

(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2005-293489

(P2005-293489A)

(43) 公開日 平成17年10月20日(2005. 10. 20)

(51) Int.Cl. ⁷	F I	テーマコード (参考)
G06F 7/58	G06F 7/58	5 J 0 4 9
H03K 3/315	H03K 3/315	
H03K 3/84	H03K 3/84	Z

審査請求 未請求 請求項の数 12 O L (全 10 頁)

(21) 出願番号	特願2004-111230 (P2004-111230)	(71) 出願人	000004226
(22) 出願日	平成16年4月5日(2004. 4. 5)		日本電信電話株式会社
			東京都千代田区大手町二丁目3番1号
		(74) 代理人	100075753
			弁理士 和泉 良彦
		(74) 代理人	100081341
			弁理士 小林 茂
		(72) 発明者	松崎 秀昭
			東京都千代田区大手町二丁目3番1号
			日本電信電話株式会
			社内
		(72) 発明者	佐野 公一
			東京都千代田区大手町二丁目3番1号
			日本電信電話株式会
			社内
		Fターム(参考)	5J049 AA01 BB02 CA00 CA07 CA09

(54) 【発明の名称】 乱数発生回路

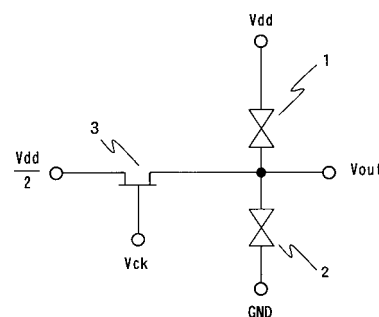
(57) 【要約】

【課題】高速で、回路規模が小さく、かつ消費電力の少ない乱数発生回路として複数の負性微分抵抗素子を用いる回路構成が知られている。従来この構成では、負性微分素子の極大電流値が等しいことが要求され、回路設計上の難点となっていた。本発明においては、極大電流値のばらつきの影響が少なく、かつ高速で、低消費電力の乱数発生回路の実現を目的とした。

【解決手段】直列に接続した2つの負性微分抵抗素子の接続点に電源電圧の1/2の電圧を印加することにより、これら負性微分抵抗素子回路の不安定点に一致させて初期状態とする。次に駆動用トランジスタをOFF状態としてこの電圧を取り除くと、出力点が上記不安定点から論理1または0のどちらかの安定点に遷移することを利用して乱数を発生させる構成とした。

【選択図】 図1

図1



【特許請求の範囲】**【請求項 1】**

二つの負性微分抵抗素子を直列に接続して得られる回路の両端に直流電圧 V_{dd} を第一の電圧として印加し、

前記回路の一方の端子には前記直流電圧 V_{dd} の高電位側を接続し、

他方の端子には前記直流電圧 V_{dd} の低電位側を接続し、

前記二つの負性微分抵抗素子の接続点に電界効果型トランジスタの第一の電極としてのソース電極を接続し、

前記電界効果型トランジスタの第二の電極としてのドレイン電極に前記直流電圧 V_{dd} の 2 分の 1 の電圧すなわち $V_{dd} / 2$ を第二の電圧として印加し、

10

前記接続点を出力電圧 V_{out} の出力点とし、

前記電界効果型トランジスタの第三の電極としてのゲート電極に、振動電圧を印加することで、前記電界効果型トランジスタの ON / OFF を制御し、

前記電界効果型トランジスタが ON の時に前記接続点に前記第 2 の電圧を印加し、

前記電界効果型トランジスタが OFF の時に、前記接続点に印加されている第二の電圧を遮断し、この際、不可避免的に加わる負性微分抵抗素子特性の熱揺らぎによって決定される出力を前記出力点から出力し、それを自然乱数として用いることを特徴とする乱数発生回路。

【請求項 2】

請求項 1 に記載の乱数発生回路において、

20

電界効果型トランジスタの代わりにバイポーラトランジスタを用い、電界効果型トランジスタのゲート、ドレイン、ソースの各電極を、それぞれバイポーラトランジスタのベース、コレクタ、エミッタの各電極と置き換えることを特徴とする乱数発生回路。

【請求項 3】

請求項 1 または請求項 2 に記載の乱数発生回路において、

前記負性微分抵抗素子の少なくとも一方について、抵抗体を前記負性微分抵抗素子に並列に接続して得られる回路を複合負性微分抵抗素子として置き換えたことを特徴とする乱数発生回路。

