(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6472766号
(P6472766)
(45)発行日　平成31年2月20日(2019.2.20)　(24)登録日　平成31年2月1日(2019.2.1)

(51)Int.Cl.　F I
G06F 7/58 (2006.01)　G06F 7/58 680
G09C 1/00 (2006.01)　G09C 1/00 650B

請求項の数 5　(全 21 頁)

(21)出願番号　特願2016-52320(P2016-52320)
(22)出願日　平成28年3月16日(2016.3.16)
(65)公開番号　特開2017-167799(P2017-167799A)
(43)公開日　平成29年9月21日(2017.9.21)
審査請求日　平成30年2月22日(2018.2.22)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　110001737
特許業務法人スズエ国際特許事務所
(72)発明者　高谷　聡
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　安田　心一
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　棚本　哲史
東京都港区芝浦一丁目１番１号　株式会社東芝内

最終頁に続く

(54)【発明の名称】乱数生成回路

(57)【特許請求の範囲】
【請求項１】
第1の発振信号が入力され、所定のデューティー比を有する第2の発振信号を出力する第1の回路と、
第2の発振信号と前記第2の発振信号の周波数よりも低い周波数を有するクロックとに基づき複数の値をラッチする第2の回路と、
前記複数の値に基づき制御信号を出力する第3の回路と、
前記制御信号に基づき、前記所定のデューティー比が５０％よりも小さくなっているときには前記所定のデューティー比を大きくし、前記所定のデューティー比が５０％よりも大きくなっているときには前記所定のデューティー比を小さくするように前記第1の回路を制御する第4の回路と、
を具備する乱数生成回路。
【請求項２】
前記第1の発振信号を生成する第5の回路をさらに備える、請求項1に記載の乱数生成回路。
【請求項３】
前記第2の回路は、直列接続される複数のラッチ部を備え、前記複数の値は、前記複数のラッチ部にラッチされる、請求項1又は2に記載の乱数生成回路。
【請求項４】
前記第1の回路は、複数の入力端子を備えるNANDゲート回路と、入力端子を備えるイン

バータ回路と、複数の入力端子を備えるNORゲート回路と、を備え、
前記第4の回路は、前記NANDゲート回路、インバータ回路、及び、NORゲート回路のうちの1つの選択を制御する、
請求項1乃至3のいずれか1項に記載の乱数生成回路。
【請求項５】
前記第1の回路は、入力端子をそれぞれ備えるPチャネルFET及びNチャネルFETを含み、
前記第4の回路は、前記PチャネルFETとNチャネルFETのうち少なくともいずれかの駆動力の変更を制御する、
請求項1乃至3のいずれか1項に記載の乱数生成回路。
【発明の詳細な説明】
【技術分野】
【０００１】
実施形態は、乱数生成回路に関する。
【背景技術】
【０００２】
情報通信技術の発展と、クレジットカードや交通系ICカードなどの普及とに伴い、これらのカード類に使用されるICチップのセキュリティ性が重要視されている。悪意のある攻撃者から情報を守るためには、暗号鍵などの生成に使用される乱数に十分な乱雑さ、即ち、エントロピー（乱数性)が求められる。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特許第５０７４３５９号公報
【特許文献２】特開２００５－１７４２０６号公報
【特許文献３】米国特許第８３４１２０１号明細書
【非特許文献】
【０００４】
【非特許文献１】Sanu K.Mathew et.al., “2.4 Gbps, 7mW All-Digital PVT-Variation Tolerant True Random Number Generator for 45 nm CMOS High-Performance Microprocessors”, IEEE JOURNAL OF SOLID-STATE CIRCUITS, VOL.47, NO.11, NOVEMBER 2012, pp. 2807-2821
【発明の概要】
【発明が解決しようとする課題】
【０００５】
実施形態は、高エントロピーのランダムデータを生成可能な乱数生成回路（RNG: Random Number Generator）を提案する。
【課題を解決するための手段】
【０００６】
実施形態によれば、乱数生成回路は、第1の発振信号が入力され、所定のデューティー比を有する第2の発振信号を出力する第1の回路と、第2の発振信号と前記第2の発振信号の周波数よりも低い周波数を有するクロックとに基づき複数の値をラッチする第2の回路と、前記複数の値に基づき制御信号を出力する第3の回路と、前記制御信号に基づき前記第1の回路を制御する第4の回路と、を備える。
【図面の簡単な説明】
【０００７】
【図１】乱数生成回路の実施例を示す図。
【図２】発振信号のデューティー比と0/1の出現頻度との関係を示す図。
【図３】0/1の出現頻度と処理内容とを示す図。
【図４】発振信号のデューティー比と0/1の出現頻度との関係を示す図。
【図５】発振信号のデューティー比と0/1の出現頻度との関係を示す図。

【図６】乱数生成回路の回路例を示す図。
【図７】セレクタの第1の例を示す図。
【図８】NANDゲート回路、インバータ回路、及び、NORゲート回路の例を示す図。
【図９】選択信号、信号経路、及び、デューティー比（増減）の関係を示す図。
【図１０】セレクタの第2の例を示す図。
【図１１】選択信号、信号経路、及び、デューティー比（増減）の関係を示す図。
【図１２】セレクタの第3の例を示す図。
【図１３】選択信号、信号経路、及び、デューティー比（増減）の関係を示す図。
【図１４】コントローラが出力する選択信号の例を示す図。
【図１５】セレクタの第4の例を示す図。
【図１６】選択信号、インバータ回路の駆動力、及び、デューティー比（増減）の関係を示す図。
【図１７】偏り検出ユニットの第1の例を示す図。
【図１８】乱数の偏りと制御信号との関係を示す図。
【図１９】偏り検出ユニットの第2の例を示す図。
【図２０】乱数の偏りと制御信号との関係を示す図。
【図２１】コントローラによるデューティー比の制御例を示す図。
【図２２】デューティー比の増減と選択信号との関係を示す図。
【図２３】乱数生成装置の例を示す図。
【図２４】Post-processingの例を示す図。
【図２５】システムの例を示す図。
【発明を実施するための形態】
【０００８】
（実施例）
以下、図面を参照しながら乱数生成回路（エントロピーソース生成回路）の実施例を説明する。乱数生成回路とは、情報セキュリティなどで用いられる高エントロピーな乱数（0又は1）を生成する回路のことである。
【０００９】
乱数を生成する方法は、大きく2つに分けられる。1つは、アルゴリズムによって何らかの初期値から疑似的に乱数を生成する方法である。もう1つは、乱数生成回路が持つ物理的な不確定要因に基づいて乱数を生成する方法である。前者の方法は、初期値が同じであるときに同じ結果を出力してしまう場合があるため、後者の方法は、前者の手法に比べて、より高いエントロピーを持つ乱数を生成できると考えられる。そこで、本実施例では、後者の方法を前提とする。
【００１０】
後者の方法において、物理的な不確定要因は、例えば、発振回路からの発振信号（0又は1）をその発振周波数よりも十分に低い周波数を持つサンプリングクロックの立ち上がりエッジ（0→1）又は立ち下がりエッジ（1→0）でラッチすることにより得ることができる。
【００１１】
例えば、発振回路（リングオシレータ）からの高周波数の発振信号をD型フリップフロップ回路のD-入力端子に入力することにより、D型フリップフロップ回路が0と1のいずれもラッチ可能なメタステーブル状態（metastable state）を作り出す。この場合、低周波数のサンプリングクロックをC-入力端子に入力すると、サンプリングクロックの立ち上がり時点のD-入力端子の値が、D型フリップフロップ回路内にラッチされ、かつ、Q-出力端子に出力される。即ち、D-入力端子に入力される0と1の割合が半々（1:1）であれば、D型フリップフロップ回路内に0がラッチされる確率と1がラッチされる確率も半々となり、これが物理的な不確定要因となる。
【００１２】
しかし、物理的な不確定要因は、このような発振回路の発振周波数とサンプリングクロ

ックの周波数との関係以外にも、温度、ノイズなどの環境的要素や、デバイスの製造ばらつきなどの製造的要素など、によっても生じる。しかも、これら環境的要素や製造的要素などは、0及び1の一方に有利となる方向、例えば、D型フリップフロップ回路内に0又は1の一方がラッチされ易くなる方向に、物理的な不確定要因に偏りを生じさせる場合がある。これでは、高エントロピーの乱数（ランダムデータ）を生成することができない。

【００１３】

そこで、本実施例では、第一に、物理的な不確定要因に偏りが発生しているか否かを検出する偏り検出ユニットを設け、第二に、物理的な不確定要因に偏りが発生しているときは、これを発振回路にフィードバックし、第三に、発振回路において物理的な不確定要因の偏りをなくす処理を行う技術を提案する。

