(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2022-178067
(P2022-178067A)
(43)公開日　令和4年12月2日(2022.12.2)

| (51)Int.Cl. | | | FI | | | テーマコード（参考） |
|---|---|---|---|---|---|---|
| G06F | 7/58 | (2006.01) | G06F | 7/58 | 680 | 5F038 |
| G09C | 1/00 | (2006.01) | G09C | 1/00 | 650B | |
| H01L | 21/822 | (2006.01) | H01L | 27/04 | T | |

審査請求 未請求　請求項の数 14　OL　（全 15 頁）

(21)出願番号　特願2021-84585(P2021-84585)
(22)出願日　令和3年5月19日(2021.5.19)

(71)出願人　302062931
ルネサスエレクトロニクス株式会社
東京都江東区豊洲三丁目２番２４号
(74)代理人　110002066
弁理士法人筒井国際特許事務所
(72)発明者　福島　和彦
東京都江東区豊洲三丁目２番２４号　ルネサスエレクトロニクス株式会社内
(72)発明者　朝見　和生
東京都江東区豊洲三丁目２番２４号　ルネサスエレクトロニクス株式会社内

Ｆターム(参考) 5F038 DF04 DF05 DF16 DT10 DT11 DT15 DT18 DT19 EZ01 EZ20

(54)【発明の名称】半導体装置および乱数データの検証方法

(57)【要約】
【課題】周期性のあるデータを乱数と誤判定することを防ぎ、乱数データのランダム性を高精度に検証することが可能な半導体装置および乱数データの検証方法を提供する。
【解決手段】半導体装置は、シリアルデータである乱数データＤＴを生成する乱数発生器と、乱数データＤＴのランダム性を検証するヘルステスト回路ＨＴＣと、を有する。ヘルステスト回路ＨＴＣは、乱数データＤＴを、ｎ（ｎは２以上の整数）ビット毎に区切ることでｎビットデータＤ［ｔ］のデータ列として取り扱い、当該ｎビットデータＤ［ｔ］に基づいてランダム性を検証する。
【選択図】図３

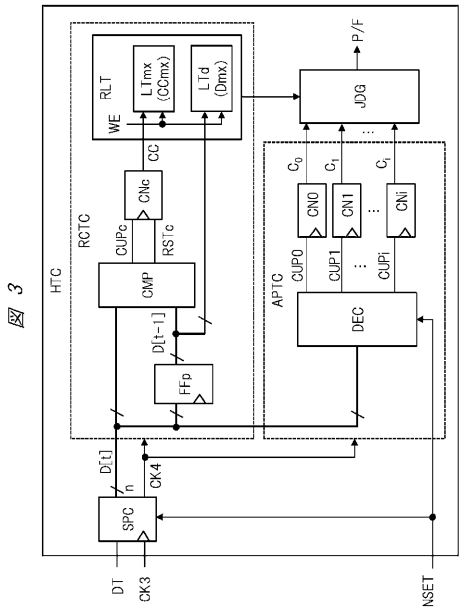



図３

【特許請求の範囲】
【請求項１】
シリアルデータである乱数データを生成する乱数発生器と、
前記乱数データのランダム性を検証するヘルステスト回路と、
を有する半導体装置であって、
前記ヘルステスト回路は、前記乱数データを、ｎ（ｎは２以上の整数）ビット毎に区切ることでｎビットデータのデータ列として取り扱い、前記ｎビットデータに基づいて前記ランダム性を検証する、
半導体装置。
【請求項２】
請求項１記載の半導体装置において、
前記ヘルステスト回路は、ビット長設定信号に応じて前記ｎビットの値を可変設定する、半導体装置。
【請求項３】
請求項１記載の半導体装置において、
前記ヘルステスト回路は、同一値の前記ｎビットデータが連続して発生した場合の連続数を検出する第１のテスト回路を有する、
半導体装置。
【請求項４】
請求項１記載の半導体装置において、
前記ヘルステスト回路は、前記ｎビットデータが表す$2^n$個の値の中の少なくとも一つの値の発生回数を検出する第２のテスト回路を有する、
半導体装置。
【請求項５】
請求項４記載の半導体装置において、
前記第２のテスト回路は、前記$2^n$個の値のそれぞれの発生回数を全て検出する、
半導体装置。
【請求項６】
請求項５記載の半導体装置において、
前記ヘルステスト回路は、前記第２のテスト回路で検出された前記$2^n$個の値のそれぞれの発生回数の合計値を算出する、
半導体装置。
【請求項７】
請求項１記載の半導体装置において、
前記乱数発生器は、特性設定信号に応じて前記ランダム性の特性を切り替えられるように構成され、
前記ヘルステスト回路は、前記ｎビットデータに基づく前記ランダム性の検証結果が予め定めた基準を満たさない場合には、前記特性設定信号を用いて前記乱数発生器における前記ランダム性の特性を切り替える、
半導体装置。
【請求項８】
請求項７記載の半導体装置において、
前記乱数発生器は、ＳＲラッチを構成する２個の論理ゲートを備え、前記２個の論理ゲート間の双方向の伝播遅延時間が前記特性設定信号に応じて可変設定されるように構成される、
半導体装置。
【請求項９】
シリアルデータである乱数データを生成する乱数発生器を対象に、前記乱数データのランダム性を検証する乱数データの検証方法であって、
前記乱数データを、ｎ（ｎは２以上の整数）ビット毎に区切ることでｎビットデータの

データ列として取り扱い、前記ｎビットデータに基づいて前記ランダム性を検証する、
乱数データの検証方法。
【請求項１０】
請求項９記載の乱数データの検証方法において、
前記ｎビットの値は、可変設定可能となっている、
乱数データの検証方法。
【請求項１１】
請求項９記載の乱数データの検証方法において、
同一値の前記ｎビットデータが連続して発生した場合の連続数を検出する、
乱数データの検証方法。
【請求項１２】
請求項９記載の乱数データの検証方法において、
前記ｎビットデータが表す$2^n$個の値の中の少なくとも一つの値の発生回数を検出する
、
乱数データの検証方法。
【請求項１３】
請求項１２記載の乱数データの検証方法において、
前記$2^n$個の値のそれぞれの発生回数を全て検出する、
乱数データの検証方法。
【請求項１４】
請求項１３記載の乱数データの検証方法において、
検出された前記$2^n$個の値のそれぞれの発生回数の合計値を算出する、
乱数データの検証方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、半導体装置および乱数データの検証方法に関する。
【背景技術】
【０００２】
特許文献１には、半導体デバイスの熱雑音による電流変化を利用してビット列を発生する第１の乱数発生部と、その後段に設けられ、帰還路付きのシフトレジスタを用いて乱数を発生する第２の乱数発生部とを有する乱数発生装置が示される。第１の乱数発生部は、電流変化に基づいて発振周波数が変化する発振器を用いて第１のクロック信号を発生し、第１のクロック信号を、それよりも低周波数の第２のクロック信号でラッチすることでビット列を発生する。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２００５－４４０９０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
乱数は、暗号技術に必要な要素であり、例えば、鍵の生成や、認証等で広く用いられている。データの秘匿性や完全性、認証の信頼性等を高めるためには、乱数データのランダム性を高めることが求められる。このような乱数発生器として、例えば、特許文献１に示されるように、物理的なランダム要因に基づき真性乱数を発生する方式が知られている。一方、このような乱数発生器を用いた場合であっても、外部からの攻撃によってランダム性が低下する場合がある。そこで、乱数発生器には、発生した乱数データのランダム性が低下したことを検知するヘルステストと呼ばれる機能を搭載することが推奨されている。
【０００５】

