(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4353435号
(P4353435)
(45)発行日　平成21年10月28日(2009.10.28)　(24)登録日　平成21年8月7日(2009.8.7)

(51)Int.Cl.　F I
G06F 7/58 (2006.01)　G06F 7/58 A

請求項の数 18 (全 32 頁)

(21)出願番号　特願2005-517843(P2005-517843)
(86)(22)出願日　平成16年2月12日(2004.2.12)
(86)国際出願番号　PCT/JP2004/001486
(87)国際公開番号　WO2005/078573
(87)国際公開日　平成17年8月25日(2005.8.25)
審査請求日　平成19年1月9日(2007.1.9)

(73)特許権者　000233169
株式会社日立超エル・エス・アイ・システムズ
東京都小平市上水本町５丁目２２番１号
(74)代理人　100081938
弁理士　徳若　光政
(72)発明者　村中　雅也
東京都小平市上水本町５丁目２２番１号
株式会社　日立超エル・エス・アイ・システムズ内

審査官　山崎　慎一

最終頁に続く

(54)【発明の名称】乱数発生方法と半導体集積回路装置及び電子装置

(57)【特許請求の範囲】
【請求項１】
乱数を利用する電子装置における乱数発生方法であって、
上記電子装置には、雑音検出対象回路と該雑音検出対象回路の出力信号が入力される増幅回路とを一組として含む単位回路の複数と、該複数の単位回路からの出力信号が入力される信号変化検出回路とが半導体基板上に配置された半導体チップまたは半導体集積回路装置が実装されており、
上記雑音検出対象回路のそれぞれは互いに同じ製造過程をもって同一の形態として形成された第１論理回路及び第２論理回路を備えてなり、
上記複数の単位回路と上記信号変化検出回路とが動作状態にされたとき、
上記単位回路のそれぞれにおいて上記第１論理回路及び第２論理回路のしきい値電圧の差電圧に重畳される雑音を増幅して２値信号を生成する段階と、
上記信号変化検出回路が、上記複数の単位回路のそれぞれから出力される２値信号のうちのいずれか１つの信号変化に応答して出力信号を生成する段階と、
上記信号変化検出回路から出力される２値信号の複数を組み合わせて乱数を生成する段階と、
が実行されることを特徴とする乱数発生方法。
【請求項２】
請求項１において、
上記第１論理回路及び第２論理回路はそれぞれ第１入力と第２入力を有する論理ゲート

回路からなり、上記第１論理回路に含まれる論理ゲート回路はその出力が当該論理ゲート回路の第１入力に接続され、上記第２論理回路に含まれる論理ゲート回路の第１入力が上記第１論理回路に含まれる論理ゲート回路の出力に接続され、

上記増幅回路は、第１入力と第２入力を有する論理ゲート回路の複数からなり、該論理ゲート回路はそれぞれ出力が当該論理ゲート回路の第１入力に接続された構成を備え、このような接続構成の前記複数の論理ゲート回路が縦列形態に接続された構成を備えてなり、

上記第１論理回路、第２論理回路及び増幅回路を構成する論理ゲートの第２入力にそれぞれ上記動作制御信号が供給されたとき上記複数の単位回路が動作状態となることを特徴とする乱数発生方法。

【請求項３】

請求項２において、

上記半導体チップまたは上記半導体集積回路装置は、動作制御信号を生成する順序回路をさらに含み、

上記複数の単位回路を上記動作制御信号に対応して順次選択状態とし、全ての単位回路の出力信号をシリアルに出力させて上記信号変化検出回路により１ビット分の乱数を生成することを特徴とする乱数発生方法。

【請求項４】

請求項３において、

上記信号変化検出回路は排他的論理回路を含み、上記動作制御信号に対応して上記選択状態となった単位回路から順次シリアルに出力される出力信号を受けて上記乱数を生成することを特徴とする乱数発生方法。

【請求項５】

請求項３において、

上記１ビットの乱数に対応した全ての単位回路からの出力信号の組み合わせに基づき、上記半導体チップまたは上記半導体集積回路装置に対する識別信号を生成することを特徴とする乱数発生方法。

【請求項６】

請求項１において、

上記電子装置はさらに算術方式の乱数発生回路を含み、

上記信号変化検出回路で生成された乱数を上記算術方式の乱数発生回路に供給し、

上記算術方式の乱数発生回路は、上記信号変化検出回路からの乱数を初期値として乱数を生成することを特徴とする乱数発生方法。

【請求項７】

乱数を利用する電子装置における乱数発生方法であって、

上記電子装置には、雑音検出対象回路と該雑音検出対象回路の出力信号が入力される増幅回路とを一組として含む単位回路の複数と、該複数の単位回路からの出力信号が入力される信号変化検出回路と、算術方式の乱数発生回路とが半導体基板上に配置された半導体チップまたは半導体集積回路装置が実装されており、