【００１４】

例えば、図1に示すように、発振回路10と、発振回路10からの高周波数（例えば、100MHz～2GHz）の発振信号を低周波数（例えば、1MHz～10MHz）のサンプリングクロックの立ち上がりエッジ又は立ち下がりエッジによりラッチ可能なラッチ回路11と、を備える乱数生成回路を考える。発振回路10は、例えば、リングオシレータであり、ラッチ回路11は、例えば、D型フリップフロップ回路である。

【００１５】

この場合、発振信号のデューティー比（duty ratio）R_dutyが50％であれば、ラッチ回路11の出力信号が0となる確率は50％となり、ラッチ回路11の出力信号が1となる確率も50％となる。従って、高エントロピーのランダムデータを生成できる。但し、本実施例において、デューティー比R_dutyとは、発振信号の1周期の期間と発振信号が1である期間との比、即ち、発振信号が1である期間を発振信号の1周期の期間で割った値に100を掛けた値を意味するものとする。

【００１６】

図2は、発振信号のデューティー比R_duty（=B/A×100）が50％である場合に、ラッチ回路11の出力信号が0又は1となる確率（probability）を示している。

【００１７】

サンプリングクロックは、発振信号が1である期間w_1のセンターで立ち上がり、かつ、サンプリングクロックの立ち上がりは、ばらつき（ジッタ）を有する、と仮定すると、ラッチ回路11の出力信号が0又は1となる確率は、正規分布に従う。例えば、発振信号が1である期間w_1においてサンプリングクロックが立ち上がると、ラッチ回路11の出力信号は、1となり、発振信号が0である期間w_0においてサンプリングクロックが立ち上がると、ラッチ回路11の出力信号は、0となる。

【００１８】

1回のサンプリングにおいて、ラッチ回路11が1をラッチする確率P1は、正規分布上の網掛け部（1）の面積の和と見なすことができ、ラッチ回路11が0をラッチする確率P0は、正規分布上の白抜き部（0）の面積の和と見なすことができる。発振信号の位相とサンプリングクロックの位相が一定であると仮定すると、網掛け部(1)の面積は、正規分布全体の面積の50%となり、白抜き部(0)の面積は、正規分布全体の面積の50%となる。

【００１９】

従って、発振信号のデューティー比R_dutyが50％である場合、ラッチ回路11が1をラッチする確率P1と、ラッチ回路11が0をラッチする確率P0とは、それぞれ、50％となる。

【００２０】

しかし、上述のように、物理的な不確定要因に偏りが発生すると、確率P1と確率P0とは同じにならない。即ち、高エントロピーのランダムデータを生成できない。そこで、偏り検出ユニット12を用いて、物理的な不確定要因に偏りが発生しているか否かを、リアルタイムに、又は、所定時期に、検出する。

【００２１】

物理的な不確定要因に偏りが発生しているか否かは、ラッチ回路11の出力信号、即ち、乱数（0又は1）の値をモニターすることにより判断可能である。

【００２２】
例えば、偏り検出ユニット12は、ラッチ回路11の出力信号が0となる頻度（0の出現頻度）、ラッチ回路11の出力信号が1となる頻度（1の出現頻度）、又は、その両方をモニターする。偏り検出ユニット12は、0の出現頻度と1の出現頻度が同じ又はそれら出現頻度の差が一定範囲内であれば、物理的な不確定要因の偏りはないと判断できる。また、それ以外の場合、偏り検出ユニット12は、物理的な不確定要因の偏りがあると判断できる。
【００２３】
偏り検出ユニット12が、物理的な不確定要因に偏りが発生していると判断したときは、これを発振回路10にフィードバックする。発振回路10は、偏り検出ユニット12からの情報に基づき、物理的な不確定要因の偏りをなくす処理を行う。
【００２４】
例えば、図3に示すように、0の出現頻度f_0が1の出現頻度f_1よりも大きい場合（f_0 > f_1）、図4に示すように、発振信号のデューティー比R_duty（=B/A×100）は、環境的要素や製造的要素などによって、50％よりも小さくなっていると考えられる。この場合、発振回路10は、発振信号のデューティー比R_dutyを大きくする処理を行う。
【００２５】
また、図3に示すように、0の出現頻度f_0と1の出現頻度f_1とが同じ場合（f_0 = f_1）、図2に示すように、発振信号のデューティー比R_duty（=B/A×100）は、50％であると考えられる。この場合、発振回路10は、そのまま発振信号を出力し続ける。
【００２６】
さらに、図3に示すように、1の出現頻度f_1が0の出現頻度f_0よりも大きい場合（f_0 < f_1）、図5に示すように、発振信号のデューティー比R_duty（=B/A×100）は、環境的要素や製造的要素などによって、50％よりも大きくなっていると考えられる。この場合、発振回路10は、発振信号のデューティー比R_dutyを小さくする処理を行う。
【００２７】
このように、本実施例によれば、乱数（0又は1）の値をモニターし、それに基づいて、発振回路が出力する発振信号のデューティー比を制御することにより、高エントロピーのランダムデータを生成可能となる。
【００２８】
（回路例）
図6は、乱数生成回路の回路例を示している。
【００２９】
ラッチ回路11は、サンプリングクロックに基づき、発振信号OSC_1から乱数としての複数の値（例えば、4つの値）Qn，Q(n-1)，Q(n-2)，Q(n-3)をラッチする。サンプリングクロックの周波数は、発振信号OSC_1の周波数よりも十分に低い。この場合、ラッチ回路11は、例えば、複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)をラッチ可能な複数のラッチ部（例えば、4つのラッチ部）11n，11(n-1)，11(n-2)，11(n-3)を備える。
【００３０】
各ラッチ部11n，11(n-1)，11(n-2)，11(n-3)は、例えば、D型フリップフロップ回路である。また、複数のラッチ部11n，11(n-1)，11(n-2)，11(n-3)は、直列接続される。
【００３１】
例えば、発振信号OSC_1は、1段目のラッチ部11nのD-入力端子に入力される。1段目のラッチ部11nのQ-出力端子は、2段目のラッチ部11(n-1)のD-入力端子に接続される。2段目のラッチ部11(n-1)のQ-出力端子は、3段目のラッチ部11(n-2)のD-入力端子に接続される。3段目のラッチ部11(n-2)のQ-出力端子は、4段目のラッチ部11(n-3)のD-入力端子に接続される。乱数は、4段目のラッチ部11(n-3)のQ-出力端子から出力される。また、サンプリングクロックは、複数のラッチ部11n，11(n-1)，11(n-2)，11(n-3)のC-入力端子に入力される。
【００３２】
1つ目の値（0又は1）は、サンプリングクロックの1つ目の立ち上がりエッジにより1段

目のラッチ部11n内にラッチされる。2つ目の値（0又は1）は、サンプリングクロックの2つ目の立ち上がりエッジにより1段目のラッチ部11n内にラッチされる。この時、1つ目の値は、2段目のラッチ部11(n-1)内にラッチされる。

【００３３】

同様に、3つ目の値（0又は1）は、サンプリングクロックの3つ目の立ち上がりエッジにより1段目のラッチ部11n内にラッチされる。この時、2つ目の値及び1つ目の値は、それぞれ、2段目のラッチ部11(n-1)内及び3段目のラッチ部11(n-2)内にラッチされる。また、4つ目の値（0又は1）は、サンプリングクロックの4つ目の立ち上がりエッジにより1段目のラッチ部11n内にラッチされる。この時、3つ目の値、2つ目の値、及び、1つ目の値は、それぞれ、2段目のラッチ部11(n-1)内、3段目のラッチ部11(n-2)内、及び、4段目のラッチ部11(n-3)内にラッチされる。

【００３４】

偏り検出ユニット12は、ラッチ回路11内にラッチされる複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)に基づき、0の数（0の出現頻度）、1の数（1の出現頻度）、又は、その両方をモニターする。偏り検出ユニット12は、例えば、0の数と1の数とが同じであれば、物理的な不確定要因の偏りがないことを示す制御信号TUNE0，TUNE1を出力する。また、偏り検出ユニット12は、例えば、0の数と1の数とが異なれば、物理的な不確定要因の偏りがあることを示す制御信号TUNE0，TUNE1を出力する。

【００３５】

制御信号TUNE0，TUNE1は、発振回路10にフィードバックされる。

【００３６】

発振回路10は、例えば、発振信号OSC_0を生成する発振器13と、選択信号SELに基づき発振信号OSC_0のデューティー比R_dutyを変更し、これを発振信号OSC_1として出力するセレクタ14と、制御信号TUNE0，TUNE1に基づき選択信号SELを出力するコントローラ15と、を備える。