例えば、“ＮＩＳＴ(National Institute of Standards and Technology) ＳＰ８００－９０Ｂ”では、ヘルステストとして、“Repetition Count Test”（明細書では、ＲＣＴと略す）、“Adaptive Proportion Test”（明細書では、ＡＰＴと略す）について言及されている。ＲＣＴは、同じ値が規定回数以上続けて出力されないことを確認するテストである。ＡＰＴは、既定のビット長で“１”又は“０”の個数をカウントし、カウント値が閾値を超えないことを確認するテストである。

【０００６】

ここで、例えば、１０１０…といったデータは、周期性のあるデータであるため、本来は、乱数と判定されるべきデータではない。しかし、通常の判定方式を用いた場合、ＲＣＴではデータ連続数が１であるため規定回数以下であると判定され、ＡＰＴでは１の発生確率が５０％であるため発生確率が規定内に収まっていると判定される。このように、ＲＣＴおよびＡＰＴにおける通常の判定方式を用いた場合、本来、ランダム性が低い乱数データであってもパス、すなわちランダム性有りと判定され、ランダム性を高精度に検証できない恐れがあった。

【０００７】

後述する実施の形態は、このようなことに鑑みてなされたものであり、その他の課題と新規な特徴は、本明細書の記述及び添付図面から明らかになるであろう。

【課題を解決するための手段】

【０００８】

一実施の形態による半導体装置は、シリアルデータである乱数データを生成する乱数発生器と、乱数データのランダム性を検証するヘルステスト回路と、を有する。ヘルステスト回路は、乱数データを、ｎ（ｎは２以上の整数）ビット毎に区切ることでｎビットデータのデータ列として取り扱い、当該ｎビットデータに基づいてランダム性を検証する。

【発明の効果】

【０００９】

前記一実施の形態によれば、周期性のあるデータを乱数と誤判定することを防ぐことが可能になり、乱数データのランダム性を高精度に検証することが可能になる。

【図面の簡単な説明】

【００１０】

【図１】本発明の実施の形態１による半導体装置の構成例を示す概略図である。

【図２Ａ】図１における乱数発生器の構成例を示す回路ブロック図である。

【図２Ｂ】図２Ａにおけるリングオシレータの構成例を示す回路図である。

【図３】図１におけるヘルステスト回路の構成例を示す回路ブロック図である。

【図４】図１におけるヘルステスト回路の“Repetition Count Test（ＲＣＴ）”時の主要部の処理内容の一例を示すフロー図である。

【図５】図１におけるヘルステスト回路の“Adaptive Proportion Test（ＡＰＴ）”時の主要部の処理内容の一例を示すフロー図である。

【図６】本発明の実施の形態２による半導体装置において、図１における乱数発生器の構成例を示す回路図である。

【図７Ａ】図６の乱数発生器の動作原理を説明する図である。

【図７Ｂ】図６の乱数発生器の動作原理を説明する図である。

【図８】本発明の実施の形態２による半導体装置において、図１におけるヘルステスト回路の構成例を示す回路ブロック図である。

【発明を実施するための形態】

【００１１】

以下の実施の形態においては便宜上その必要があるときは、複数のセクションまたは実施の形態に分割して説明するが、特に明示した場合を除き、それらは互いに無関係なものではなく、一方は他方の一部または全部の変形例、詳細、補足説明等の関係にある。また、以下の実施の形態において、要素の数等（個数、数値、量、範囲等を含む）に言及する場合、特に明示した場合および原理的に明らかに特定の数に限定される場合等を除き、そ

の特定の数に限定されるものではなく、特定の数以上でも以下でも良い。

【００１２】

さらに、以下の実施の形態において、その構成要素（要素ステップ等も含む）は、特に明示した場合および原理的に明らかに必須であると考えられる場合等を除き、必ずしも必須のものではないことは言うまでもない。同様に、以下の実施の形態において、構成要素等の形状、位置関係等に言及するときは、特に明示した場合および原理的に明らかにそうでないと考えられる場合等を除き、実質的にその形状等に近似または類似するもの等を含むものとする。このことは、上記数値および範囲についても同様である。

【００１３】

また、実施の形態の各機能ブロックを構成する回路素子は、特に制限されないが、公知のＣＭＯＳ（相補型ＭＯＳトランジスタ）等の集積回路技術によって、単結晶シリコンのような半導体基板上に形成される。

【００１４】

以下、本発明の実施の形態を図面に基づいて詳細に説明する。なお、実施の形態を説明するための全図において、同一の部材には原則として同一の符号を付し、その繰り返しの説明は省略する。

【００１５】

（実施の形態１）

《半導体装置の概略》

図１は、本発明の実施の形態１による半導体装置の構成例を示す概略図である。図１に示す半導体装置ＤＥＶは、代表的には、マイクロコントローラや、ＳｏＣ（System on a chip）等である。当該半導体装置ＤＥＶは、プロセッサＰＲＣと、ＲＡＭ（Random Access Memory）および不揮発性メモリＮＶＭといったメモリと、各種周辺回路ＰＥＲＩとに加えて、乱数発生器ＲＮＧと、ヘルステスト回路ＨＴＣとを有する。これらの各部は、互いにバスＢＳで接続される。

【００１６】

プロセッサＰＲＣは、メモリに保存されたプログラムを実行することで、所定の機能を実現する。各種周辺回路ＰＥＲＩには、例えば、アナログディジタル変換器、ディジタルアナログ変換器、外部通信インタフェース等を代表に、様々なものが含まれる。乱数発生器ＲＮＧは、シリアルデータである乱数データを発生する。ヘルステスト回路ＨＴＣは、乱数発生器ＲＮＧからの乱数データのランダム性を検証する。具体的には、ヘルステスト回路ＨＴＣは、例えば、乱数データのランダム性が低下したことを検出する。