【請求項 4】

請求項 1 または請求項 2 に記載の乱数発生回路において、

30

前記負性微分抵抗素子の少なくとも一方について、トランジスタを前記負性微分抵抗素子に並列に接続して得られる回路を複合負性微分抵抗素子として置き換えたことを特徴とする乱数発生回路。

【請求項 5】

請求項 1 または請求項 2 に記載の乱数発生回路において、

前記負性微分抵抗素子の少なくとも一方について、抵抗体とトランジスタとを前記負性微分抵抗素子に並列に接続して得られる複合負性微分抵抗素子に置き換えたことを特徴とする乱数発生回路。

【請求項 6】

請求項 1 乃至請求項 5 の何れかに記載の乱数発生回路において、

40

前記負性微分抵抗素子として共鳴トンネルダイオードを用いることを特徴とする乱数発生回路。

【請求項 7】

請求項 1 乃至請求項 5 の何れかに記載の乱数発生回路において、

前記負性微分抵抗素子としてエサキダイオードを用いることを特徴とする乱数発生回路。

【請求項 8】

請求項 1 乃至請求項 5 の何れかに記載の乱数発生回路において、

前記負性微分抵抗素子としてトランジスタで構成される負性微分抵抗特性を有する回路を用いることを特徴とする乱数発生回路。

50

【請求項 9】

請求項 1 乃至請求項 8 の何れかに記載の乱数発生回路を複数個使用し、
前記複数の乱数発生回路を並列に設置し、
並列データ構成の乱数出力を得ることを特徴とする乱数発生回路。

【請求項 10】

請求項 1 乃至請求項 8 の何れかに記載の乱数発生回路を用い、
単一の乱数発生回路を複数回サンプリングすることにより直列データ出力を得ることを
特徴とする乱数発生回路。

【請求項 11】

請求項 1 乃至請求項 8 の何れかに記載の乱数発生回路において、
前記電界効果型トランジスタまたは前記バイポーラトランジスタの前記第 2 の電極に前
記第二の電圧 $V_{dd}/2$ を印加する方法として、
前記二つの負性微分抵抗素子の直列接続回路への前記第一の電圧 V_{dd} と接地との間に
同じ大きさの 2 本の抵抗体を直列に接続し、該 2 本の抵抗体の接続点から、前記第二の電
圧 $V_{dd}/2$ を得、該第二の電圧 $V_{dd}/2$ を前記電界効果型トランジスタまたは前記バ
イポーラトランジスタの前記第二の電極に供給することを特徴とする乱数発生回路。

【請求項 12】

請求項 11 に記載の乱数発生回路において、
前記抵抗体の代わりに 2 個の直列接続したキャパシタを用い、該キャパシタの接続点か
ら前記第二の電圧 $V_{dd}/2$ に相当する電圧を発生せしめることを特徴とする乱数発生回
路。

【発明の詳細な説明】**【技術分野】****【0001】**

本発明は、自然乱数の高速発生が可能で、低消費電力であり、かつ占有面積を小さくし
得る小回路規模な乱数発生回路に関する。

【背景技術】**【0002】**

乱数を得る方法としては、予め定められたプログラムによって乱数を発生する擬似乱数
発生法と、自然界で生じる確率的事象を利用した自然乱数発生法との 2 つが挙げられる。
ともに、暗号化通信における鍵の生成などに利用されるが、前者はアルゴリズムが知られ
てしまうと、生成される乱数が予測できるが、後者は文字通り、自然界で確率的に生じる
事象を利用するため、予測不可能な真の乱数が得られる。このため、後者の自然界におけ
る確率事象を利用する方法による乱数発生を用いることが通信における情報の暗号化には
最適とされている。

【0003】

従来の自然乱数を得る方法として、抵抗体を用意し、熱雑音によって生じる抵抗値の揺
らぎを電圧変換し、さらに増幅器によって雑音信号を増幅し、得られる雑音信号に対して
、予め定めた閾値と比較することで、論理値 “0” または “1” の判定を行い、乱数を得
るという方法がある。

【0004】

あるいは、下記（特許文献 1）で開示されている負性微分抵抗素子を用いた、高速かつ
低電力消費を満たしながら乱数を得る方法もある。これは二つの極大電流値の等しい負性
微分抵抗素子を直列に接続した回路を振動型の電圧で駆動し、その際、雑音によって 2 つ
の素子の極大電流値の均衡を崩し、論理値 “0” または “1” のどちらかに出力を決定す
る方法である。