【００３７】

発振器13は、例えば、リングオシレータである。発振器13からの発振信号OSC_0のデューティー比R_dutyは、環境的要素や製造的要素などに起因する物理的な不確定要因の偏りによって変化する。コントローラ15は、制御信号TUNE0，TUNE1に基づき、この物理的な不確定要因の偏りを取り除く処理を制御する。

【００３８】

例えば、制御信号TUNE0，TUNE1が、乱数としての複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)に関して0の数が1の数よりも多いことを示すとき、発振信号OSC_0のデューティー比R_dutyは、50％よりも小さくなっていると考えられる。この場合、コントローラ15は、発振信号OSC_0のデューティー比R_dutyを大きくする選択信号SELを出力する。

【００３９】

また、制御信号TUNE0，TUNE1が、乱数としての複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)に関して1の数が0の数よりも多いことを示すとき、発振信号OSC_0のデューティー比R_dutyは、50％よりも大きくなっていると考えられる。この場合、コントローラ15は、発振信号OSC_0のデューティー比R_dutyを小さくする選択信号SELを出力する。

【００４０】

セレクタ14は、発振信号OSC_0のデューティー比R_dutyを変更又は維持する複数のオプションを備える。セレクタ14は、選択信号SELに基づき、複数のオプションのうちの1つを選択する。セレクタ14から出力される発振信号OSC_1は、50％又はそれに近いデューティー比R_dutyを持つ発振信号である。

【００４１】

（セレクタ）

図6の乱数生成回路内のセレクタの例を説明する。

【００４２】

図7は、セレクタの第1の例を示している。

【００４３】
セレクタ14は、発振信号OSC_0が入力され、発振信号OSC_0の位相を反転させた反転発振信号を出力するインバータ回路14_I0と、共通接続される複数の入力端子を備えるNANDゲート回路14_NANDと、1つの入力端子を備えるインバータ回路14_I1と、共通接続される複数の入力端子を備えるNORゲート回路14_NORと、NANDゲート回路14_NAND、インバータ回路14_I1、及び、NORゲート回路14_NORからの出力信号を選択し、発振信号OSC_1を出力するマルチプレクサ14_MUXと、を備える。
【００４４】
NANDゲート回路14_NAND、インバータ回路14_I1、及び、NORゲート回路14_NORは、それぞれ、発振信号OSC_0のデューティー比R_dutyを変更又は維持する複数のオプションである。
【００４５】
NANDゲート回路14_NANDは、例えば、2つの入力端子を備える2入力NANDゲート回路である。従って、インバータ回路14_I0からの反転発振信号は、NANDゲート回路14_NANDの2つの入力端子に入力される。
【００４６】
NANDゲート回路14_NANDは、例えば、図8に示すように、電源端子Vdd及び出力端子OUT間に並列接続される2つのPチャネルFETs (Field Effect Transistors)と、出力端子OUT及び電源端子Vss間に直列接続される2つのNチャネルFETsと、を備える。また、入力端子INは、全てのFETsのゲートに接続される。この場合、NANDゲート回路14_NANDは、PチャネルFETsのトータル駆動力（チャネル幅）がNチャネルFETsのトータル駆動力（チャネル幅）よりも大きなインバータ回路と等価となる。
【００４７】
従って、NANDゲート回路14_NANDが選択される場合、NANDゲート回路14_NANDは、0よりも1を出力し易くなる。これは、デューティー比R_dutyを大きくする（1の位相を長くする）ことを意味する。即ち、発振信号OSC_0のデューティー比R_dutyが50％よりも小さくなっていると想定されるときは、NANDゲート回路14_NANDを選択し、デューティー比R_dutyを大きくする補正処理を行う。その結果、発振信号OSC_1は、デューティー比R_dutyが50％又はそれに近い値の発振信号となる。
【００４８】
インバータ回路14_I1は、例えば、図8に示すように、電源端子Vdd及び出力端子OUT間に接続される1つのPチャネルFETと、出力端子OUT及び電源端子Vss間に接続される1つのNチャネルFETと、を備える。この場合、インバータ回路14_I1は、PチャネルFETの駆動力（チャネル幅）とNチャネルFETの駆動力（チャネル幅）とが等しいインバータ回路（デフォルト）となる。
【００４９】
従って、インバータ回路14_I1が選択される場合、インバータ回路14_I1は、入力信号のデューティー比R_dutyを変えずに、これをそのまま出力信号として出力する。即ち、発振信号OSC_0のデューティー比R_dutyが50％又はそれに近いときは、インバータ回路14_I1を選択し、デューティー比R_dutyを変化させない。
【００５０】
NORゲート回路14_NORは、例えば、2つの入力端子を備える2入力NORゲート回路である。従って、インバータ回路14_I0からの反転発振信号は、NORゲート回路14_NORの2つの入力端子に入力される。
【００５１】
NORゲート回路14_NORは、例えば、図8に示すように、電源端子Vdd及び出力端子OUT間に直列接続される2つのPチャネルFETsと、出力端子OUT及び電源端子Vss間に並列接続される2つのNチャネルFETsと、を備える。また、入力端子INは、全てのFETsのゲートに接続される。この場合、NORゲート回路14_NORは、NチャネルFETsのトータル駆動力（チャネル幅）がPチャネルFETsのトータル駆動力（チャネル幅）よりも大きなインバータ回路と等価と

なる。

【００５２】

従って、NORゲート回路14_NORが選択される場合、NORゲート回路14_NORは、1よりも0を出力し易くなる。これは、デューティー比R_dutyを小さくする（0の位相を長くする）ことを意味する。即ち、発振信号OSC_0のデューティー比R_dutyが50％よりも大きくなっていると想定されるときは、NORゲート回路14_NORを選択し、デューティー比R_dutyを小さくする補正処理を行う。その結果、発振信号OSC_1は、デューティー比R_dutyが50％又はそれに近い値の発振信号となる。

【００５３】

図9は、図7のセレクタにおいて、選択信号、信号経路、及び、デューティー比（増減）の関係を示している。

【００５４】

選択信号は、例えば、2ビットデータSEL[1:0]=SEL[1]，SEL[0]を使用可能である。選択信号SEL[1:0]は、図7のマルチプレクサ14_MUXに入力される。

【００５５】

例えば、選択信号SEL[1:0]が00のとき、NANDゲート回路14_NANDが選択される。NANDゲート回路14_NANDは、例えば、2入力NANDゲート回路であり、発振信号OSC_0のデューティー比R_dutyを+5％増やす。マルチプレクサ14_MUXは、選択信号SEL[1:0]が00のとき、NANDゲート回路14_NANDの出力信号を発振信号OSC_1として出力する。

【００５６】

また、選択信号SEL[1:0]が01のとき、インバータ回路14_I1が選択される。インバータ回路14_I1は、発振信号OSC_0のデューティー比R_dutyを変化させない（±0％）。マルチプレクサ14_MUXは、選択信号SEL[1:0]が01のとき、インバータ回路14_I1の出力信号を発振信号OSC_1として出力する。

【００５７】

さらに、選択信号SEL[1:0]が10のとき、NORゲート回路14_NORが選択される。NORゲート回路14_NORは、例えば、2入力NORゲート回路であり、発振信号OSC_0のデューティー比R_dutyを-5％減らす。マルチプレクサ14_MUXは、選択信号SEL[1:0]が10のとき、NORゲート回路14_NORの出力信号を発振信号OSC_1として出力する。

【００５８】

図7、図8、及び、図9の例では、デューティー比R_dutyを変更する複数のオプションは、3つであるが、複数のオプションの数は、変更可能である。一般的に、複数のオプションの数が多ければ、デューティー比R_dutyを高精度に制御可能となる。しかし、この場合、セレクタ14の回路規模が大きくなる。

【００５９】

従って、複数のオプションの数は、システムが要求するエントロピーや、乱数生成回路が形成されるチップのフロアプランなどを参考に、最適な数を選択すればよい。

【００６０】

図10は、セレクタの第2の例を示している。

【００６１】

第2の例は、デューティー比R_dutyを変更する複数のオプションの数が6種類ある例である。

【００６２】

セレクタ14は、発振信号OSC_0が入力され、発振信号OSC_0の位相を反転させた反転発振信号を出力するインバータ回路14_I0を備える。

【００６３】

セレクタ14は、6種類のオプションとして、共通接続される2つの入力端子を備えるNANDゲート回路14_NAND0と、共通接続される3つの入力端子を備えるNANDゲート回路14_NAND1と、共通接続される4つの入力端子を備えるNANDゲート回路14_NAND2と、1つの入力端子を備えるインバータ回路14_I1と、共通接続される2つの入力端子を備えるNORゲート回路14_

