読み出し回路を示す。読み出し回路２２０１は参照用メモリセル２２０２、差動増幅回路２２０３、ラッチ回路２２０４によって構成される。ワード線が選択されるとメモリセル２２０５によってビット線に電位Ｖｂｉｔが充電される。一方、参照用メモリセル２２０２からは参照電位Ｖｒｅｆが出力され、この２つの電位が差動増幅回路２２０３によって比較増幅され、ラッチ回路２２０４に格納される。
【０１３８】
なお、参照電位Ｖｒｅｆは、メモリセルによって充電されるビット線電位の平均値に近いことが好ましい。そうすることで、各メモリセル列においても、ほぼ１／２の確率でメモリセルのデータが０もしくは１に割り当てられ、一様な乱数が発生する。例えば、参照用メモリセルを構成するＴＦＴのチャネル幅を大きくすることで実現することができる。
【０１３９】
以上のようにして、参照用メモリセル２２０２を構成するＴＦＴのしきい値電圧と選択されたメモリセル２２０５を構成するＴＦＴのしきい値電圧の差に基づいて、１ビットの乱数が決定しラッチ回路２２０４に格納される。より正確には、乱数は差動増幅回路２２０３を構成するＴＦＴのばらつきも含めて決定されるが、いずれにせよ、ＴＦＴの特性ばらつきによって乱数が決まる。こうして、製造工程を変更することなしに用いてもランダムな固定データを格納する乱数生成器を構成することができる。
【０１４０】
なお、上述した乱数生成器は、通常のＴＦＴ作製技術を用いることで作製することが可能であり、他の集積回路を製造するプロセスと同じプロセスで作製することが可能である。従って、本乱数生成器の作製に伴うプロセスコストの上昇はなく、フラッシュメモリを作製する場合と比較してプロセスコストを低く抑えることが可能である。
【０１４１】

なお、乱数メモリ回路に格納される値はランダムであるから、異なるＩＤチップにおいて同一のＩＤが格納される確率は０ではない。しかしながら、例えば、１２８ビット程度の容量を考えても、存在し得る乱数は２１２８個あり、乱数が一致する確率は０に近いため、問題にはならない。

【０１４２】

上記のような乱数生成器を用い、そのデータをＩＤチップに固有のデータ（識別番号など）として使用することで、マスクＲＯＭを製造する場合のフォトマスクの使い捨てを回避し、かつ、プロセスコストの上昇を伴わない、低コストのＩＤチップを作製することが可能となる。

【０１４３】

また、本実施の形態は、本明細書中の他の実施の形態の記載とも適宜組み合わせて実施することが可能である。そのため、本発明の半導体装置のサイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、ＩＣチップから漏れる物理的情報の時間変化をより複雑にする。そのため、第３者が傍受した物理的情報から内部情報を取り出すことに時間がかかり、セキュリティを高めることが出来る。また、サイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、サイドチャネル攻撃を阻止する方法が変更になることに伴う仕様の変更により、ＩＣチップのマスク設計の段階から作り直す必要ない。そのため、製造コストの削減及び製造時間の短縮ができる。また、マスク設計の変更によって再度作り直したＩＣチップに不具合が生じているといった懸念もない。

【０１４４】

また従来においては、サイドチャネル攻撃を阻止する機能を有するＩＣチップを製造する際においては、サイドチャネル攻撃を阻止する回路を搭載することもあった。しかしながら、本発明を採用することで、サイドチャネル攻撃を阻止する機能を読み出し専用メモリにプログラムとして格納することにより、別途サイドチャネル攻撃を阻止する機能を備えた回路を設ける場合より、ＩＣチップを小型化することができる。そのため、ＩＣチップの軽量化、１枚の基板から作製できるＩＣチップの数の増加に伴うコストの削減、サイドチャネル攻撃を阻止する機能を備えた回路の分だけ、トランジスタ数が減少することによる歩留まりの向上に貢献することができる。