前記雑音検出対象回路のそれぞれは互いに同じ製造過程をもって同一の形態として形成された第１論理回路及び第２論理回路を備えてなり、

動作状態において、

上記単位回路のそれぞれにおいて上記第１論理回路及び第２論理回路のしきい値電圧の差電圧に重畳される雑音を増幅して２値信号を生成する段階と、

上記単位回路の複数から出力される複数ビットからなる信号を上記算術方式の乱数発生回路に供給する段階と、

上記算術方式の乱数発生回路が、上記単位回路の複数から供給された複数ビットからなる信号を初期値として乱数を生成する段階と、

を実行することを特徴とする乱数発生方法。

【請求項８】

互いに同じ製造過程をもって同一の形態として形成された第１論理回路及び第２論理回路と、上記第１論理回路及び第２論理回路のしきい値電圧の差電圧に重畳される雑音を増幅して２値信号を形成する増幅回路とからなる単位回路の複数と、

上記複数の単位回路から出力される複数からなる２値信号のうちのいずれか１つの信号変化に応答して出力信号を形成する信号変化検出回路と

を備え、

上記信号変化検出回路から出力される２値信号から乱数を生成してなることを特徴とする半導体集積回路装置。

【請求項９】

請求項８において、

上記第１論理回路及び第２論理回路と上記増幅回路とは、第１入力と第２入力を有する論理ゲート回路からなり、

上記第１論理回路に対応した論理ゲート回路の第１入力と出力とが接続され、

上記第２論理回路に対応した論理ゲート回路の第１入力は、上記第１論理回路に対応した論理ゲート回路の共通接続された入力と出力に接続され、

上記第１論理回路及び第２論理回路に対応した論理ゲート回路の第２入力には、動作制御信号が供給されてなり、

上記増幅回路は、複数の論理ゲート回路の第１入力と出力とが縦列形態に接続され、第２入力には上記動作制御信号が供給されてなることを特徴とする半導体集積回路装置。

【請求項１０】

請求項９において、

動作制御信号を生成する順序回路をさらに含み、

上記複数の単位回路は、上記動作制御信号に対応して順次に選択状態にされ、

上記複数の単位回路の出力部に上記信号変化検出回路が設けられてなることを特徴とする半導体集積回路装置。

【請求項１１】

請求項１０において、

上記信号変化検出回路は排他的論理回路を含み、上記動作制御信号に対応して選択状態になった前記単位回路から順次出力される出力信号を受けて上記乱数を生成することを特徴とする半導体集積回路装置。

【請求項１２】

請求項１１において、

上記論理ゲート回路は、ＣＭＯＳ構成の論理ゲート回路であり、上記動作制御信号により単位回路が非動作状態にされるときに、次段のゲート回路のＰチャネルＭＯＳＦＥＴをオフ状態にさせるものであることを特徴とする半導体集積回路装置。

【請求項１３】

請求項１１において、

上記複数の単位回路は、行列配置されてなり、

行列配置される各単位回路の入力部には、第１入力と第２入力を有する論理ゲート回路が設けられて、第１入力と第２入力に行及び列選択信号が供給され、その出力により上記第１論理回路及び第２論理回路を構成する論理ゲート回路を選択状態にさせる動作制御信号が形成され、

上記各単位回路の増幅回路を構成する論理ゲート回路の第２入力には、行方向に配置される前段からの単位回路の出力信号が伝えられるものであり、かかる増幅回路は上記動作制御信号が非選択状態のときに前段からの単位回路の出力信号を増幅して伝えるものであることを特徴とする半導体集積回路装置。