【００１７】

なお、実施の形態１の半導体装置は、マイクロコントローラ等の他に、例えば、ＦＰＧＡ（Field Programmable Gate Array）やＡＳＩＣ（Application Specific Integrated Circuit）等であってもよい。また、ヘルステスト回路ＨＴＣは、詳細は後述するが、ハードウェア回路に限らず、プロセッサＰＲＣによるプログラム処理で実現されてもよい。

【００１８】

《乱数発生器の詳細》

図２Ａは、図１における乱数発生器の構成例を示す回路ブロック図である。図２Ｂは、図２Ａにおけるリングオシレータの構成例を示す回路図である。図２Ａに示す乱数発生器ＲＮＧは、リングオシレータＲＯ１，ＲＯ２と、分周器ＫＤＶと、フリップフロップＦＦｓとを有する。リングオシレータＲＯ１，ＲＯ２は、それぞれ、イネーブル信号ＥＮがアサートレベルの期間で発振動作を行うことでクロック信号ＣＫ１，ＣＫ２を生成する。

【００１９】

分周器ＫＤＶは、リングオシレータＲＯ２からのクロック信号ＣＫ２の周期をＫ（Ｋ＞１）倍に分周することで、クロック信号ＣＫ２よりも低周波数のクロック信号ＣＫ３を生成する。フリップフロップＦＦｓは、リングオシレータＲＯ１からのクロック信号ＣＫ１を、分周器ＫＤＶからのクロック信号ＣＫ３のエッジでサンプリングすることで、シリアルデータである乱数データＤＴを生成する。

【００２０】
図２Ｂのリングオシレータ ＲＯは、図２Ａのリングオシレータ ＲＯ１，ＲＯ２のそれぞれに対応する。当該リングオシレータ ＲＯは、ナンドゲート ＮＤ０と、その後段に順次接続される複数段（ｊ段）のバッファ ＢＦ１～ＢＦｊとを備える。ナンドゲート ＮＤ０には、イネーブル信号 ＥＮと、最終段のバッファ ＢＦｊから帰還したクロック信号 ＣＫとが入力される。
【００２１】
バッファ ＢＦ１～ＢＦｊのそれぞれは、例えば、偶数段の ＣＭＯＳ（Complementary Metal Oxide Semiconductor）インバータ回路等で構成される。ナンドゲート ＮＤ０は、イネーブル信号 ＥＮがアサートレベル（“１”レベル）の期間でインバータ回路として機能する。これにより、リングオシレータ ＲＯは、奇数段のインバータ回路によって発振動作を行い、最終段のバッファ ＢＦｊからクロック信号 ＣＫを出力する。
【００２２】
図２Ａに示した乱数発生器 ＲＮＧは、主に、リングオシレータ ＲＯ１に含まれる熱雑音からくるジッタ成分を利用して、乱数データ ＤＴを発生している。このような回路構成の乱数発生器 ＲＮＧは、ＥＲＯ(Elementary Ring Oscillator）型と呼ばれる。なお、乱数発生器 ＲＮＧは、図２Ａのような構成に限らず、乱数データ、望ましく、真性乱数からなる乱数データを発生できるものであればよい。
【００２３】
《前提となる問題点》
乱数データ ＤＴのランダム性を低下させるための乱数発生器への攻撃方法が知られている。例えば、図２Ｂのリングオシレータ ＲＯに外部から周期的な電磁波を与えることで、クロック信号 ＣＫのジッタ成分を抑制する方法が知られている。図２Ａの乱数発生器 ＲＮＧにおいて、特に、リングオシレータ ＲＯ１のジッタ成分が抑えられると、乱数データ ＤＴのランダム性が低下する可能性が高くなる。その結果、例えば、秘匿や認証といった暗号機能の安全性が低下する恐れがある。
【００２４】
そこで、図１のヘルステスト回路 ＨＴＣには、乱数データ ＤＴのランダム性を高精度に検証し、ランダム性が低下したことを確実に検出することが求められる。通常の方式を用いたヘルステスト回路は、ＲＣＴおよび ＡＰＴの際に、乱数データを１ビット単位で取り扱うことでランダム性を検証する。具体例として、乱数データがケース Ａ“１０１０１０１０…”の場合、ケース Ｂ“００１１１０００１１１０…”の場合、ケース Ｃ“０１１００１１０…”の場合を想定する。
【００２５】
この場合、ＲＣＴでのテスト指標となる同一データの最大連続数は、ケース Ａでは１回となり、ケース Ｂでは３回となり、ケース Ｃでは２回となる。その結果、ケース Ａ、ケース Ｂおよびケース Ｃは、共に、最大連続数が小さいため、ＲＣＴでパスと判定され得る。また、ＡＰＴでのテスト指標となる同一データの最大発生確率は、ケース Ａ、ケース Ｂおよびケース Ｃ共に５０％となる。その結果、ケース Ａ、ケース Ｂおよびケース Ｃは、共に、最大発生確率が５０％前後の範囲に含まれるため、ＡＰＴにおいてもパスと判定され得る。
【００２６】
しかし、ケース Ａ、ケース Ｂおよびケース Ｃの乱数データは、周期的なデータであり、本来はランダム性が低いデータである。このように、通常の方式では、ＲＣＴおよび ＡＰＴの際に、本来、ランダム性が低いデータであっても、パスと判定される恐れがあった。すなわち、通常の方式では、乱数データ ＤＴのランダム性を高精度に検証できず、ランダム性が低下したことを確実に検出できない恐れがあった。
【００２７】
《ヘルステスト回路の詳細》
図３は、図１におけるヘルステスト回路の構成例を示す回路ブロック図である。図３に

示すヘルステスト回路ＨＴＣは、概略的には、乱数発生器ＲＮＧからの乱数データＤＴを、ｎ（ｎは２以上の整数）ビット毎に区切ることでｎビットデータのデータ列として取り扱い、当該ｎビットデータに基づいてランダム性を検証する。詳細には、ヘルステスト回路ＨＴＣは、シリアルパラレル変換器ＳＰＣと、ＲＣＴ回路ＲＣＴＣと、ＡＰＴ回路ＡＰＴＣと、結果判定回路ＪＤＧとを有する。