【０１４５】

（実施の形態９）

本発明の半導体装置は、ＩＣチップとして利用できる。例えば、紙幣、硬貨、有価証券類、証書類、無記名債券類、及び身分証明書等に設けて使用することができる。これらの具体例に関して図２０を用いて説明する。本発明のＩＣチップは、リーダライタとＩＣチップ間の信号の送受信におけるサイドチャネル攻撃を阻止する機能を有している。このため、図２０に示すような様々な物品に添付されたＩＣチップの情報が漏洩することを抑止できる。また、ＩＣチップは実施の形態３で示したように薄膜トランジスタを用いることで薄型化できるため、物品のデザイン性の低下を防ぐことができる。

【０１４６】

図２０に本発明の読み取りにおける一態様を示す。図２０に示すＩＣチップ２１０１は、非接触でリーダライタ２１０３とデータの送受信を行う非接触型である。電波圏内２１０２に存在するＩＣチップ２１０１は、リーダライタ２１０３と無線通信を行うことができる。なお、ＩＣチップ２１０１とリーダライタ２１０３との距離、すなわち電波圏内２１０２の距離は、無線通信に用いる周波数に起因する。また周波数は、ＩＣチップ２１０１に用いられるアンテナ長、又はアンテナ形状に起因する。

【０１４７】

図２０において、紙幣２１０５、パスポート２１０６、小切手２１０７が電波圏内に存在し、リーダライタ２１０３はコンピュータ２１０４と電気的に接続され、物品の情報の読み取り等をおこなう。なお、図２０において、電波圏内２１０２に存在する本発明のサイドチャネル攻撃を阻止する機能を有するＩＣチップ２１０１を有する紙幣２１０５、パスポート２１０６、小切手２１０７は、リーダライタ２１０３により、瞬時にそれぞれの

情報を読み出される。

【０１４８】

紙幣２１０５、パスポート２１０６、小切手２１０７等にＩＣチップ２１０１を設けることにより、リーダライタとＩＣチップ間の通信情報が漏洩することを抑止できる。ＩＣチップ２１０１の設け方としては、物品の表面に貼ったり、物品に埋め込んだりして設ける。例えば、紙幣ならば紙に埋め込んだり、有機樹脂からなるカードなら当該有機樹脂に埋め込んだりするとよい。このようにして、紙幣２１０５、パスポート２１０６、小切手２１０７等にＩＣチップを設けることにより、金融機関や公的機関のシステムなどの情報漏えいを抑止することができる。

【０１４９】

以上のように、本発明の半導体装置は物品であればどのようなものにでも設けて使用してもよく、ほかにも免許証、保険証、定期券、キャッシュカード、クレジットカード、電子キー、電子マネー等に使用することができる。本実施の形態は、上述した他の実施の形態とも適宜組み合わせて行うことができる。

【０１５０】

また、本実施の形態は、本明細書中の他の実施の形態の記載とも適宜組み合わせて実施することが可能である。そのため、本発明の半導体装置のサイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、ＩＣチップから漏れる物理的情報の時間変化をより複雑にする。そのため、第３者が傍受した物理的情報から内部情報を取り出すことに時間がかかり、セキュリティを高めることが出来る。また、サイドチャネル攻撃を阻止する機能を有するＩＣチップにおいて、サイドチャネル攻撃を阻止する方法が変更になることに伴う仕様の変更により、ＩＣチップのマスク設計の段階から作り直す必要ない。そのため、製造コストの削減及び製造時間の短縮ができる。また、マスク設計の変更によって再度作り直したＩＣチップに不具合が生じているといった懸念もない。

【０１５１】

また従来においては、サイドチャネル攻撃を阻止する機能を有するＩＣチップを製造する際においては、サイドチャネル攻撃を阻止する回路を搭載することもあった。しかしながら、本発明を採用することで、サイドチャネル攻撃を阻止する機能を読み出し専用メモリにプログラムとして格納することにより、別途サイドチャネル攻撃を阻止する機能を備えた回路を設ける場合より、ＩＣチップを小型化することができる。そのため、ＩＣチップの軽量化、１枚の基板から作製できるＩＣチップの数の増加に伴うコストの削減、サイドチャネル攻撃を阻止する機能を備えた回路の分だけ、トランジスタ数が減少することによる歩留まりの向上に貢献することができる。