NOR0と、共通接続される3つの入力端子を備えるNORゲート回路14_NOR1と、を備える。

【００６４】

セレクタ14は、さらに、3つのNANDゲート回路14_NAND0，14_NAND1，14_NAND2、インバータ回路14_I1、及び、2つのNORゲート回路14_NOR0，14_NOR1からの出力信号を選択し、発振信号OSC_1を出力するマルチプレクサ14_MUXを備える。

【００６５】

3つのNANDゲート回路14_NAND0，14_NAND1，14_NAND2、インバータ回路14_I1、及び、2つのNORゲート回路14_NOR0，14_NOR1の回路例は、第1の例（図8の回路例）から容易に類推可能であるため、ここでの説明を省略する。

【００６６】

図11は、図10のセレクタにおいて、選択信号、信号経路、及び、デューティー比（増減）の関係を示している。

【００６７】

選択信号は、例えば、3ビットデータSEL[2:0]=SEL[2]，SEL[1]，SEL[0]を使用可能である。選択信号SEL[2:0]は、図10のマルチプレクサ14_MUXに入力される。

【００６８】

例えば、選択信号SEL[2:0]が001のとき、NANDゲート回路14_NAND2が選択される。NANDゲート回路14_NAND2は、例えば、4入力NANDゲート回路であり、発振信号OSC_0のデューティー比R_dutyを+15％増やす。マルチプレクサ14_MUXは、選択信号SEL[2:0]が001のとき、NANDゲート回路14_NAND2の出力信号を発振信号OSC_1として出力する。

【００６９】

選択信号SEL[2:0]が010のとき、NANDゲート回路14_NAND1が選択される。NANDゲート回路14_NAND1は、例えば、3入力NANDゲート回路であり、発振信号OSC_0のデューティー比R_dutyを+10％増やす。マルチプレクサ14_MUXは、選択信号SEL[2:0]が010のとき、NANDゲート回路14_NAND1の出力信号を発振信号OSC_1として出力する。

【００７０】

選択信号SEL[2:0]が011のとき、NANDゲート回路14_NAND0が選択される。NANDゲート回路14_NAND0は、例えば、2入力NANDゲート回路であり、発振信号OSC_0のデューティー比R_dutyを+5％増やす。マルチプレクサ14_MUXは、選択信号SEL[2:0]が011のとき、NANDゲート回路14_NAND0の出力信号を発振信号OSC_1として出力する。

【００７１】

選択信号SEL[2:0]が100のとき、インバータ回路14_I1が選択される。インバータ回路14_I1は、発振信号OSC_0のデューティー比R_dutyを変化させない（±0％）。マルチプレクサ14_MUXは、選択信号SEL[2:0]が100のとき、インバータ回路14_I1の出力信号を発振信号OSC_1として出力する。

【００７２】

選択信号SEL[2:0]が101のとき、NORゲート回路14_NOR0が選択される。NORゲート回路14_NOR0は、例えば、2入力NORゲート回路であり、発振信号OSC_0のデューティー比R_dutyを-5％減らす。マルチプレクサ14_MUXは、選択信号SEL[2:0]が101のとき、NORゲート回路14_NOR0の出力信号を発振信号OSC_1として出力する。

【００７３】

選択信号SEL[2:0]が110のとき、NORゲート回路14_NOR1が選択される。NORゲート回路14_NOR1は、例えば、3入力NORゲート回路であり、発振信号OSC_0のデューティー比R_dutyを-10％減らす。マルチプレクサ14_MUXは、選択信号SEL[2:0]が110のとき、NORゲート回路14_NOR1の出力信号を発振信号OSC_1として出力する。

【００７４】

図12は、セレクタの第3の例を示している。

【００７５】

第3の例は、第1の例（図7～図9）において、2入力NANDゲート回路を、PチャネルFETの駆動力（チャネル幅）DF_PがNチャネルFETの駆動力（チャネル幅）DF_Nの2倍であるインバ

ータ回路14_I2に置き換え、かつ、2入力NORゲート回路を、NチャネルFETの駆動力（チャネル幅）DF_NがPチャネルFETの駆動力（チャネル幅）DF_Pの2倍であるインバータ回路14_I3に置き換えた例である。但し、PチャネルFETのチャネル幅W_PとNチャネルFETのチャネル幅W_Nは、等しいものとする。

【００７６】

インバータ回路14_I2は、駆動力（チャネル幅）が$DF_P=2W_P$であるPチャネルFETと、駆動力（チャネル幅）が$DF_N=W_N$であるNチャネルFETと、を備える。PチャネルFETは、チャネル幅が$2W_P$である1つのトランジスタであってもよいし、チャネル幅がW_Pである2つのトランジスタを並列接続してもよい。

【００７７】

インバータ回路14_I3は、駆動力（チャネル幅）が$DF_P=W_P$であるPチャネルFETと、駆動力（チャネル幅）が$DF_N=2W_N$であるNチャネルFETと、を備える。NチャネルFETは、チャネル幅が$2W_N$である1つのトランジスタであってもよいし、チャネル幅がW_Nである2つのトランジスタを並列接続してもよい。

【００７８】

尚、2つのインバータ回路14_I0，14_I1は、第1の例と同じであるため、ここでの説明を省略する。

【００７９】

図13は、図11のセレクタにおいて、選択信号、信号経路、及び、デューティー比（増減）の関係を示している。

【００８０】

選択信号は、例えば、2ビットデータSEL[1:0]=SEL[1]，SEL[0]を使用可能である。選択信号SEL[1:0]は、図12のマルチプレクサ14_MUXに入力される。

【００８１】

例えば、選択信号SEL[1:0]が00のとき、インバータ回路14_I2が選択される。インバータ回路14_I2は、PチャネルFETの駆動力DF_PがNチャネルFETの駆動力DF_Nよりも大きいため、発振信号OSC_0のデューティー比R_dutyを+5％増やす。マルチプレクサ14_MUXは、選択信号SEL[1:0]が00のとき、インバータ回路14_I2の出力信号を発振信号OSC_1として出力する。

【００８２】

また、選択信号SEL[1:0]が01のとき、インバータ回路（デフォルト）14_I1が選択される。インバータ回路14_I1は、発振信号OSC_0のデューティー比R_dutyを変化させない（±0％）。マルチプレクサ14_MUXは、選択信号SEL[1:0]が01のとき、インバータ回路14_I1の出力信号を発振信号OSC_1として出力する。

【００８３】

さらに、選択信号SEL[1:0]が10のとき、インバータ回路14_I3が選択される。インバータ回路14_I3は、NチャネルFETの駆動力DF_NがPチャネルFETの駆動力DF_Pよりも大きいため、発振信号OSC_0のデューティー比R_dutyを-5％減らす。マルチプレクサ14_MUXは、選択信号SEL[1:0]が10のとき、インバータ回路14_I3の出力信号を発振信号OSC_1として出力する。

【００８４】

尚、セレクタの第1の例（図7～図9）、第2の例（図10～図11）、及び、第3の例（図12～図13）において、不選択のオプションをインバータ回路14_I0の出力端子から切断するゲート回路を追加してもよい。この場合、不選択のオプションを非動作状態にすることが可能なため、低消費電力化に有効である。

【００８５】

図15は、セレクタの第4の例を示している。

【００８６】

第4の例は、第1の例（図7～図9）において、バッファ回路としてのインバータ回路14_I0，14_I1を常に選択し、マルチプレクサを省略し、インバータ回路14_I1のPチャネルFET

の駆動力（チャネル幅）又はNチャネルFETの駆動力（チャネル幅）を実質的に変更することが可能な補助回路14_sub0，14_sub1を新たに追加する例である。

【００８７】

本例では、セレクタ14の選択信号として、PE0，PE1，NE0，NE1を使用する。従って、図14に示すように、コントローラ15は、選択信号PE0，PE1，NE0，NE1を出力する。

【００８８】

補助回路14_sub0は、電源端子Vdd及び出力端子OUT間に直列接続される2つのPチャネルFETsと、出力端子OUT及び電源端子Vss間に直列接続される2つのNチャネルFETsと、を備える。インバータ回路14_I0からの反転発振信号は、2つのPチャネルFETsの一方のゲート端子、及び、2つのNチャネルFETsの一方のゲート端子に、それぞれ入力される。選択信号PE0は、2つのPチャネルFETsの他方のゲート端子に入力され、選択信号NE0は、2つのNチャネルFETsの他方のゲート端子に入力される。