【0005】

上記の抵抗体の熱雑音によって生じる抵抗値の揺らぎは非常に微小であるため、信号増
幅のため利得の大きな増幅器を用意する必要があり、結果として、乱数発生回路の大規模

10

20

30

40

50

化およびそれに伴う消費電力の増大を引き起こす。据え置き型の端末であれば、このような乱数発生器を利用しても大きな問題は生じないが、携帯端末やスマートカード等、端末の物理的サイズが小さく、あらゆる回路部品の低消費電力化が望まれる場合にこれを利用することは不可能である。また、乱数の発生速度も 240 Mbit/s 程度であり、最近の高速・大容量化するネットワークに対応するためには、より高速な乱数発生回路が要求される。

【0006】

【特許文献1】特開2000-259395号公報

【発明の開示】

【発明が解決しようとする課題】

10

【0007】

このため、本発明においては、以上の問題点を解決した、高速、小回路規模（小占有面積）、かつ低消費電力の乱数発生回路を実現するため負性微分抵抗素子を利用する構成とした。しかし、従来技術では、熱雑音のような微小な揺らぎを検出するためには、回路中で使用する複数の負性微分抵抗素子の極大電流値をあらかじめ等しく揃えておく必要があった。

【0008】

しかし、実際上は、結晶構造の不均一性や素子作製工程上で生ずる素子面積の微小な揺らぎ（ばらつき）等により、上記の極大電流値を等しく揃えることは極めて困難であり、乱数を発生させるためには、極大電流値を等しく揃えるための回路上の工夫が不可欠となり、回路設計が困難になる、という問題があった。本発明では、上記課題を克服するために、素子特性のばらつきに対して影響が小さく、極大電流値に多少の大小があっても、極めて簡単な回路構成で高速かつ、低電力消費を満たしながら安定で実用性の高い自然乱数を得る回路を提供することを目的とした。

20

【課題を解決するための手段】

【0009】

上記目的を達成するために、本発明の請求項1においては、二つの負性微分抵抗素子を直列に接続して得られる回路の両端に直流電圧 V_{dd} を第一の電圧として印加し、前記回路の一方の端子には前記直流電圧 V_{dd} の高電位側を接続し、他方の端子には前記直流電圧 V_{dd} の低電位側、例えば接地電位を接続し、前記二つの負性微分抵抗素子の接続点に電界効果型トランジスタの第一の電極としてのソース電極を接続し、前記電界効果型トランジスタの第二の電極としてのドレイン電極に前記直流電圧 V_{dd} の2分の1の電圧すなわち $V_{dd}/2$ を第二の電圧として印加し、前記接続点を出力電圧 V_{out} の出力点とし、前記電界効果型トランジスタの第三の電極としてのゲート電極に、振動電圧を印加することで、前記電界効果型トランジスタのON/OFFを制御し、前記電界効果型トランジスタがONの時に前記接続点に前記第2の電圧を印加し、前記電界効果型トランジスタがOFFの時に、前記接続点に印加されている第二の電圧を遮断し、この際、不可避免に加わる負性微分抵抗素子特性の熱揺らぎ、すなわち熱雑音、によって決定される出力を前記出力点から出力し、それを自然乱数として用いる構成について規定した。

30

【0010】

請求項2においては、請求項1に記載の乱数発生回路において、電界効果型トランジスタの代わりにバイポーラトランジスタを用い、電界効果型トランジスタのゲート、ドレイン、ソースの各電極を、それぞれバイポーラトランジスタのベース、コレクタ、エミッタの各電極と置き換えた構成について規定した。

40

【0011】

請求項3においては、請求項1または請求項2に記載の乱数発生回路において、前記負性微分抵抗素子の少なくとも一方について、抵抗体を前記負性微分抵抗素子に並列に接続して得られる回路を複合負性微分抵抗素子として置き換えた構成について規定した。

【0012】

請求項4においては、請求項1または請求項2に記載の乱数発生回路において、前記負

50

性微分抵抗素子の少なくとも一方について、トランジスタを前記負性微分抵抗素子に並列に接続して得られる回路を複合負性微分抵抗素子として置き換えた構成について規定した。