【図面の簡単な説明】

【０１５２】

【図１】実施の形態１に係る半導体装置を示したブロック図。
【図２】実施の形態１に係る半導体装置におけるメモリのブロック図。
【図３】実施の形態１に係る信号のブロック図。
【図４】実施の形態１に係るサイドチャネル攻撃阻止機構を示したフローチャート図。
【図５】実施の形態１に係るサイドチャネル攻撃阻止機構を示したフローチャート図。
【図６】実施の形態１に係るサイドチャネル攻撃阻止機構を示したフローチャート図。
【図７】実施の形態１に係るサイドチャネル攻撃阻止機構を示したフローチャート図。
【図８】実施の形態１に係るサイドチャネル攻撃阻止機構を示したフローチャート図。
【図９】実施の形態１に係るサイドチャネル攻撃阻止機構を示したフローチャート図。
【図１０】実施の形態１に係る補助演算装置を示したブロック図。
【図１１】実施の形態２に係るサイドチャネル攻撃阻止機構を示したフローチャート図。
【図１２】実施の形態２に係る半導体装置を示したブロック図。
【図１３】実施の形態３に係る半導体装置の断面図。
【図１４】実施の形態４に係る半導体装置の断面図。
【図１５】実施の形態５に係る半導体装置を示したブロック図。

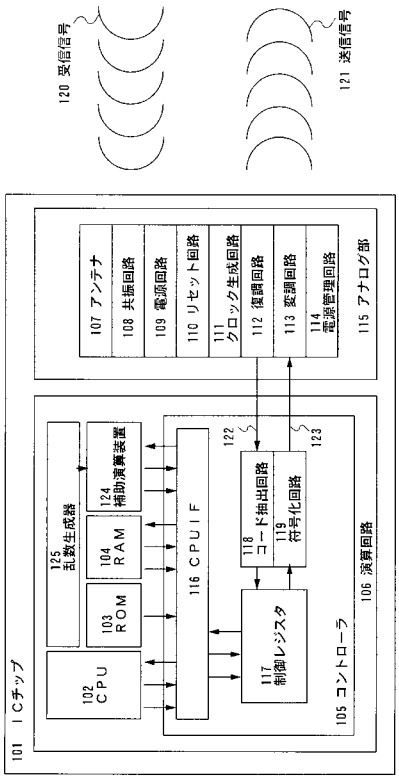
【図１６】実施の形態６に係るアンテナ形状について示した図。
【図１７】実施の形態７に係るアンテナ形状について示した図。
【図１８】実施の形態８に係る半導体装置を示した回路図およびＴＦＴの閾値電圧のばらつきを示す図。
【図１９】実施の形態８に係る乱数生成器の形態について説明する図。
【図２０】実施の形態９に係る半導体装置の使用例について示した図。
【符号の説明】
【０１５３】
１０１　ＩＣチップ
１０２　ＣＰＵ
１０３　ＲＯＭ
１０４　ＲＡＭ
１０５　コントローラ
１０６　演算回路
１０７　アンテナ
１０８　共振回路
１０９　電源回路
１１０　リセット回路
１１１　クロック生成回路
１１２　復調回路
１１３　変調回路
１１４　電源管理回路
１１５　アナログ部
１１６　ＣＰＵＩＦ
１１７　制御レジスタ
１１８　コード抽出回路
１１９　符号化回路
１２０　受信信号
１２１　送信信号
１２２　受信データ
１２３　送信データ
１２４　補助演算装置
１２５　乱数生成器
２０１　サイドチャネル攻撃阻止プログラム
２０２　秘密鍵
２０１Ａ　コマンド判断ルーチン
２０１Ｂ　ラウンド判断ルーチン
２０３　送信データレジスタ
２０４　受信データレジスタ
３０１　ＳＯＦ
３０２　フラグ
３０３　コマンド
３０４　データ
３０５　ＣＲＣ
３０６　ＥＯＦ
４０１　初期リセット
４０２　開始
４０３　制御レジスタ判断
４０４　プログラム読み込み
４０９　ルーチン実行