【００８９】

同様に、補助回路14_sub1は、電源端子Vdd及び出力端子OUT間に直列接続される2つのPチャネルFETsと、出力端子OUT及び電源端子Vss間に直列接続される2つのNチャネルFETsと、を備える。インバータ回路14_I0からの反転発振信号は、2つのPチャネルFETsの一方のゲート端子、及び、2つのNチャネルFETsの一方のゲート端子に、それぞれ入力される。選択信号PE1は、2つのPチャネルFETsの他方のゲート端子に入力され、選択信号NE1は、2つのNチャネルFETsの他方のゲート端子に入力される。

【００９０】

インバータ回路14_I1内のPチャネルFETの駆動力（チャネル幅）DF_P、補助回路14_sub0内の2つのPチャネルFETの駆動力（チャネル幅）DF_P、及び、補助回路14_sub1内の2つのPチャネルFETの駆動力（チャネル幅）DF_Pは、例えば、等しく、かつ、W_Pである。また、インバータ回路14_I1内のNチャネルFETの駆動力（チャネル幅）DF_N、補助回路14_sub0内の2つのNチャネルFETの駆動力（チャネル幅）DF_N、及び、補助回路14_sub1内の2つのNチャネルFETの駆動力（チャネル幅）DF_Nも、例えば、等しく、かつ、W_Nである。さらに、PチャネルFETのチャネル幅W_PとNチャネルFETのチャネル幅W_Nは、例えば、互いに等しい。

【００９１】

図16は、図15のセレクタにおいて、選択信号、信号経路、及び、デューティー比（増減）の関係を示している。

【００９２】

例えば、選択信号PE0，PE1が共に1であり、選択信号NE0，NE1が共に0であるとき、2つの補助回路14_sub0，14_sub1は、非動作状態である。この場合、インバータ回路14_I1内のPチャネルFETの駆動力$DF_P(=W_P)$とNチャネルFETの駆動力$DF_N(=W_N)$は、互いに等しいため、発振信号OSC_0のデューティー比R_dutyは変化せず、発振信号OSC_0が発振信号OSC_1として出力される（±0％）。

【００９３】

選択信号PE1が1であり、選択信号PE0，NE0，NE1が0であるとき、補助回路14_sub0において、制御信号PE0が入力されるPチャネルFETがオン状態となる。また、補助回路14_sub1は、非動作状態である。この場合、インバータ回路14_I1内のPチャネルFETの駆動力DF_Pが実質的に$2W_P$となる。即ち、インバータ回路14_I1内のPチャネルFETの駆動力DF_Pは、インバータ回路14_I1内のNチャネルFETの駆動力DF_Nの2倍となる。

【００９４】

従って、セレクタ14は、発振信号OSC_0のデューティー比R_dutyを+5％増やし、これを発振信号OSC_1として出力する。

【００９５】

選択信号PE0，PE1，NE0，NE1が全て0であるとき、2つの補助回路14_sub0，14_sub1において、制御信号PE0，PE1が入力される2つのPチャネルFETがそれぞれオン状態となる。この場合、インバータ回路14_I1内のPチャネルFETの駆動力DF_Pが実質的に$3W_P$となる。即ち、インバータ回路14_I1内のPチャネルFETの駆動力DF_Pは、インバータ回路14_I1内のNチャ

ネルFETの駆動力DF_Nの3倍となる。

【００９６】

従って、セレクタ14は、発振信号OSC_0のデューティー比R_dutyを+10％増やし、これを発振信号OSC_1として出力する。

【００９７】

選択信号PE0，PE1，NE0が1であり、選択信号NE1が0であるとき、補助回路14_sub0において、制御信号NE0が入力されるNチャネルFETがオン状態となる。また、補助回路14_sub1は、非動作状態である。この場合、インバータ回路14_I1内のNチャネルFETの駆動力DF_Nが実質的に$2W_N$となる。即ち、インバータ回路14_I1内のNチャネルFETの駆動力DF_Nは、インバータ回路14_I1内のPチャネルFETの駆動力DF_Pの2倍となる。

【００９８】

従って、セレクタ14は、発振信号OSC_0のデューティー比R_dutyを-5％減らし、これを発振信号OSC_1として出力する。

【００９９】

選択信号PE0，PE1，NE0，NE1が全て1であるとき、2つの補助回路14_sub0，14_sub1において、制御信号NE0，NE1が入力される2つのNチャネルFETがそれぞれオン状態となる。この場合、インバータ回路14_I1内のNチャネルFETの駆動力DF_Nが実質的に$3W_N$となる。即ち、インバータ回路14_I1内のNチャネルFETの駆動力DF_Nは、インバータ回路14_I1内のPチャネルFETの駆動力DF_Pの3倍となる。

【０１００】

従って、セレクタ14は、発振信号OSC_0のデューティー比R_dutyを-10％減らし、これを発振信号OSC_1として出力する。

【０１０１】

（偏り検出ユニット）

図6の乱数生成回路内の偏り検出ユニットの例を説明する。

【０１０２】

図17は、偏り検出ユニットの第1の例を示している。

【０１０３】

偏り検出ユニット12は、乱数としての複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)が入力され、制御信号TUNE0を出力するAND回路12_0と、複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)の反転信号が入力され、制御信号TUNE1を出力するAND回路12_1と、を備える。制御信号TUNE0，TUNE1は、コントローラ15に入力される。

【０１０４】

この場合、例えば、図18に示すように、乱数としての複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)の全てが0のとき、制御信号TUNE1が1となる。

【０１０５】

複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)の全てが0であるということは、0の出現頻度が多いことを意味する。0の出現頻度が多いということは、発振信号のデューティー比R_dutyが50％よりも小さいと考えられる。従って、偏り検出ユニット12は、発振信号のデューティー比R_dutyを大きくする指示として、制御信号TUNE1(=1)を出力する。

【０１０６】

また、例えば、図18に示すように、乱数としての複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)の全てが1のとき、制御信号TUNE0が1となる。

【０１０７】

複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)の全てが1であるということは、1の出現頻度が多いことを意味する。1の出現頻度が多いということは、発振信号のデューティー比R_dutyが50％よりも大きいと考えられる。従って、偏り検出ユニット12は、発振信号のデューティー比R_dutyを小さくする指示として、制御信号TUNE0(=1)を出力する。

【０１０８】

さらに、複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)が、全て0でなく、かつ、全て1でない場

合、2つの制御信号TUNE0，TUNE1は、共に0となる。

【０１０９】

本例では、複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)が、全て0でなく、かつ、全て1でない場合、乱数（0又は1）の生成に大きな偏りはないと判断し、現在の発振信号のデューティー比R_dutyをそのまま維持する。

【０１１０】

図19は、偏り検出ユニットの第2の例を示している。

【０１１１】

第2の例は、乱数としての複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)，…Q(n-7)に関し、1の数が閾値（下限）N_lower又はそれよりも小さいか、及び、1の数が閾値（上限）N_higher又はそれよりも大きいか、を判断することにより、制御信号TUNE0，TUNE1を決定する例である。本例では、1の数を対象とするが、これに代えて、0の数を対象としてもよい。

【０１１２】

偏り検出ユニット12は、乱数としての複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)，…Q(n-7)が入力され、制御信号TUNE0を出力する論理回路12_0’と、複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)，…Q(n-7)が入力され、制御信号TUNE1を出力する論理回路12_1’と、を備える。制御信号TUNE0，TUNE1は、コントローラ15に入力される。

【０１１３】

この場合、例えば、図20に示すように、論理回路12_1’は、乱数としての複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)，…Q(n-7)のうち、1の数の合計Total_1が閾値（例えば、1）N_lowerと同じ又はそれよりも少ないと判断すると、制御信号TUNE1を1にする。

【０１１４】

複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)，…Q(n-7)のうち、1の数の合計Total_1が閾値N_lowerと同じ又はそれよりも少ないということは、0の出現頻度が多いことを意味する。0の出現頻度が多いということは、発振信号のデューティー比R_dutyが50％よりも小さいと考えられる。従って、偏り検出ユニット12は、発振信号のデューティー比R_dutyを大きくする指示として、制御信号TUNE1(=1)を出力する。

【０１１５】

また、例えば、図20に示すように、論理回路12_0’は、乱数としての複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)，…Q(n-7)のうち、1の数の合計Total_1が閾値（例えば、7）N_higherと同じ又はそれよりも多いと判断すると、制御信号TUNE0を1にする。