【0013】

請求項5においては、請求項1または請求項2に記載の乱数発生回路において、前記負性微分抵抗素子の少なくとも一方について、抵抗体とトランジスタとを前記負性微分抵抗素子に並列に接続して得られる回路を複合負性微分抵抗素子として置き換えた構成について規定した。

【0014】

請求項6においては、請求項1乃至請求項5の何れかに記載の乱数発生回路において、前記負性微分抵抗素子として共鳴トンネルダイオードを用いる構成について規定した。 10

【0015】

請求項7においては、請求項1乃至請求項5の何れかに記載の乱数発生回路において、前記負性微分抵抗素子としてエサキダイオードを用いた構成について規定した。

【0016】

請求項8においては、請求項1乃至請求項5の何れかに記載の乱数発生回路において、前記負性微分抵抗素子としてトランジスタで構成される負性微分抵抗特性を有する回路を用いた構成について規定した。

【0017】

請求項9においては、請求項1乃至請求項8の何れかに記載の乱数発生回路を複数個使用し、前記複数の乱数発生回路を並列に設置し、並列データ構成の乱数出力を得る構成について規定した。 20

【0018】

請求項10においては、請求項1乃至請求項8の何れかに記載の乱数発生回路を用い、単一の乱数発生回路を複数回サンプリングすることにより直列データ出力を得る構成について規定した。

【0019】

請求項11においては、請求項1乃至請求項10の何れかに記載の乱数発生回路において、前記電界効果型トランジスタまたは前記バイポーラトランジスタの前記第2の電極に前記第二の電圧 $V_{dd}/2$ を印加する方法として、前記二つの負性微分抵抗素子の直列接続回路への前記第一の電圧 V_{dd} と接地との間に同じ大きさの2本の抵抗体を直列に接続し、該2本の抵抗体の接続点から、前記第二の電圧 $V_{dd}/2$ を得、該第二の電圧 $V_{dd}/2$ を前記電界効果型トランジスタまたは前記バイポーラトランジスタの前記第二の電極に供給する構成について規定している。 30

【0020】

請求項12においては、請求項11に記載の乱数発生回路において、前記抵抗体の代わりに2個の直列接続したキャパシタを用い、該キャパシタの接続点から前記第二の電圧 $V_{dd}/2$ に相当する電圧を発生せしめる構成について規定している。

【発明の効果】

【0021】

本発明によれば、2つの負性微分抵抗素子および1つの駆動用トランジスタの僅か3つの素子を用いるだけで高速で安定な乱数を発生させることができ、かつ2つの負性微分抵抗素子に要求される電気特性の均一性も緩和されるようになる。このため、本発明は高速、低消費電力を特長とする自然乱数発生回路の作製を容易にし、ならびに設計自由度の向上にも資するものである。

【発明を実施するための最良の形態】

【0022】

本発明は、負性微分抵抗素子を直列に接続した回路に直流電圧を印加し、2つの負性微分抵抗素子の接続点に接続されたトランジスタをON/OFFすることにより乱数発生回路動作の制御を行うことで、乱数発生動作を制御するものである。すなわち、駆動用トラ 50

10

20

30

40

50

ンジスタをON状態とすることで、負性微分抵抗素子を直列に接続した回路の出力電位を、2つの負性微分抵抗素子から得られる負荷曲線上の不安定点に一致させ、これを初期状態とし、そこから、駆動用トランジスタをOFF状態とすることで、負性微分抵抗素子に生じる雑音によって、出力電位が負荷曲線上の不安定点から、(0, 1)どちらかの安定点に遷移することを利用して、乱数出力を得る。本回路では、2つの負性微分抵抗素子の極大電流値に多少の大小関係があっても、それが、負荷曲線上の不安定点における不安定性や、安定点へ遷移に大きな影響を与えることがないため、出来上がりの素子の電流 - 電圧特性に多少のばらつきがあっても、乱数を得る上で致命的な問題は生じない。わずかにでも雑音が生じさえすれば、安定点への遷移、すなわち(0, 1)の出力分岐を得ること(熱雑音のような微小な揺らぎを検出すること)が充分可能となるのである。