５０１　ルーチン開始
５０３　コマンド取得
５０４　終了
６０１　データ取得
６１３　第二の逆変換
６１４　逆転置
６１５　第二の逆変換
６１６　逆転置
６１７　第二の逆変換
６２１　逆変換前データ送信
６２２　開始
６２３　乱数値読み込み
６２４　スイッチマトリクス切り替え
６２５　鍵読み込み
６２６　データ入力
６２８　逆変換
６２９　データ出力
６３０　終了
６３１　逆変換後データ受信
１００１　逆変換パターン選択
１００２　逆変換開始
１００３　逆変換
１００４　逆変換終了
１１０１　入力データ
１１０２　鍵
１１０３　出力データ
１１０４　スイッチパラメータ
１３００　絶縁基板
１３０１　剥離層
１３０２　下地層
１３０４　半導体層
１３０５　ゲート絶縁層
１３０６　ゲート電極層
１３０７　サイドウォール
１３１０　高濃度不純物領域
１３１１　低濃度不純物領域
１３１２　高濃度不純物領域
１３１４　絶縁層
１３１５　絶縁層
１３１６　絶縁層
１３１８　配線
１３１９　保護膜
１３２５　エッチング剤
１３２７　フィルム
１３２８　フィルム
１３２９　接着層
１３３０　Ｎチャネル型ＴＦＴ
１３３１　Ｐチャネル型ＴＦＴ
１６０１　ＩＣチップ
１６０２　アンテナ

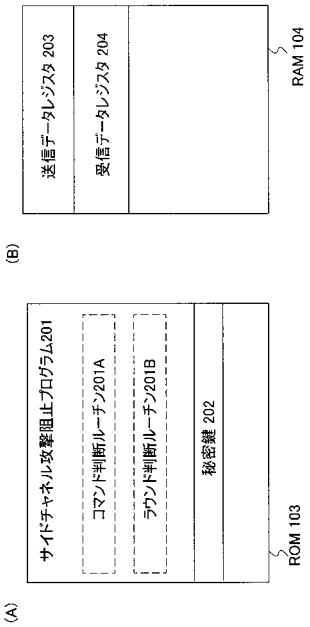
１６０３　アンテナ
１６０４　アンテナ
１６０５　アンテナ
１７０１　無線チップ
１７０２　第１のアンテナ
１７０３　第２のアンテナ
１７０４　第３のアンテナ
１７０５　電気容量
１７０６　外側アンテナ
１７０７　第１のスルーホール
１７０８　第２のスルーホール
１７０９　第１のスルーホール
１７１０　第２のスルーホール
１８０１　デコーダ
１８０２　メモリセルアレイ
１８０３　読み出し回路
１８０４　メモリセル
１８０５　ＴＦＴ
１９０１　シリコン基板
１９０２　ｎ型ウェル
１９０３　ｐ型ウェル
１９０４　フィールド酸化膜
１９０５　ゲート電極
１９０５ａ　シリサイド層
１９０５ｂ　ポリシリコン層
１９０６　ゲート電極
１９０６ａ　シリサイド層
１９０６ｂ　ポリシリコン層
１９０７　エクステンション領域
１９０８　エクステンション領域
１９０９　サイドウォール
１９１０　サイドウォール
１９１１　ゲート絶縁膜
１９１２　ゲート絶縁膜
１９１３　ソース領域
１９１４　ドレイン領域
１９１５　ソース領域
１９１６　ドレイン領域
１９１７　第１の層間絶縁膜
１９１８　第２の層間絶縁膜
１９１９　ソース電極
１９２０　ドレイン電極
１９２１　ソース電極
１９２２　ドレイン電極
１９２３　パッシベーション膜
１９２５　ｐチャネル型トランジスタ
１９２６　ｎチャネル型トランジスタ
１９２７　フィルム
１９２８　フィルム
２１０１　ＩＣチップ

２１０２　電波圏内
２１０３　リーダライタ
２１０４　コンピュータ
２１０５　紙幣
２１０６　パスポート
２１０７　小切手
２２０１　読み出し回路
２２０２　参照用メモリセル
２２０３　差動増幅回路
２２０４　ラッチ回路
２２０５　メモリセル
３００１　秘密鍵