【０１１６】

複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)，…Q(n-7)のうち、1の数の合計Total_1が閾値N_higherと同じ又はそれよりも多いということは、1の出現頻度が多いことを意味する。1の出現頻度が多いということは、発振信号のデューティー比R_dutyが50％よりも大きいと考えられる。従って、偏り検出ユニット12は、発振信号のデューティー比R_dutyを小さくする指示として、制御信号TUNE0(=1)を出力する。

【０１１７】

本例では、複数の値Qn，Q(n-1)，Q(n-2)，Q(n-3)，…Q(n-7)のうち、1の数の合計Total_1が、N_lower＜Total_1＜N_higherであるときは、乱数（0又は1）の生成に大きな偏りはないと判断し、現在の発振信号のデューティー比R_dutyをそのまま維持する。即ち、制御信号TUNE0，TUNE1は、共に0となる。

【０１１８】

（コントローラ）

図21は、コントローラによるデューティー比の制御例を示している。図22は、図21の制御例における選択信号の状態を示している。

【０１１９】

コントローラは、図6、図14、図17、及び、図19のコントローラ15である。コントローラは、偏り検出ユニットからの制御信号TUNE0，TUNE1に基づき、発振信号のデューティー比R_dutyの増減を制御する。

【０１２０】
例えば、制御信号TUNE1が1（0の出現頻度が多い）を示しているとき、コントローラは、発振信号のデューティー比R_dutyを+5％増やす選択信号SEL[1:0]=00を出力する。
【０１２１】
また、デューティー比R_dutyが+5％増加している状態において、さらに、制御信号TUNE1が1を示すとき、コントローラは、発振信号のデューティー比R_dutyをさらに増やすか、又は、この状態(+5％)を維持する選択信号を出力する。いずれを選択するかは、セレクタ内の複数のオプションの数に依存する。例えば、図7又は図12のセレクタを採用する場合、複数のオプションの数は、3つである。
【０１２２】
従って、図21及び図22に示すように、デューティー比R_dutyが+5％増加している状態において、さらに、制御信号TUNE1が1を示すとき、コントローラは、発振信号のデューティー比R_dutyを+5％増加のまま維持する選択信号SEL[1:0]=00を出力する。
【０１２３】
また、デューティー比R_dutyが+5％増加している状態において、制御信号TUNE0，TUNE1が共に0を示すときも、コントローラは、発振信号のデューティー比R_dutyを+5％増加のまま維持する選択信号SEL[1:0]=00を出力する。
【０１２４】
さらに、デューティー比R_dutyが+5％増加している状態において、制御信号TUNE0が1を示すとき、コントローラは、発振信号のデューティー比R_dutyを減らす、即ち、デューティー比R_dutyの増減を±0％に戻す選択信号SEL[1:0]=01を出力する。デューティー比R_dutyの増減が±0％の状態において、制御信号TUNE0，TUNE1が共に0を示すとき、コントローラは、発振信号のデューティー比R_dutyの増減が±0％の状態を維持する選択信号SEL[1:0]=01を出力する。
【０１２５】
また、デューティー比R_dutyの増減が±0％の状態において、制御信号TUNE0が1を示すとき、コントローラは、発振信号のデューティー比R_dutyを-5％減らす選択信号SEL[1:0]=10を出力する。デューティー比R_dutyが-5％減少している状態において、さらに、制御信号TUNE0が1を示すとき、及び、制御信号TUNE0，TUNE1が共に0を示すとき、コントローラは、発振信号のデューティー比R_dutyを-5％減少のまま維持する選択信号SEL[1:0]=10を出力する。
【０１２６】
さらに、デューティー比R_dutyが-5％減少している状態において、制御信号TUNE1が1を示すとき、コントローラは、発振信号のデューティー比R_dutyを増やす、即ち、デューティー比R_dutyの増減を±0％に戻す選択信号SEL[1:0]=01を出力する。
【０１２７】
（乱数生成装置）
上述の乱数生成回路を用いた乱数生成装置の例を説明する。
【０１２８】
図23は、乱数生成装置の例を示している。
【０１２９】
乱数生成装置30は、複数の乱数生成回路RNG_0，RNG_1，…RNG_n（nは2以上の自然数）と、複数の乱数生成回路RNG_0，RNG_1，…RNG_nの出力信号ROSC_0，ROSC1，…ROSC_nが入力され、乱数を出力するポストプロセッシング(Post-processing)20と、を備える。
【０１３０】
各乱数生成回路RNG_0，RNG_1，…RNG_nは、上述の乱数生成回路である。ポストプロセッシング20は、複数の乱数生成回路RNG_0，RNG_1，…RNG_nからの出力信号（乱数）ROSC_0，ROSC1，…ROSC_nに、さらに論理的な処理を加え、さらに高エントロピーの乱数を生成するための回路である。
【０１３１】

ポストプロセッシング20は、例えば、図24に示すように、攪拌回路21と、LFSR（Linear Feedback Shift Register）22と、加算器23と、ビットシフト回路24と、自己平滑回路25と、シフトレジスタ26と、を備える。

【０１３２】

攪拌回路21は、出力信号ROSC_0，ROSC1，…ROSC_nをランダムに選択し、選択された複数の出力信号を攪拌関数により互いに結合し、複数ビットを出力する。LFSR22は、自己平滑回路25からの複数ビットをフィードバックすることにより、出力データ（乱数）の周期性を取り除き、より高いエントロピーを実現する回路である。加算器23は、攪拌回路21からの複数ビットとLFSR22からの複数ビットを加算する。

【０１３３】

ビットシフト回路24は、加算器23からの複数ビットをシフトし、自己平滑回路25に出力する。自己平滑回路25は、ビットシフト回路24からの複数ビットに対して、0/1の出現頻度を均等化する処理を行い、0/1の出現頻度が均等化された複数ビットを出力する回路である。シフトレジスタ26は、自己平滑回路25からの複数ビットに基づき、最終的な乱数を出力する。

【０１３４】

（システム）

上述の乱数生成回路を利用したシステムの例を説明する。

【０１３５】

図25は、システムの例を示している。

【０１３６】

このシステムは、無線通信などの情報通信において高いセキュリティ性が求められるシステム、例えば、クレジットカードやICカードなどに搭載されるシステムである。

【０１３７】

プロセッサ31は、例えば、情報通信におけるデータ転送などを制御する。バッファメモリ32は、例えば、RAM (Random Access Memory)などの揮発性メモリであり、データを一時的に記憶する。ストレージメモリ33は、例えば、NANDフラッシュメモリなどの不揮発性メモリであり、ファームウェアを記憶する。

【０１３８】

セキュリティモジュール34は、例えば、情報通信においてデータの暗号化に使用される暗号鍵を生成し、データを暗号化(encrypt)／復号化(decrypt)する。乱数生成装置30は、例えば、暗号鍵の生成に使用される乱数を出力する。乱数生成装置30は、例えば、図23の乱数生成装置である。通信モジュール35は、例えば、情報通信においてデータの送受信(transmitting/receiving)を制御する。

【０１３９】

システムバス36は、乱数生成装置30、プロセッサ31、バッファメモリ32、ストレージメモリ33、セキュリティモジュール34、及び、通信モジュール35を互いに接続する。

【０１４０】

（むすび）

以上、本実施例によれば、発振回路が出力する発振信号のデューティー比を制御することにより高エントロピーの乱数（ランダムデータ）を生成できる。

【０１４１】

本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

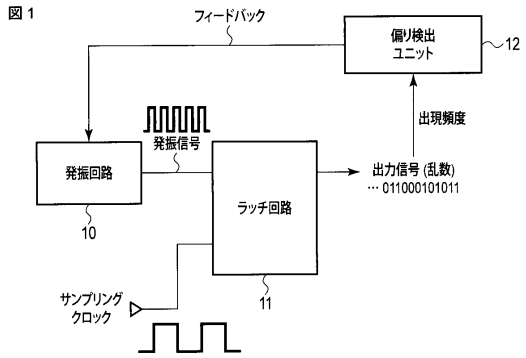
【符号の説明】

【０１４２】

10： 発振回路、 11： ラッチ回路、 11n, 11(n-1), 11(n-2), 11(n-3)： ラッチ部（フリップフロップ回路）、 12： 偏り検出ユニット、 13： 発振器、 14： セレクタ、 15： コントローラ、 20： Post-processing、 21： 攪拌回路、 22： LFSR、 23： 加算器、 24： ビットシフト回路、 25： 自己平滑回路、 26： シフトレジスタ、 30： 乱数生成装置、 31： プロセッサ、 32： バッファメモリ、 33： ストレージメモリ、 34： セキュリティモジュール、 35： 通信モジュール。