【請求項１４】

請求項１３において、

上記単位回路を構成するＭＯＳＦＥＴのゲート長及びゲート幅は、上記信号変化検出回路又は順序回路を含む他の論理回路を構成するＭＯＳＦＥＴのゲート長及びゲート幅より

も大きく形成されてなることを特徴とする半導体集積回路装置。
【請求項１５】
請求項１１において、
上記順序回路は、同じ単位回路を複数回連続して選択するテストモードを備え、
かかるテストモードにおいて、同じ単位回路から複数回出力される出力信号のうち異なる出力を形成する単位回路の数を計数する回路を設け、上記異なる出力信号を形成する単位回路の数が１以上であるときには乱数発生回路は良品として判定してなることを特徴とする半導体集積回路装置。
【請求項１６】
半導体基板上に複数の回路機能ブロックが配置された半導体集積回路装置であって、
上記半導体基板上には、さらに雑音検出対象回路と該雑音検出対象回路の出力信号が入力される増幅回路とを一組として含む単位回路の複数と、該複数の単位回路からの出力信号が入力される信号変化検出回路とが形成されており、
上記雑音検出対象回路のそれぞれは互いに同じ製造過程をもって同一の形態として形成された第１論理回路および第２論理回路を備えてなり、
上記半導体集積回路の動作状態において、
上記単位回路のそれぞれにおいて上記第１論理回路及び第２論理回路のしきい値電圧の差電圧に重畳される雑音を増幅して２値信号を生成し、
上記信号変化検出回路が上記複数の単位回路のそれぞれから出力される２値信号のうちの少なくとも１つの信号変化に応答して出力信号を生成する
動作を実行し、
生成された乱数が上記回路機能ブロックに供給されることを特徴とする半導体集積回路装置。
【請求項１７】
乱数を利用する電子装置であって、
上記電子装置には、雑音検出対象回路と該雑音検出対象回路の出力信号が入力される増幅回路とを一組として含む単位回路の複数と、上記複数の単位回路からの出力信号が入力される信号変化検出回路とが半導体基板上に配置された半導体チップまたは半導体集積回路装置が実装されており、
上記雑音検出対象回路のそれぞれは互いに同じ製造過程をもって同一の形態として形成された第１論理回路および第２論理回路を備えてなり、
動作状態において、
上記単位回路のそれぞれにおいて上記第１論理回路及び第２論理回路のしきい値電圧の差電圧に重畳される雑音を増幅して２値信号を生成し、
上記信号変化検出回路が上記複数の単位回路のそれぞれから出力される２値信号のうちのすくなくとも１つの信号変化に応答して出力信号を生成する
動作を実行し、
生成された乱数が電子装置の他の回路によって利用されることを特徴とする電子装置。
【請求項１８】
乱数を利用する電子装置における乱数発生方法であって、
上記電子装置には、雑音検出対象回路と該雑音検出対象回路の出力信号が入力される増幅回路とを一組として含む単位回路の複数と、上記複数の単位回路からの出力信号が入力される信号変化検出回路とが半導体基板上に配置された半導体チップまたは半導体集積回路装置が実装されており、
前記雑音検出対象回路のそれぞれは互いに同じ製造過程をもって同一の形態として形成された第１論理回路および第２論理回路を備えてなり、
上記複数の単位回路と上記信号変化検出回路とが動作状態にされたとき、
上記単位回路のそれぞれにおいて上記第１論理回路及び第２論理回路のしきい値電圧の差電圧に重畳される雑音を増幅して２値信号を生成する段階と、
上記信号変化検出回路が上記複数の単位回路のそれぞれから出力される２値信号のうち

の少なくとも１つの信号変化に応答して出力信号を生成する段階と、
が実行されることを特徴とする乱数発生方法。

【発明の詳細な説明】

【技術分野】

この発明は、乱数発生方法と半導体集積回路装置に関し、主として半導体製造技術に好適な乱数発生方法及びその半導体集積回路装置に利用して有効な技術に関するものである。

【背景技術】

近年のネットワーク化及びＩＴ化急速に拡大する社会において、暗号技術や認証技術等のセキュリティ技術の重要性が高まっている。それらの技術の重要な要素の一つとして乱数がしばしば用いられている。現在、数種類の基本原理に基づいた乱数発生回路が実用化されている。高度情報セキュリティ向け超小型真性乱数生成回路の例として、「東芝レビュー」Ｖｏｌ．５８・８（２００３）（第１の先行技術）がある。また、特開２００３－１７３２５４号公報（第２の先行技術）には、ＲＳフリップフロップの電源をオンオフすることにより得られる不確定出力を利用する乱数生成回路が記載されている。