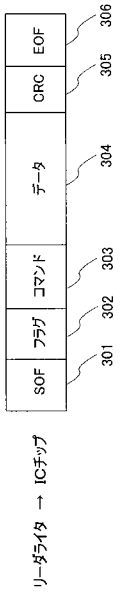
【図１】



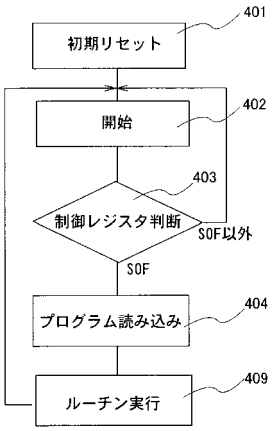
【図２】



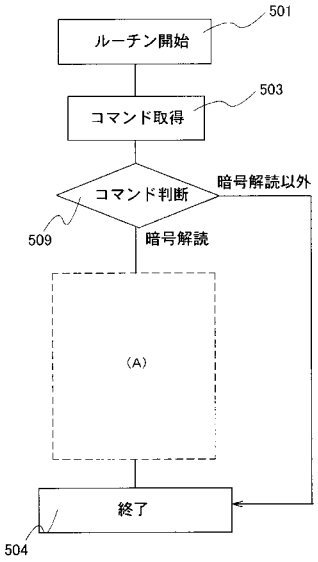
【図３】


EOF
CRC
データ
コマンド
フラグ
SOF
306
305
304
303
302
301
リーダライタ → ICチップ

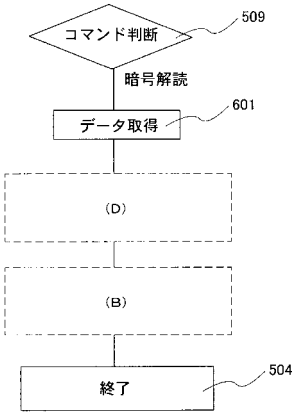
【図４】


初期リセット
401
開始
402
制御レジスタ判断
403
SOF以外
SOF
プログラム読み込み
404
ルーチン実行
409

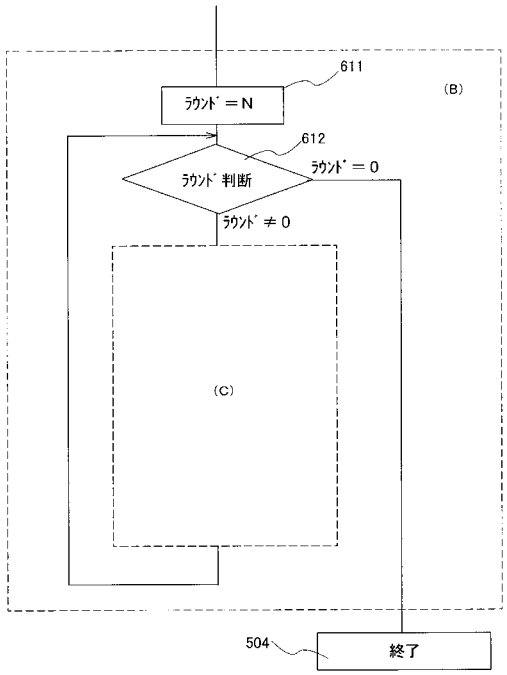
【図５】


ルーチン開始
501
コマンド取得
503
コマンド判断
509
暗号解読以外
暗号解読
(A)
終了
504

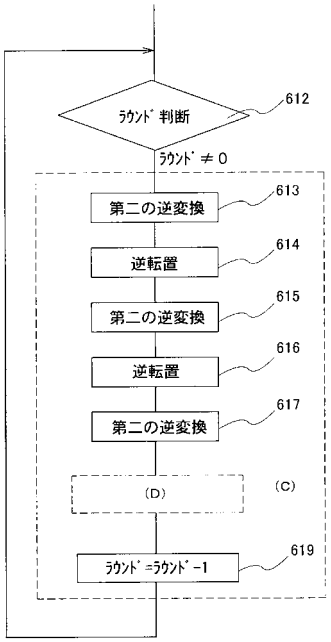