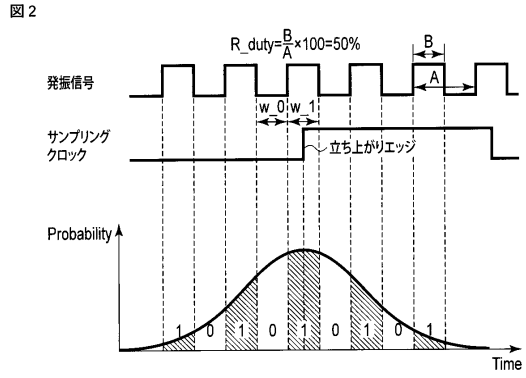
【図１】

図1



【図２】

図2



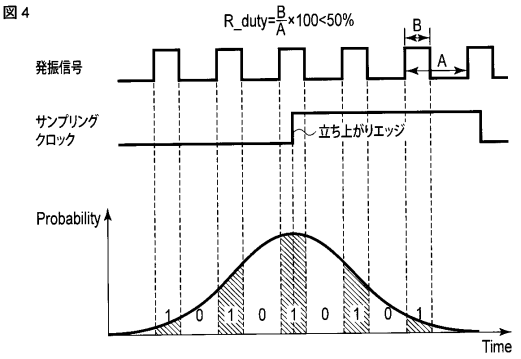
【図３】

図3

出現頻度	発振信号のデューティー比	処理
f_0 > f_1 (0が多い)	R_duty < 50%	発振信号のデューティー比を大きくする
f_0 = f_1	R_duty = 50%	そのまま
f_0 < f_1 (1が多い)	R_duty > 50%	発振信号のデューティー比を小さくする

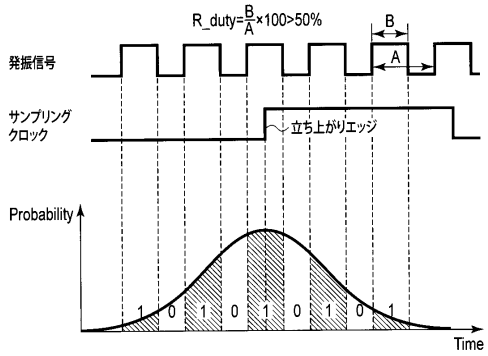
【図４】

図4



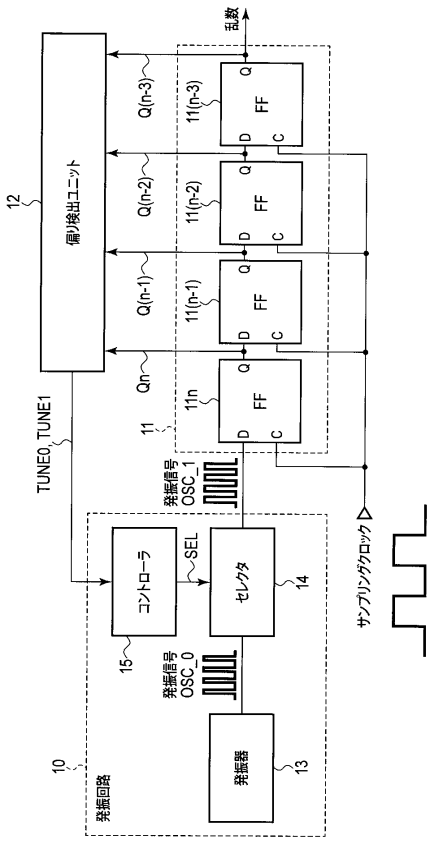
【図５】

図５



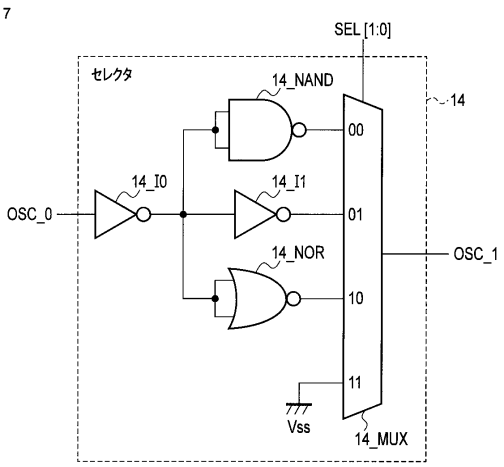
【図６】

図６



【図７】

図７



【図８】

図８

シンボル	回路例
NANDゲート回路 IN — OUT	Vdd Vdd IN OUT Vss ※P-channel FETsのトータル駆動力が N-channel FETsのトータル駆動力よりも大きい
インバータ回路 IN — OUT	Vdd IN OUT Vss ※P-channel FETsのトータル駆動力と N-channel FETsのトータル駆動力とが等しい
NORゲート回路 IN — OUT	Vdd OUT IN Vss Vss ※N-channel FETsのトータル駆動力が P-channel FETsのトータル駆動力よりも大きい

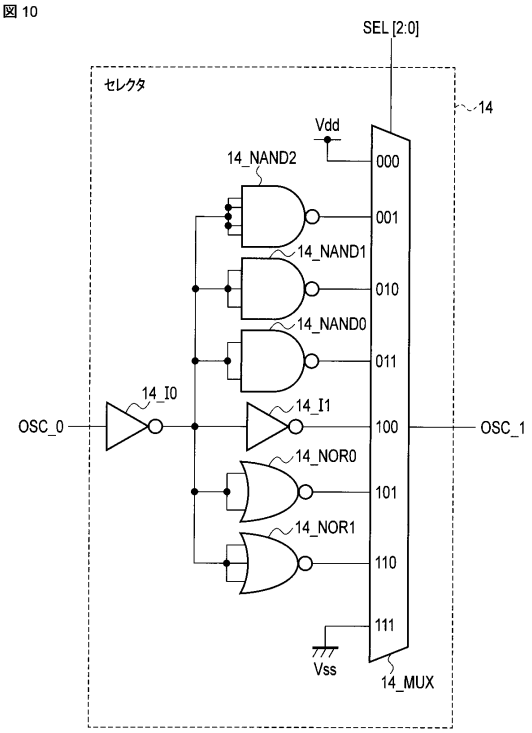
【図９】

図 9

SEL [1:0]	信号経路	デューティー比 (増減)
00	2入力NANDゲート回路	+5%
01	インバータ回路	±0%
10	2入力NORゲート回路	-5%
11	(不使用)	(不使用)

【図１０】

図 10



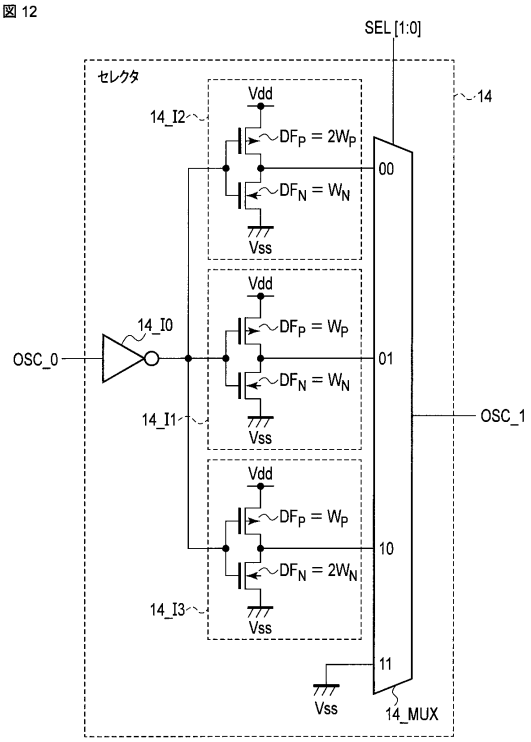
【図１１】

図 11

SEL [2:0]	信号経路	デューティー比 (増減)
000	(不使用)	(不使用)
001	4入力NANDゲート回路	+15%
010	3入力NANDゲート回路	+10%
011	2入力NANDゲート回路	+5%
100	インバータ回路	±0%
101	2入力NORゲート回路	-5%
110	3入力NORゲート回路	-10%
111	(不使用)	(不使用)

【図１２】

図 12



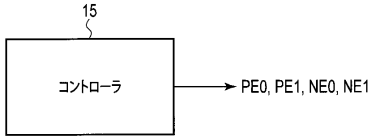
【図１３】

図 13

SEL [1:0]	信号経路	デューティー比 (増減)
00	インバータ回路 ($DF_P > DF_N$)	+5%
01	インバータ回路 (デフォルト:$DF_P = DF_N$)	±0%
10	インバータ回路 ($DF_P < DF_N$)	-5%
11	(不使用)	(不使用)