【００２８】

シリアルパラレル変換器ＳＰＣは、シリアルデータである乱数データＤＴをクロック信号ＣＫ３に同期して取り込み、当該乱数データＤＴをｎ（ｎは２以上の整数）ビット毎に区切ることで、パラレルデータであるｎビットデータＤ［ｔ］を出力する。また、シリアルパラレル変換器ＳＰＣは、当該ｎビットデータＤ［ｔ］の出力タイミングに同期するクロック信号ＣＫ４を生成する。なお、単位ビット長“ｎ”の値は、ビット長設定信号ＮＳＥＴによって任意に設定可能となっている。

【００２９】

ＲＣＴ回路ＲＣＴＣは、概略的には、乱数発生器ＲＮＧからの乱数データＤＴにおいて、同一値のｎビットデータＤ［ｔ］が連続して発生した場合の連続数を検出する。詳細には、ＲＣＴ回路ＲＣＴＣは、フリップフロップＦＦｐと、比較器ＣＭＰと、カウンタＣＮｃと、結果保持回路ＲＬＴとを有する。ＲＣＴ回路ＲＣＴＣは、シリアルパラレル変換器ＳＰＣからのクロック信号ＣＫ４に基づいて動作する。

【００３０】

フリップフロップＦＦｐは、シリアルパラレル変換器ＳＰＣからのｎビットデータＤ［ｔ］をクロック信号ＣＫ４に基づいて１クロック周期分遅延させることで、前クロック周期のｎビットデータＤ［ｔ－１］を生成する。比較器ＣＭＰは、当該前クロック周期のｎビットデータＤ［ｔ－１］と、現クロック周期のｎビットデータＤ［ｔ］とを比較する。そして、比較器ＣＭＰは、当該２個のｎビットデータＤ［ｔ］，Ｄ［ｔ－１］が同一値の場合には、カウントアップ信号ＣＵＰｃを生成、言い換えればアサートし、同一値でない場合には、リセット信号ＲＳＴｃを生成、言い換えればアサートする。

【００３１】

カウンタＣＮｃは、比較器ＣＭＰからのカウントアップ信号ＣＵＰｃに応じて、カウント値ＣＣを更新、例えば、カウントアップし、比較器ＣＭＰからのリセット信号ＲＳＴｃに応じて、カウント値ＣＣをリセットする。その結果、カウント値ＣＣは、同一値のｎビットデータＤ［ｔ］が連続して発生した場合の連続数を表す。

【００３２】

結果保持回路ＲＬＴは、最大連続数保持回路ＬＴｍｘと、最大連続データ保持回路ＬＴｄとを有する。最大連続数保持回路ＬＴｍｘは、カウンタＣＮｃからのカウント値ＣＣが最大となった場合の最大カウント値ＣＣｍｘを保持する。最大連続データ保持回路ＬＴｄは、この最大カウント値ＣＣｍｘに対応するｎビットデータＤ［ｔ－１］を、最大連続時データＤｍｘとして保持する。

【００３３】

具体的には、結果保持回路ＲＬＴは、例えば、カウンタＣＮｃからのカウント値ＣＣが最大連続数保持回路ＬＴｍｘに保持している最大カウント値ＣＣｍｘよりも大きくなった場合に、ライトイネーブル信号ＷＥを用いて、当該カウント値ＣＣで最大カウント値ＣＣｍｘを更新する。さらに、結果保持回路ＲＬＴは、ライトイネーブル信号ＷＥを用いて、最大カウント値ＣＣｍｘを更新した際のｎビットデータＤ［ｔ－１］で最大連続時データＤｍｘを更新する。

【００３４】

ＡＰＴ回路ＡＰＴＣは、概略的には、乱数発生器ＲＮＧからの乱数データＤＴにおいて、ｎビットデータＤ［ｔ］が表す$2^n$個の値のそれぞれの発生回数を検出する。詳細には、ＡＰＴ回路ＡＰＴＣは、デコーダＤＥＣと、$2^n$個のカウンタＣＮ０～ＣＮｉ（ｉ＝$2^n$－１）とを有する。デコーダＤＥＣは、ｎビットデータＤ［ｔ］が$2^n$個の値のいずれであるかを判別し、判別結果に応じて、$2^n$個のカウントアップ信号ＣＵＰ０～ＣＵＰｉ

を生成、言い換えればアサートする。カウンタＣＮ０～ＣＮｉは、それぞれ、カウントアップ信号ＣＵＰ０～ＣＵＰｉに応じて、各値の発生回数を表すカウント値$C_0$～$C_i$を更新、例えば、カウントアップする。

【００３５】

結果判定回路ＪＤＧは、ＲＣＴ回路ＲＣＴＣ内の結果保持回路ＲＬＴで保持される最大カウント値ＣＣｍｘおよび最大連続時データＤｍｘに基づいて、ＲＣＴのパスＰ／フェイルＦを判定する。さらに、結果判定回路ＪＤＧは、ＡＰＴ回路ＡＰＴＣ内のカウンタＣＮ０～ＣＮｉからのカウント値$C_0$～$C_i$に基づいて、ＡＰＴのパスＰ／フェイルＦを判定する。

【００３６】

《乱数発生器のテスト方法》

図４は、図１におけるヘルステスト回路の“Repetition Count Test（ＲＣＴ）”時の主要部の処理内容の一例を示すフロー図である。図５は、図１におけるヘルステスト回路の“Adaptive Proportion Test（ＡＰＴ）”時の主要部の処理内容の一例を示すフロー図である。図４および図５のフローは、例えば、図１のプロセッサＰＲＣによって実行されてもよい。すなわち、図３のヘルステスト回路ＨＴＣは、プロセッサＰＲＣによるプログラム処理で実現されてもよい。

【００３７】

図４において、ヘルステスト回路ＨＴＣは、まず、乱数発生器ＲＮＧからの乱数データＤＴをｎビット毎に区切る（ステップＳ１０１）。続いて、ヘルステスト回路ＨＴＣは、現周期のｎビットデータＤ［ｔ］と前周期のｎビットデータＤ［ｔ－１］とを参照する（ステップＳ１０２）。次いで、ヘルステスト回路ＨＴＣは、ｎビットデータＤ［ｔ］とｎビットデータＤ［ｔ－１］とが同一か否かを判定する（ステップＳ１０３）。

【００３８】

ステップＳ１０３でＤ［ｔ］＝Ｄ［ｔ－１］の場合、ヘルステスト回路ＨＴＣは、同一データの連続数、すなわち、図３のカウント値ＣＣを更新する（ステップＳ１０４）。その後、ヘルステスト回路ＨＴＣは、同一データの最大連続数、すなわち、図３の最大カウント値ＣＣｍｘを取得する（ステップＳ１０５）。そして、ヘルステスト回路ＨＴＣは、ステップＳ１０４でのカウント値ＣＣがステップＳ１０５での最大カウント値ＣＣｍｘよりも大きいか否かを判定する（ステップＳ１０６）。