10

【0023】

以下、本発明の実施の形態を図により説明する。図1はその回路図である。

共鳴トンネルダイオード1および2を直列に接続し、この直列接続した回路の両端に直流電圧V_{dd}を印加し、その一端にこの直流電圧の高電位側を接続し、他の一端には同じ直流電圧の低電位側、例えば接地電位(GND)を接続し、駆動用トランジスタ3のドレインにはV_{dd}/2の直流電圧を印加し、ゲートには駆動用のクロック(V_{ck})を印加する。図2(a)および(b)は、この回路の動作原理を示すための直列接続した負性微分抵抗素子の電流(I) - 電圧(V)特性である。図2(a)および(b)における負荷曲線4は共鳴トンネルダイオード1に、負荷曲線5は共鳴トンネルダイオード2に対応している。

20

【0024】

クロックV_{ck}が高電位にある場合、トランジスタ3はON状態となり、図2(a)に示す様に、回路の出力電位V_{out}は、負荷曲線上の不安定点電圧V_{dd}/2に一致し、これに固定される。しかし、クロックV_{ck}が低電位(例えば接地電位)となると、トランジスタ3はOFF状態となり、2つの共鳴トンネルダイオード1および2の接続点に印加されていた電位V_{dd}/2が取り除かれるので出力点の電位V_{out}は不安定状態となる。

【0025】

従ってこの場合は、図2(b)に示す様に、出力点の電位V_{out}は、必ず高電位側("1")か、低電位側("0")の何れか一方の安定点に遷移することになる。どちらの安定点に遷移するかは、少なくとも一方の共鳴トンネルダイオード1または2の電流(I) - 電圧(V)特性に熱雑音由来の揺らぎが生じることによる負荷曲線の変化の様子によって決定される。

30

【0026】

図3(a)のような負荷曲線(I - V特性)の熱雑音由来の揺らぎによる変化が生じた場合、すなわち例えば負荷曲線5が高電位側にシフトした場合(図3/a-1)、2つの共鳴トンネルダイオード1および2の接続点の電位、すなわち出力点の電位V_{out}は低電位側の安定点に遷移し、出力点の論理レベル"0"が得られる。また、負荷曲線4が高電位側にシフトした場合(図3/a-2)においても出力点の電位は低電位側の安定点に遷移し、出力として論理レベル"0"が得られる。一方、図3(b)のような負荷曲線の変化が生じた場合、すなわち負荷曲線5が低電位側にシフトした場合(図3/b-1)、高電位側の安定点へ遷移し、出力点の論理レベル"1"が得られる。また、負荷曲線4が低電位側にシフトした場合(図3/b-2)、出力点の電位は高電位側の安定点に遷移し、出力点の電位"1"が得られる。図4は共鳴トンネルダイオードの電流 - 電圧特性に適当な揺らぎを与えた場合の出力変化の様子をシミュレーションで示したもので、下側の波形図は駆動用のトランジスタ3のゲートに印加したクロックV_{ck}の電圧波形で、上側の波形図は出力点V_{out}における電圧波形を示している。この場合の乱数発生速度(シミュレーションでは恣意的な揺らぎを与えているため、正確には乱数ではないことに注意)は1 Gbit/sであり、出力振幅として0.7 V程度が得られている。また、共鳴トンネルダイオードの電流 - 電圧特性における電流の絶対値が5%ほど揺らいだとしても、

40

50

同様な出力波形を得ることができ、従来技術に比べ、2つの負性微分抵抗素子の電流 - 電圧特性に多少の違いがあっても、自然乱数が極めて簡単に得られることがわかる。

【0027】

また、熱雑音による揺らぎの効果を大きくするために、図5に示すように、共鳴トンネルダイオード1および2にそれぞれ並列にダイオード接続したトランジスタ6および7を接続する回路構成、あるいは図6に示すように共鳴トンネルダイオード1および2にそれぞれ並列に抵抗体8および9を接続する構成も可能である。このような構成をとることによって、熱雑音による効果が拡大されるため周辺回路や環境に起因する外部雑音の影響を減らすことができ、回路作成上、外部雑音の遮蔽に関する要求条件が緩和される、という利点がある。しかしながら、共鳴トンネルダイオードのみで回路を構成した場合とくらべ、消費電力は大きくなってしまう。また、さらなる熱揺らぎの効果を得るために共鳴トンネルダイオードに並列にトランジスタと抵抗体の両者を接続する構成もあるが、この場合も、外部雑音の遮蔽に関する要求条件が緩和される。しかしながら、これら2方法においては、共鳴トンネルダイオードのみで回路を構成した場合と比べ、消費電力が大きくなることは避けられない。