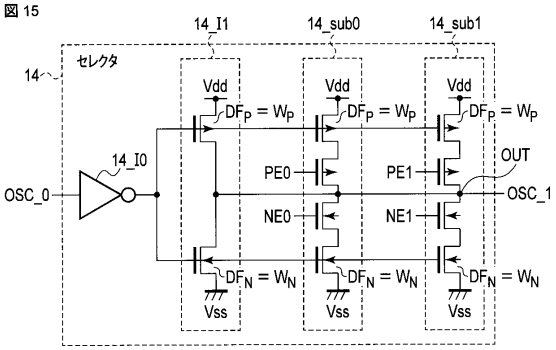
【図１４】

図 14



【図１５】

図 15



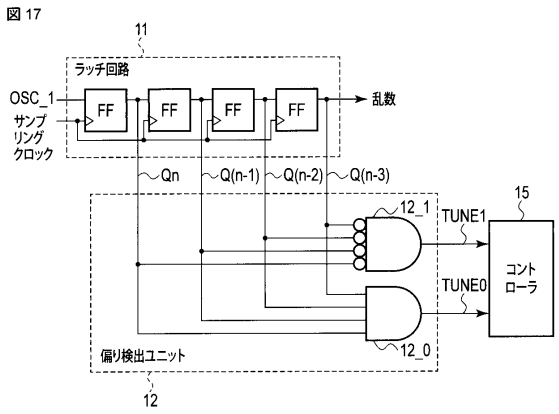
【図１６】

図 16

NE1	NE0	PE0	PE1	インバータ回路 14_I1 の駆動力	デューティー比 (増減)
0	0	0	0	$DF_P = DF_N \times 3$	+10%
0	0	0	1	$DF_P = DF_N \times 2$	+5%
0	0	1	1	デフォルト $DF_P = DF_N$	±0%
0	1	1	1	$DF_N = DF_P \times 2$	-5%
1	1	1	1	$DF_N = DF_P \times 3$	-10%

【図１７】

図 17



【図１８】

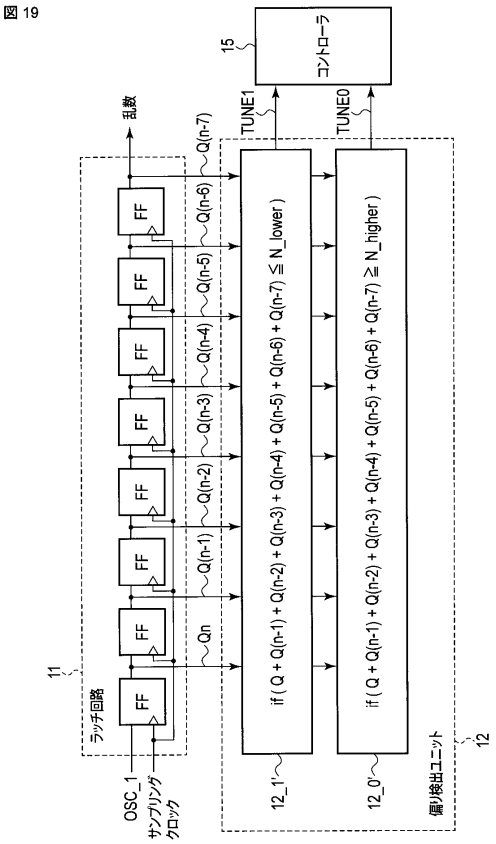
図 18

Qn	Q(n-1)	Q(n-2)	Q(n-3)	TUNE1	TUNE0
0	0	0	0	1	0
1	1	1	1	0	1
X	X	X	X	0	0

XXXXは、Qn,Q(n-1),Q(n-2)及びQ(n-3)が全て0でなく、かつ、全て1でない場合を示す

【図１９】

図 19

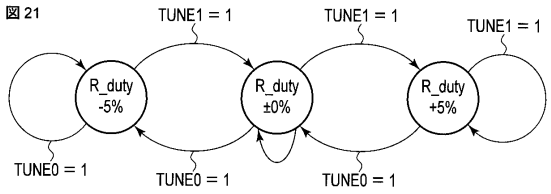


【図２０】

図 20

1の数の合計 Total_1	TUNE1	TUNE0
Total_1 ≦ N_lower	1	0
Total_1 ≧ N_higher	0	1
N_lower < Total_1 < N_higher	0	0

【図２１】

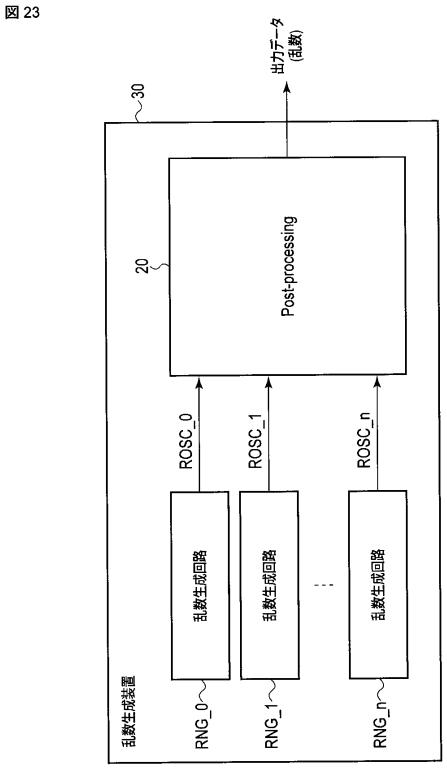


【図２２】

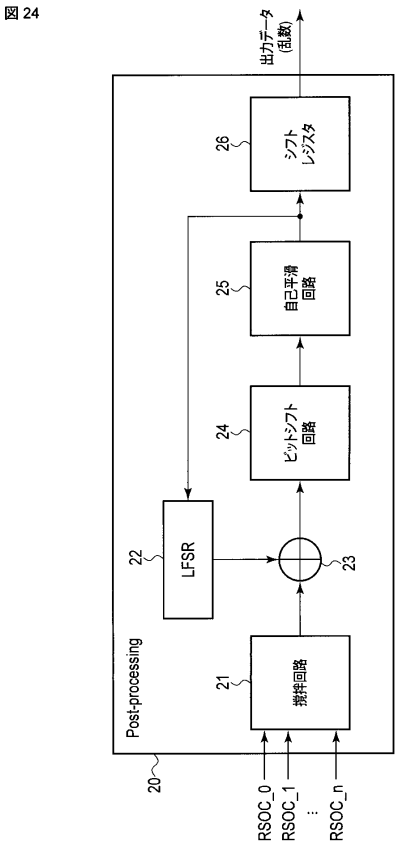
図 22

State	SEL [1:0]
R_duty +5%	00
R_duty ±0%	01
R_duty -5%	10

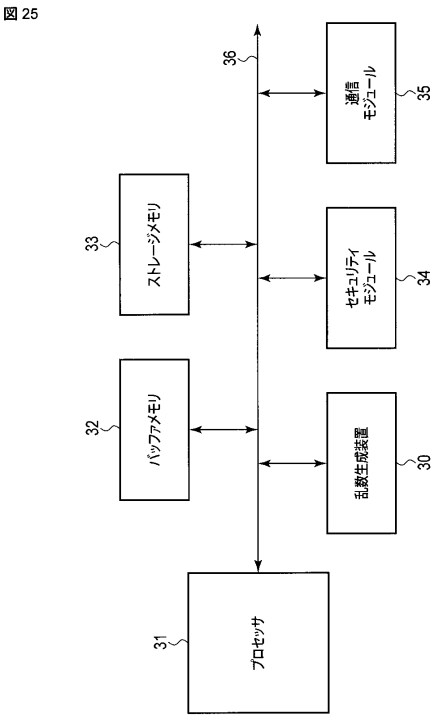
【図２３】



【図２４】



【図２５】



フロントページの続き

(72)発明者　藤田　忍
東京都港区芝浦一丁目１番１号　株式会社東芝内

審査官　佐賀野　秀一

(56)参考文献　米国特許出願公開第２０１０／０１０６７５７（ＵＳ，Ａ１）
特開２００５－０３３０８９（ＪＰ，Ａ）
特開平１０－３０３７３８（ＪＰ，Ａ）
特開２００３－１０８３６３（ＪＰ，Ａ）
特開２０１４－１０２７６８（ＪＰ，Ａ）
特開昭６１－２６５９１４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　１／０４－　１／１４
Ｇ０６Ｆ　　７／５８－　７／７２
Ｇ０９Ｃ　　１／００－　５／００
Ｈ０３Ｋ　　３／６４－　３／８６
Ｈ０４Ｋ　　１／００－　３／００
Ｈ０４Ｌ　　９／００－　９／３８