【００３９】

ステップＳ１０６でＣＣ＞ＣＣｍｘの場合、ヘルステスト回路ＨＴＣは、最大カウント値ＣＣｍｘをカウント値ＣＣで更新し（ステップＳ１０７）、対応するｎビットデータＤ［ｔ－１］で最大連続時データＤｍｘを更新する（ステップＳ１０８）。一方、ステップＳ１０６でＣＣ≦ＣＣｍｘの場合、ヘルステスト回路ＨＴＣは、処理を終了する。また、ステップＳ１０３でＤ［ｔ］　Ｄ［ｔ－１］の場合、ヘルステスト回路ＨＴＣは、同一データの連続数、すなわち、図３のカウント値ＣＣをリセットし、処理を終了する（ステップＳ１０９）。なお、ヘルステスト回路ＨＴＣは、乱数データＤＴが生成されている限り、図４のフローを繰り返し実行する。

【００４０】

図５において、ヘルステスト回路ＨＴＣは、まず、乱数発生器ＲＮＧからの乱数データＤＴをｎビット毎に区切る（ステップＳ２０１）。続いて、ヘルステスト回路ＨＴＣは、現周期のｎビットデータＤ［ｔ］を参照する（ステップＳ２０２）。次いで、ヘルステスト回路ＨＴＣは、ｎビットデータＤ［ｔ］の値が$D_0$，$D_1$，…，$D_{i-1}$，$D_i$（$i=2^n-1$）のいずれであるかを判定する（ステップＳ２０３［０］，Ｓ２０３［１］，…，Ｓ２０３［ｉ－１］）。

【００４１】

そして、ヘルステスト回路ＨＴＣは、ｎビットデータＤ［ｔ］の値が$D_0$，$D_1$，…，$D_{i-1}$，$D_i$のいずれであるかに応じて、対応する発生回数、すなわち図３のカウント値$C_0$，$C_1$，…，$C_{i-1}$，$C_i$を更新し、処理を終了する（ステップＳ２０４［０］

，Ｓ２０４［１］，…，Ｓ２０４［ｉ－１］，Ｓ２０４［ｉ］）。なお、ヘルステスト回路ＨＴＣは、乱数データＤＴが生成されている限り、図５のフローを繰り返し実行する。

【００４２】

以上のように、乱数データＤＴを、前述した通常の方式とは異なりｎビット単位で取り扱うことで、ランダム性を高精度で検証することができ、ランダム性の低下をより確実に検出することが可能になる。具体例として、単位ビット長“ｎ”を４に設定した場合、ヘルステスト回路ＨＴＣは、前述したケースＡ、ケースＢおよびケースＣの乱数データを、それぞれ、“０ｘＡＡ…”、“０ｘ３８Ｅ３８Ｅ…”および“０ｘ６６…”のデータ列として取り扱う。

【００４３】

この場合、ＲＣＴでのテスト指標となる同一データの最大連続数は、ケースＢでは１回となるが、ケースＡおよびケースＣでは多数回となる。その結果、ケースＡおよびケースＣに関しては、共に、最大連続数が大きいため、ＲＣＴでフェイルと判定することができる。また、ＡＰＴでのテスト指標となる同一データの最大発生確率は、ケースＡおよびケースＣでは１００％となり、ケースＢでは約３３％となる。一方、最大発生確率の基準値は約６％（＝１／$2^4$）である。その結果、ケースＡ、ケースＢおよびケースＣは、共に、最大発生確率が基準値から大きく解離しているため、ＡＰＴでフェイルと判定することができる。

【００４４】

このように、乱数データＤＴをｎビット単位で取り扱うことで、１ビット単位で取り扱う通常の方式と異なり、特に、２ビット周期、４ビット周期、６ビット周期といった複数ビットで周期性のある乱数データに対して、ランダム性を高精度に検証することが可能になる。この際に、単位ビット長“ｎ”の値は、図３に示したビット長設定信号ＮＳＥＴによって任意に設定することが可能である。

【００４５】

《ＡＰＴの判定方式の詳細》

図３の結果判定回路ＪＤＧは、ＡＰＴの判定に際し、例えば、次の２通りの方式を用いることができる。ここでは、単位ビット長“ｎ”が４である場合を例とする。一つ目の方式は、ｎビットデータＤ［ｔ］が表す１６（＝$2^4$）個の値０ｘ０～０ｘＦの中の少なくとも一つの値の発生回数に基づいて判定する方式である。この場合、結果判定回路ＪＤＧは、予め１６個の値の中のどの値をカウント対象とするかを定めておく。

【００４６】

そして、結果判定回路ＪＤＧは、例えば、２０４８ビット等の乱数データＤＴに対して、カウント対象とした値のカウント値が予め定めた基準値を超えなければパスＰと判定し、カウント値が基準値を超えていればフェイルＦと判定する。これにより、乱数発生器ＲＮＧに致命的な故障が生じていないことを保証することができる。なお、この一つ目の方式の場合には、必ずしも、図３に示したようなｉ＋１個のカウンタＣＮ０～ＣＮｉを設ける必要はなく、カウント対象とした値に対応する少なくとも１個のカウンタを設ければよい。

【００４７】

二つ目の方式は、ミニマムエントロピーを考慮した判定方式であり、ｎビットデータＤ［ｔ］が表す１６個の値のそれぞれの発生回数を全て検出する方式である。この場合、結果判定回路ＪＤＧは、例えば、２０４８ビット等の乱数データＤＴに対して、１６個の値０ｘ０～０ｘＦの中のいずれの値のカウント値も基準値を超えなければパスＰと判定し、基準値を超えているカウント値が一つでもあれば、フェイルＦと判定する。

【００４８】

これにより、乱数発生器ＲＮＧに致命的な故障が生じていないことに加えて、乱数発生器ＲＮＧによって生成される乱数データＤＴの品質、すなわちランダム性が一定の水準を満たしていることを保証することができる。その結果、例えば、ランダム性を低下させる攻撃に対して耐性を得ることが可能になる。なお、結果判定回路ＪＤＧは、例えば、１６

個のカウント値の合計値を算出し、テストで使用した乱数データＤＴのビット数と照合してもよい。これにより、乱数データＤＴの数を改ざんするような攻撃に対しても耐性を得ることが可能になる。