【図６】


コマンド判断
509
暗号解読
データ取得
601
(D)
(B)
終了
504

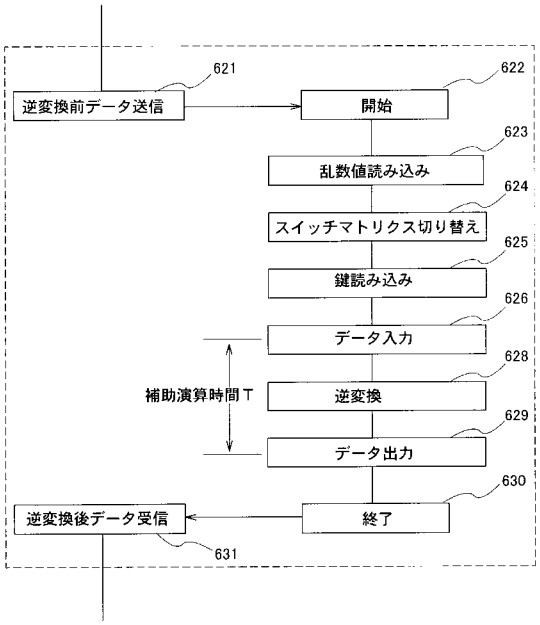
【図７】


611
ﾗｳﾝﾄﾞ＝N
(B)
612
ﾗｳﾝﾄﾞ判断
ﾗｳﾝﾄﾞ＝0
ﾗｳﾝﾄﾞ≠0
(C)
504
終了

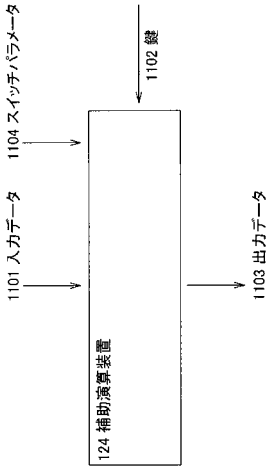
【図８】


612
ﾗｳﾝﾄﾞ判断
ﾗｳﾝﾄﾞ≠0
613
第二の逆変換
614
逆転置
615
第二の逆変換
616
逆転置
617
第二の逆変換
(D)
(C)
619
ﾗｳﾝﾄﾞ=ﾗｳﾝﾄﾞ-1

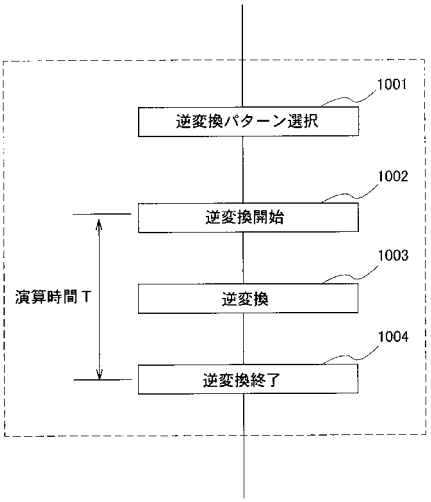
【図９】


621
逆変換前データ送信
622
開始
623
乱数値読み込み
624
スイッチマトリクス切り替え
625
鍵読み込み
626
データ入力
補助演算時間T
628
逆変換
629
データ出力
630
終了
逆変換後データ受信
631