10

【0028】

さらにまた、これらの実施例における負性抵抗素子として、共鳴トンネルダイオードの代わりにエサキダイオードや、トランジスタを複数組み合わせ得られる負性微分抵抗特性を有する回路を用いても同様の発明の効果が得られる。しかしながら、エサキダイオードやトランジスタ回路に比べ、共鳴トンネルダイオードのスイッチング速度は速いため、高速乱数発生という観点では共鳴トンネルダイオードを用いた方がよい。さらに、共鳴トンネルダイオードの代わりにトランジスタで負性微分抵抗特性を有する回路を使用しても同様の結果を得ることが出来る。

20

なお、駆動用トランジスタへの印加電圧 $V_{dd}/2$ を確保するためには、図7に示すように、抵抗体10および11を直列接続し、その接続点から電圧 $V_{dd}/2$ を得る抵抗分割回路、あるいは図8に示すようにキャパシタ12および13を直列接続し、その接続点から $V_{dd}/2$ に相当する電圧を得る容量分割回路を用いてもよい。

【0029】

以上の説明においては駆動用トランジスタとして電界効果型トランジスタを使用した場合について説明したが、電界効果型トランジスタのソース、ドレイン、ゲートの代わりにバイポーラトランジスタのエミッタ、コレクタ、ベースを使用しても同様の結果を得ることが出来る。

30

さらに、図1に示す回路を複数個並列に用意し、所望のbit数の並列データ出力としての乱数を得ることも可能である。また、例えば負性微分抵抗素子として共鳴トンネルダイオードを用いれば、回路の高速性を活かすことで、一つの回路で複数回のサンプリングを行い、所望のbit数の直列データ出力としての乱数を得ることも可能である。

【図面の簡単な説明】

【0030】

【図1】本発明における基本構成を示す回路図。

【図2】本発明の動作原理を説明する負荷曲線図で、(a)は不安定点に直流電圧を印加した時の状態、(b)は前記印加電圧を取り除いたときの安定点への移動の状態を示す負荷曲線。

40

【図3】負荷曲線の変動と論理値設定の関係を示し、(a)は論理値“0”に安定する場合、(b)は論理値“1”に安定する場合を示すI-V特性の変化を示す負荷曲線図。

【図4】シミュレーションによる乱数出力波形図で、(a)は出力の乱数の、(b)は乱数発生駆動用クロックの波形図。

【図5】負性微分抵抗素子に並列にトランジスタを接続した場合の回路図。

【図6】負性微分抵抗素子に並列に抵抗体を接続した場合の回路図。

【図7】抵抗分割により電圧 $V_{dd}/2$ を設定する場合の回路図。

【図8】容量分割により電圧 $V_{dd}/2$ を設定する場合の回路図。

50

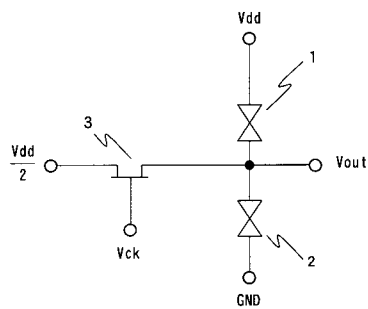
【符号の説明】

【0031】

- 1、2：共鳴トンネルダイオード
 3：駆動用トランジスタ
 4、5：負荷曲線（I - V 特性）
 6、7：トランジスタ
 8、9、10、11：抵抗体
 12、13：キャパシタ

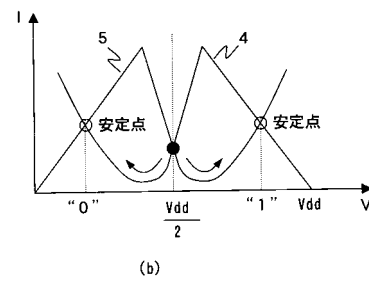
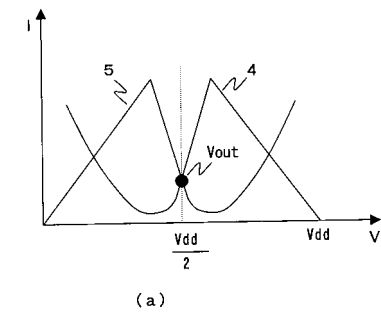
【図1】