【００４９】

《ヘルステスト回路の各種変形例》

図３の変形例として、ＲＣＴ回路ＲＣＴＣとＡＰＴ回路ＡＰＴＣとで、単位ビット長“ｎ”の値を個別に設定可能な構成であってもよい。この場合、シリアルパラレル変換器ＳＰＣを、ＲＣＴ回路ＲＣＴＣ向けとＡＰＴ回路ＡＰＴＣ向けに２個設ければよい。また、図３のヘルステスト回路ＨＴＣを複数個設け、各ヘルステスト回路ＨＴＣに互いに異なる単位ビット長“ｎ”の値を設定してもよい。この際には、複数のヘルステスト回路ＨＴＣの一つは、ｎ＝１に設定されてもよい。すなわち、比較例のヘルステスト回路に図３のヘルステスト回路ＨＴＣを追加したような構成であってもよい。

【００５０】

このような各種変形例を用いると、適用されるシステム毎に、ヘルステストの検出性能、ひいては暗号の安全性・秘匿性と、回路規模あるいはプログラムサイズといったコストとのバランスを考慮して、最適な構成を定めることが可能になる。

【００５１】

《実施の形態１の主要な効果》

以上、実施の形態１の方式を用いることで、代表的には、周期性のあるデータを乱数と誤判定することを防ぐことが可能になり、乱数データのランダム性を高精度に検証することが可能になる。すなわち、ランダム性が低下したことを確実に検出することが可能になる。その結果、暗号の安全性・秘匿性を高めることができる。さらに、ランダム性を低下させる攻撃に対して耐性を得ることができる。

【００５２】

（実施の形態２）

《乱数発生器の詳細》

図６は、本発明の実施の形態２による半導体装置において、図１における乱数発生器の構成例を示す回路図である。図７Ａおよび図７Ｂは、図６の乱数発生器の動作原理を説明する図である。図７Ａには、ＴＥＲＯ（Transition Effect Ring Oscillator）型と呼ばれる乱数発生器の回路構成例が示される。図７Ｂには、図７Ａの動作例が示される。図６に示す乱数発生器ＲＮＧａは、詳細は後述するが、特性設定信号となるイネーブル信号ＥＮ１～ＥＮ３に応じてランダム性の特性を切り替えられるように構成される。

【００５３】

まず、図７Ａにおいて、ナンドゲートＮＤｓ，ＮＤｒからなる２個の論理ゲートは、ＳＲラッチを構成する。各ナンドゲートＮＤｓ，ＮＤｒにおいて、２入力の一方には、イネーブル信号ＥＮが共通に入力される。また、ナンドゲートＮＤｓにおける２入力の他方には、ナンドゲートＮＤｒの出力信号がインバータ回路ＩＶｓ１，ＩＶｓ２を介して帰還される。同様に、ナンドゲートＮＤｒにおける２入力の他方にも、ナンドゲートＮＤｓの出力信号がインバータ回路ＩＶｒ１，ＩＶｒ２を介して帰還される。

【００５４】

このようなＳＲラッチでは、イネーブル信号ＥＮが“０”の状態は禁止状態であり、イネーブル信号ＥＮが“１”の状態はラッチ状態である。図７Ｂには、この禁止状態の期間Ｔ１ａ，Ｔ１ｂの動作波形と、ラッチ状態の期間Ｔ２の動作波形とが示される。禁止状態では、ナンドゲートＮＤｓ，ＮＤｒの出力信号は、共に“１”に固定され、ナンドゲートＮＤｓ，ＮＤｒにおける２入力の他方も“１”に固定される。その結果、図７Ｂの期間Ｔ１ａ，Ｔ１ｂに示されるように、例えば、インバータ回路ＩＶｒ２の出力信号ＯＴは、“１”に固定される。

【００５５】

ここで、ＳＲラッチでは、禁止状態から、セット入力／リセット入力を経ることなくラッチ状態へ遷移させると、発振が生じる。仮に回路特性にばらつきが無く、ナンドゲート

ＮＤｒからナンドゲートＮＤｓへの伝播遅延時間とその逆方向の伝播遅延時間とが同一であれば、この発振は無限に続く。一方、例えば、２個の伝播遅延時間にばらつきが生じると、結果的にセット入力またはリセット入力が生じ、ＳＲラッチは、セットまたはリセットのラッチ状態に収束する。このため、図７Ｂの期間Ｔ２に示されるように、出力信号ＯＴは、ある程度の周期の発振を経たのち、“０”または“１”に収束する。

【００５６】

その後、イネーブル信号ＥＮを“１”から“０”に立下げると、ＳＲラッチは、セットまたはリセットのラッチ状態から再び禁止状態へ遷移する。図７Ａのフリップフロップ ＦＦｓは、図７Ｂの期間Ｔ２および期間Ｔ１ｂに示されるように、このイネーブル信号ＥＮの立下りエッジで、セットまたはリセットのラッチ状態に伴う“０”または“１”の出力信号ＯＴをラッチすることで、乱数データＤＴを出力する。すなわち、イネーブル信号ＥＮをクロック信号とすることで、その立下りエッジ毎に、“０”または“１”がランダムにラッチされ、これによって乱数データＤＴを生成することが可能になる。

【００５７】

図６に示す乱数発生器ＲＮＧａは、４個のナンドゲートＮＤ１～ＮＤ３，ＮＤｒと、アンドゲートＡＤ０と、２個のインバータ回路ＩＶｒ１，ＩＶｒ２と、フリップフロップＦＦｓとを備える。この内、ナンドゲートＮＤｒ、２個のインバータ回路ＩＶｒ１，ＩＶｒ２およびフリップフロップＦＦｓに関しては、図７Ａの場合と同様である。

【００５８】

アンドゲートＡＤ０は、３個のイネーブル信号ＥＮ１～ＥＮ３を入力としてアンド演算を行うことでクロック信号ＣＫ３を生成する。ナンドゲートＮＤｒにおける２入力の一方と、フリップフロップＦＦｓには、図７Ａに示したイネーブル信号ＥＮの代わりに、このクロック信号ＣＫ３が入力される。また、ナンドゲートＮＤｒにおける２入力の他方には、ナンドゲートＮＤ３の出力信号ＯＴが入力される。

【００５９】

ナンドゲートＮＤ１～ＮＤ３における２入力の一方には、それぞれ、イネーブル信号ＥＮ１～ＥＮ３が入力される。また、ナンドゲートＮＤ１～ＮＤ３は、ナンドゲートＮＤ１を初段、ナンドゲートＮＤ３を最終段として、縦続接続される。これに伴い、ナンドゲートＮＤ１～ＮＤ３における２入力の他方には、前段からの出力信号が入力される。この際に、初段のナンドゲートＮＤ１における２入力の他方には、インバータ回路ＩＶｒ２の出力信号が入力される。