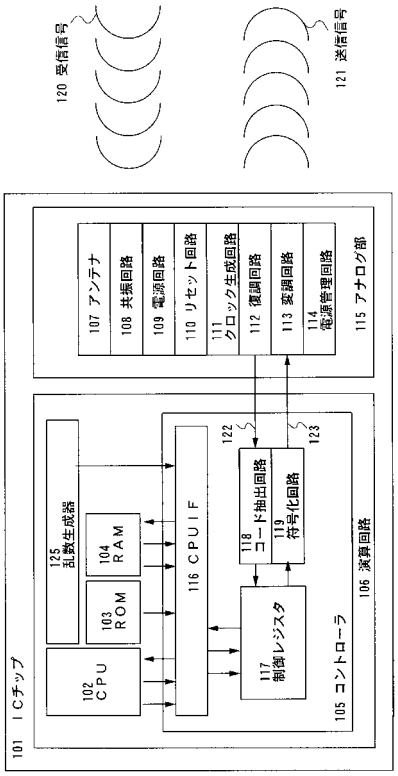
【図１０】


1102 鍵
1104 スイッチパラメータ
1101 入力データ
1103 出力データ
124 補助演算装置

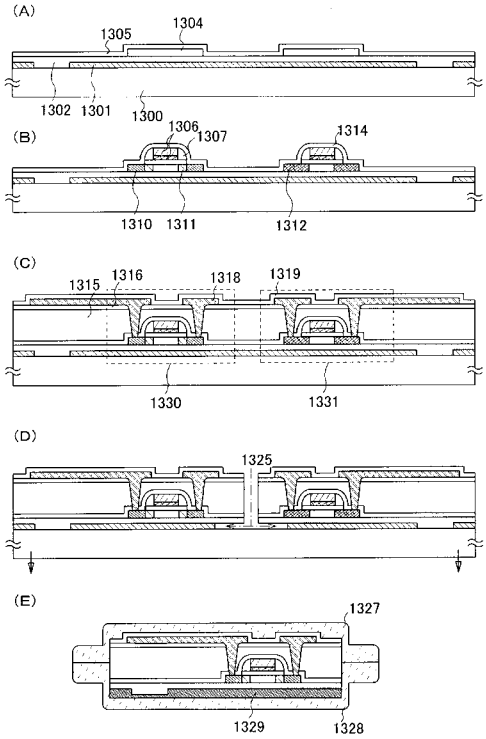
【図１１】



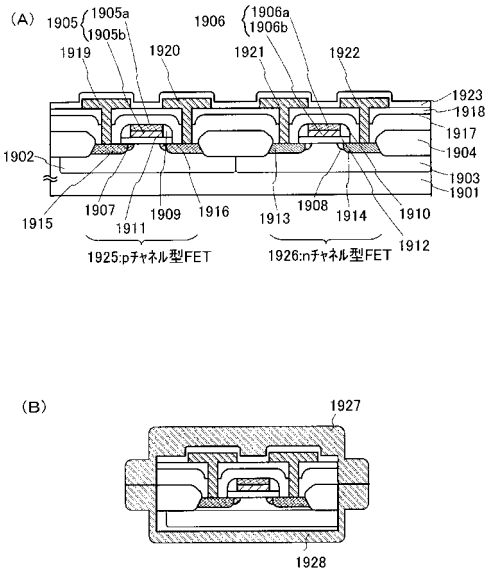
【図１２】



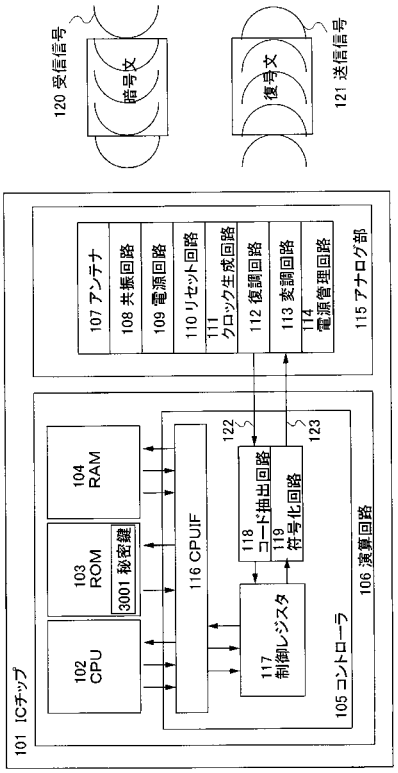
【図１３】



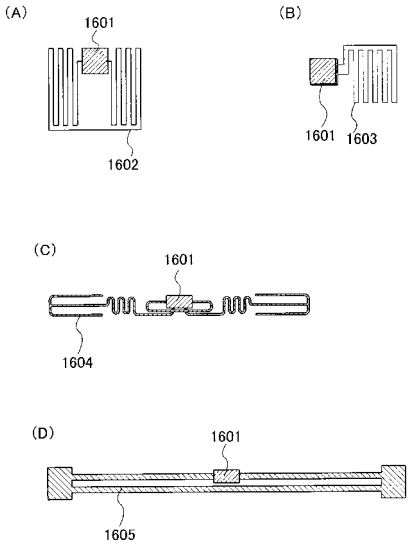
【図１４】



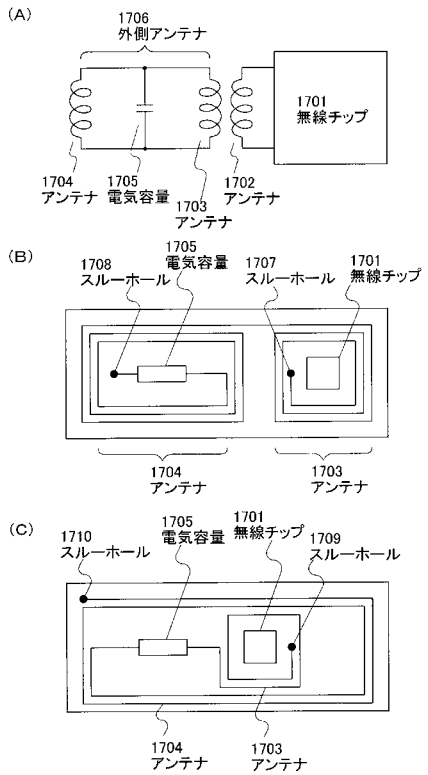