図1



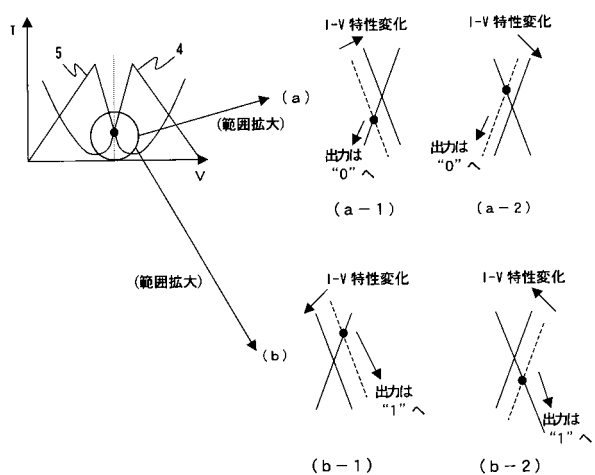
【図2】

図2



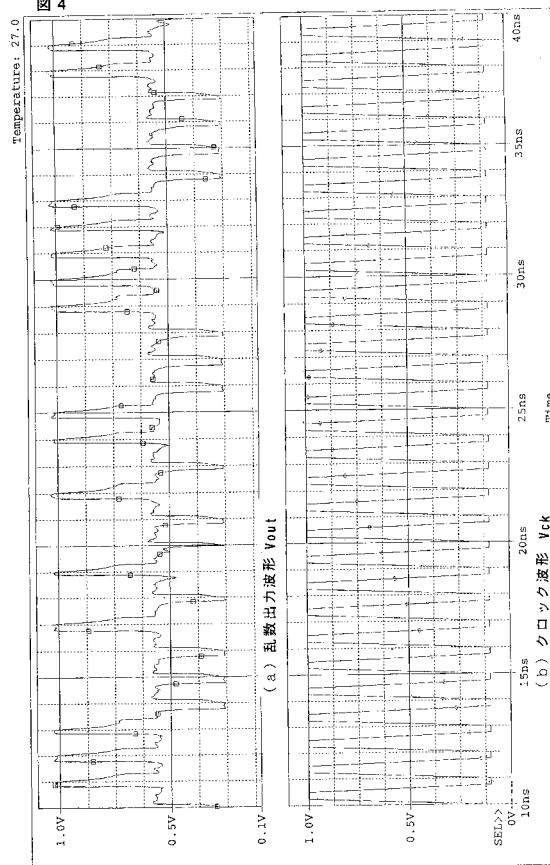
【図 3】

図 3



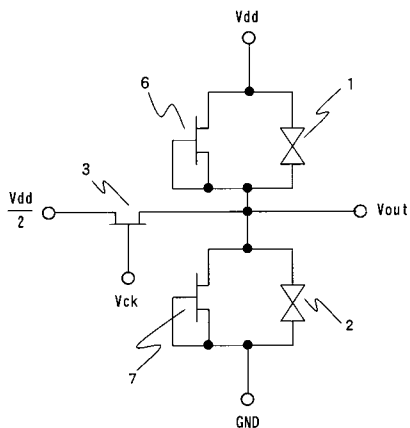
【図 4】

図 4



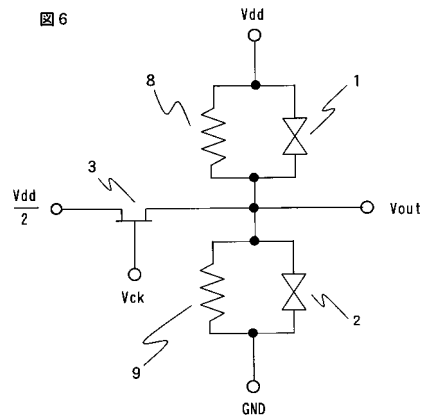
【図 5】

図 5



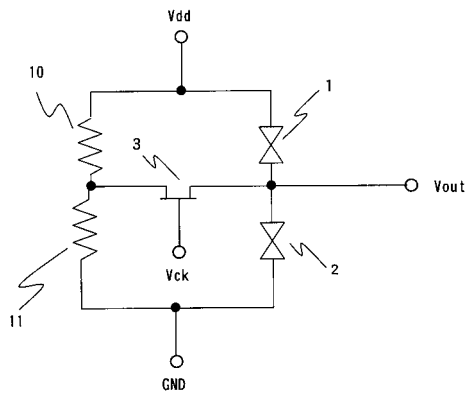
【図 6】

図 6



【 図 7 】

図 7



【 図 8 】

図 8