【００６０】

これにより、特性設定信号となるイネーブル信号ＥＮ１～ＥＮ３の設定状態に応じて、ナンドゲートＮＤ１～ＮＤ３のいずれか一つは、図７Ａに示したナンドゲートＮＤｓとして機能し、残りはインバータ回路として機能する。具体的には、ナンドゲートＮＤｓに対応するものは、イネーブル信号ＥＮ１，ＥＮ２が共に“１”固定の場合（ケース（１）と呼ぶ）にはナンドゲートＮＤ３である。また、ナンドゲートＮＤｓに対応するものは、イネーブル信号ＥＮ２，ＥＮ３が共に“１”固定の場合（ケース（２）と呼ぶ）にはナンドゲートＮＤ１であり、イネーブル信号ＥＮ１，ＥＮ３が共に“１”固定の場合（ケース（３）と呼ぶ）にはナンドゲートＮＤ２である。

【００６１】

一方、ケース（１）では、残りのナンドゲートＮＤ１，ＮＤ２は、インバータ回路として機能する。その結果、ナンドゲートＮＤｒの出力からナンドゲートＮＤ３の入力までに４段のインバータ回路を介することになり、ナンドゲートＮＤ３の出力からナンドゲートＮＤｒの入力までに０段のインバータ回路を介することになる。

【００６２】

同様にして、ケース（２）では、ナンドゲートＮＤｒからナンドゲートＮＤ１までと、その逆方向とで共に２段のインバータ回路を介することになる。この場合、図７Ａの構成例と等価になる。さらに、ケース（３）では、ナンドゲートＮＤｒからナンドゲートＮＤ２までに３段のインバータ回路を介することになり、ナンドゲートＮＤ２からナンドゲー

トＮＤｒまでに１段のインバータ回路を介することになる。

【００６３】

ここで、ケース（２）を例として、“１”固定を除く残り一つのイネーブル信号ＥＮ１をクロック信号に定めると、アンドゲートＡＤ０は、当該クロック信号をクロック信号ＣＫ３として出力する。その結果、図７Ｂの場合と同じ動作が行われる。ケース（１）およびケース（３）に関しても同様であり、“１”固定を除く残り一つのイネーブル信号がクロック信号に定められる。

【００６４】

この際に、図６の構成例は、図７Ａの構成例と異なり、前述したように、イネーブル信号ＥＮ１～ＥＮ３の設定状態に応じて、ＳＲラッチの構成する２個のナンドゲートＮＤｓ，ＮＤｒ間の双方向の伝播遅延時間が可変設定される構成となっている。双方向の伝播遅延時間を可変設定することで、乱数発生器ＲＮＧａにおけるランダム性の特性を切り替えることが可能になる。

【００６５】

《ヘルステスト回路の詳細》

図８は、本発明の実施の形態２による半導体装置において、図１におけるヘルステスト回路の構成例を示す回路ブロック図である。図８に示すヘルステスト回路ＨＴＣａは、図３の構成例と比較して、結果判定回路ＪＤＧａの構成および動作が異なっている。図８の結果判定回路ＪＤＧａは、図３の場合と同様に、結果保持回路ＲＬＴで保持される最大カウント値ＣＣｍｘおよび最大連続時データＤｍｘや、カウンタＣＮ０～ＣＮｉからのカウント値$C_0$～$C_i$に基づいてランダム性を検証し、パスＰ／フェイルＦを判定する。

【００６６】

さらに、当該結果判定回路ＪＤＧａは、図３の場合と異なり、ランダム性の検証結果が予め定めた基準を満たさない場合には、特性設定信号となるイネーブル信号ＥＮ１～ＥＮ３を用いて乱数発生器ＲＮＧａにおけるランダム性の特性を切り替える。具体的には、結果判定回路ＪＤＧａは、判定結果（言い換えれば検証結果）がフェイルＦとなる度に、図６で述べた各イネーブル信号の設定状態、すなわちケース（１）～ケース（３）を順に切り替える。これにより、図６に示した乱数発生器ＲＮＧａにおけるランダム性の特性が変わり、判定結果がパスＰとなるように切り替えられる可能性が高くなる。

【００６７】

《実施の形態２の主要な効果》

以上、実施の形態２の方式を用いることで、実施の形態１で述べた各種効果と同様の効果が得られる。さらに、実施の形態２の方式を用いると、ランダム性が低下したことを検出できることに加えて、この検出に応じてランダム性の特性を変えるように制御することが可能になる。その結果、例えば、乱数発生器の可用性を高めること等が可能になる。

【００６８】

以上、本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能である。例えば、前述した実施の形態は、本発明を分かり易く説明するために詳細に説明したものであり、必ずしも説明した全ての構成を備えるものに限定されるものではない。また、ある実施の形態の構成の一部を他の実施の形態の構成に置き換えることが可能であり、また、ある実施の形態の構成に他の実施の形態の構成を加えることも可能である。また、各実施の形態の構成の一部について、他の構成の追加・削除・置換をすることが可能である。

【符号の説明】

【００６９】

ＡＰＴＣ　ＡＰＴ回路（第２のテスト回路）

$C_0$～$C_i$　カウント値

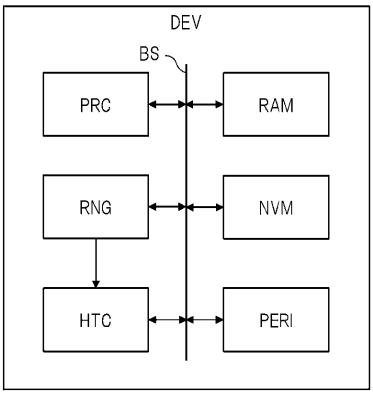
ＣＣｍｘ　最大カウント値

Ｄ［ｔ］，Ｄ［ｔ－１］　ｎビットデータ

ＤＥＶ　半導体装置
ＤＴ　乱数データ
Ｄｍｘ　最大連続時データ
ＥＮ　イネーブル信号
ＥＮ１～ＥＮ３　イネーブル信号（特性設定信号）
ＨＴＣ　ヘルステスト回路
ＪＤＧ　結果判定回路
ＮＤ　ナンドゲート（論理ゲート）
ＮＳＥＴ　ビット長設定信号
ＲＣＴＣ　ＲＣＴ回路（第１のテスト回路）
ＲＮＧ　乱数発生器