【図１５】



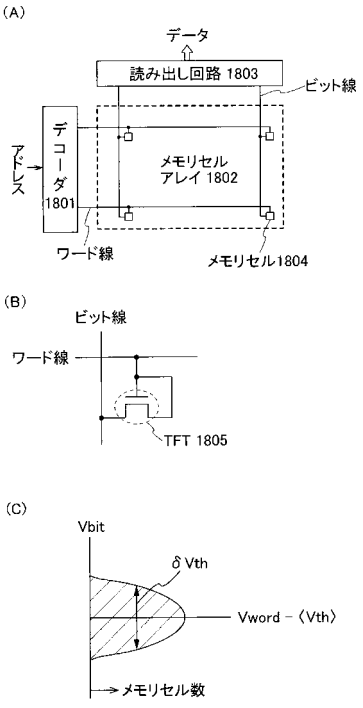
【図１６】



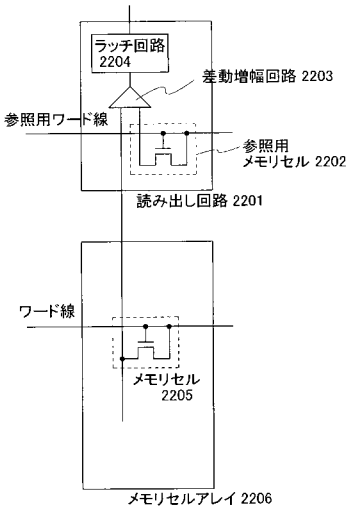
【図１７】



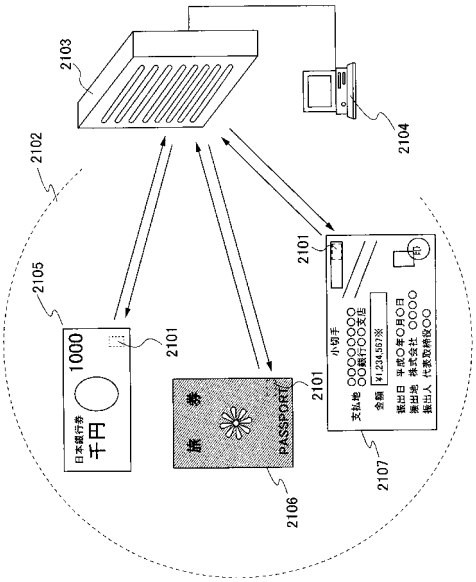
【図１８】



【図１９】


ラッチ回路
2204
差動増幅回路 2203
参照用ワード線
参照用
メモリセル 2202
読み出し回路 2201
ワード線
メモリセル
2205
メモリセルアレイ 2206

【図２０】


2103
2104
2102
2101
2105
2101
2101
2107
2106
1000
千円
PASSPORT