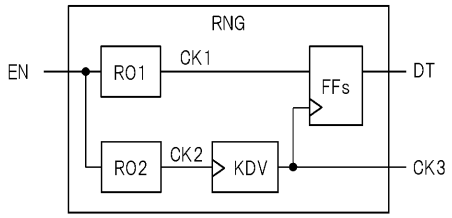
【図１】

*図 1*



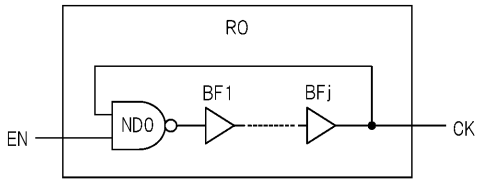

【図２Ａ】

*図 2A*



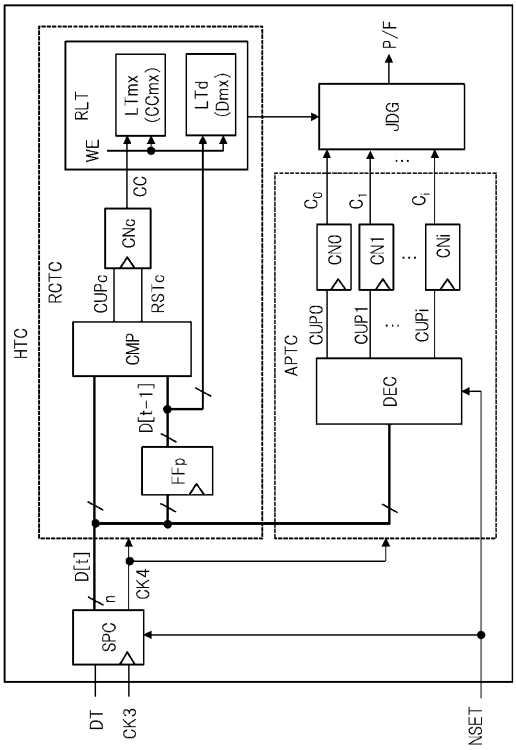

【図２Ｂ】

*図 2B*



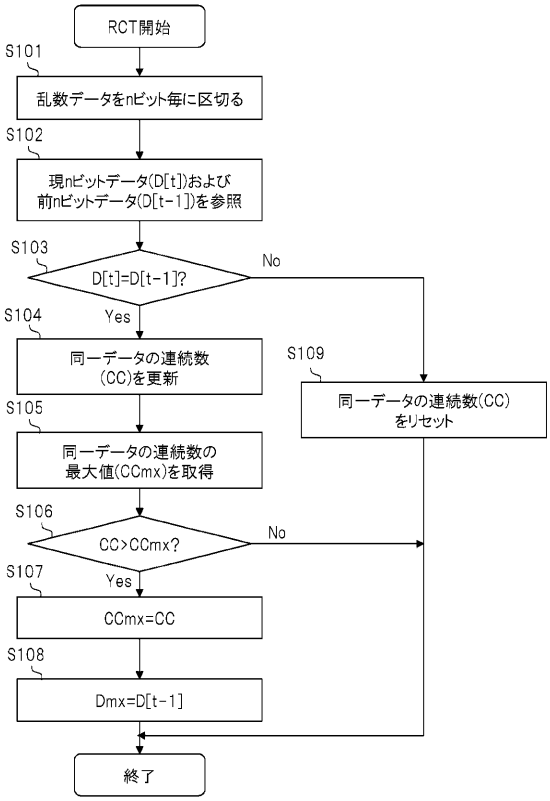
【図３】

図 3



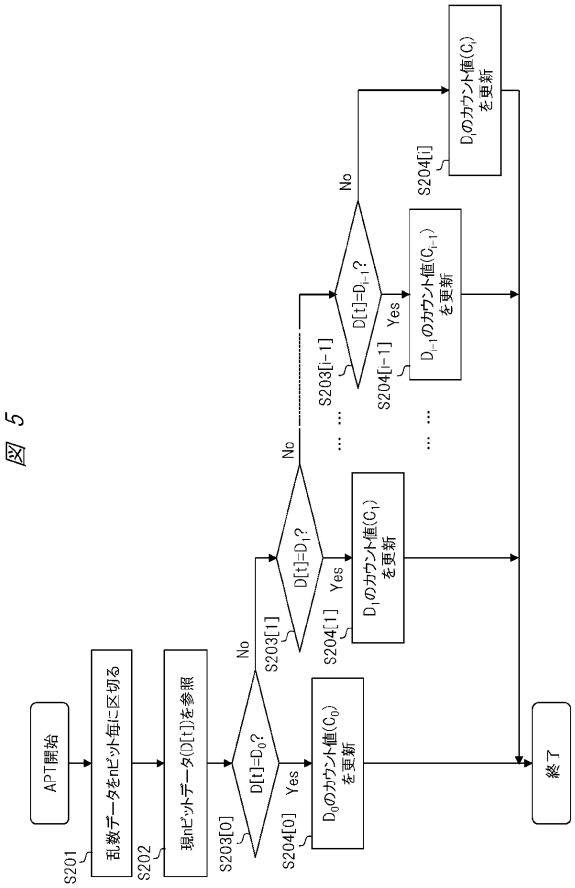

【図４】

図 4



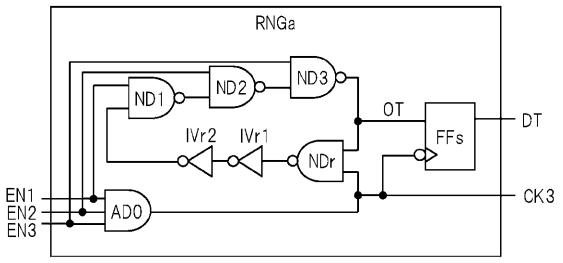

【図５】

図 5



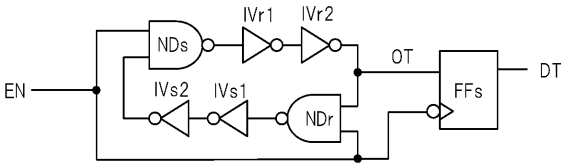

【図６】

図 6



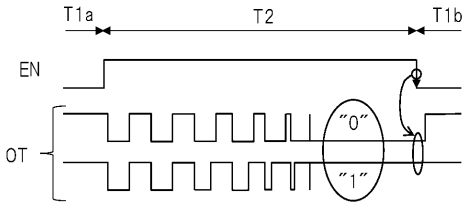
【図７Ａ】

図 7A




【図７Ｂ】

図 7B




【図８】

図 8