【発明の開示】

乱数発生回路の性能を比較する要素は、乱数の品位（不規則性）、回路面積、消費電力及び応答時間（新しい乱数を生成するために要する時間）などであるが、従来の乱数発生回路はいずれも一長一短を持っている。乱数には、コンピュータのアルゴリズムなどで乱数を発生させる擬似乱数と、自然界の物理現象などを使って乱数を発生させる真性乱数の二つがある。一般的に、後者の方の品位が高いとされている。真性乱数は、偶然性、非再現性、予測不可能性の特長を持っているが複雑な回路や素子を必要とし、簡便な装置への適用に適していない。例えば、上記第１の先行技術において提案されている技術は、真性乱数発生回路であるが、プロセス（エッチング工程）の変更及びその制御が必要となるものである。また、上記第２の先行技術は電源投入時の過渡的状況下での現象を利用するため、乱数の不規則性を低下させる要因が設計段階では予測不能であり、乱数の品質を保証することが困難であると考えられる。

したがって、この発明の一つの目的は、製造プロセスの変更を行うことなく、小面積で高い品位の乱数を生成することができる乱数発生方法及び乱数発生回路を備えた半導体集積回路装置を提供することにある。この発明の他の目的は、低消費電力化を実現した乱数発生方法及びかかる乱数発生回路を備えた半導体集積回路装置を提供することにある。この発明の前記ならびにそのほかの目的と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。

本願において開示される発明のうち代表的なものの概要を簡単に説明すれば、下記の通りである。すなわち、互いに同じ製造過程をもって同一の形態として形成された第１及び第２論理回路と、上記第１論理回路及び第２論理回路のしきい値電圧の差電圧に重畳される雑音を増幅して２値信号を形成する増幅回路とからなる単位回路の複数個と、上記複数個の単位回路から出力される複数個からなる２値信号のうちのいずれか１つの信号変化に応答して出力信号を形成する信号変化検出回路とを備え、上記信号変化検出回路から出力される２値信号の複数個を組み合わせて乱数を生成する。

【図面の簡単な説明】

第１図は、この発明に係る半導体集積回路装置に搭載される真性乱数発生回路の基本概念を示す回路図であり、

第２図は、第１図の真性乱数発生回路を説明する動作原理図であり、

第３図は、この発明に係る真性乱数発生回路の一実施例を示す基本的回路図であり、

第４図は、第３図の真性乱数発生回路の一実施例を示す具体的回路図であり、

第５図は、第３図の真性乱数発生回路の動作の一例を説明するための波形図であり、

第６図は、第４図の真性乱数発生回路の信号変化検出回路の一実施例を示す具体的回路図であり、

第７図は、この発明に係る真性乱数発生回路の他の一実施例を示す回路図であり、

第８図は、第７図の真性乱数発生回路の動作の一例を説明するための概念的な波形図であり、
第９図は、この発明に係る真性乱数発生回路とその要素回路の一実施例を示す回路図であり、
第１０図は、この発明に係る真性乱数発生回路とその要素回路の他の一実施例を示す回路図であり、
第１１図は、第９図の真性乱数発生回路の動作の一例を説明するための概略波形図であり、
第１２図は、この発明に係る真性乱数発生回路の他の一実施例を示す概念図であり、
第１３図は、第１２図の初期値発生回路の一実施例を示す回路図であり、
第１４図は、第１２図の初期値発生回路の他の一実施例を示す回路図であり、
第１５図は、第１３図と第１４図の初期値発生回路の動作を説明するための波形図であり、
第１６図は、この発明に係る真性乱数発生回路の他の一実施例を示す回路図であり、
第１７図は、この発明に係る真性乱数発生回路の一実施例を示す回路図であり、
第１８図は、第１７図の真性乱数発生回路に設けられたテスト回路の動作の一例を説明するためのタイミング図であり、
第１９図は、この発明に係る真性乱数発生回路の一実施例を示す回路図であり、
第２０図は、第１９図の真性乱数発生回路の動作波形図であり、
第２１図は、この発明に係る真性乱数発生回路の一実施例を示す回路図であり、
第２２図は、この発明に係る真性乱数発生回路の出力部の他の一実施例を示す回路図であり、
第２３図は、第２１図に示した真性乱数発生回路の動作波形図であり、
第２４図は、この発明に係る真性乱数発生回路の一実施例を示すチップ構成図であり、
第２５図は、この発明に係る半導体集積回路装置の一実施例を示すブロック図であり、
第２６図は、この発明に係る半導体集積回路装置の他の一実施例を示すブロック図であり、
第２７図は、この発明に係る真性乱数発生回路の他の一実施例を示す構成図であり、
第２８図は、第２７図に示した真性乱数発生回路の動作の一例を示すタイミング図であり、
第２９図は、この発明が適用されるＩＣカードの一実施例を示す外観図であり、
第３０図は、この発明に係るＩＣカードに搭載されるＩＣカード用チップの一実施例を示す概略ブロック図であり、
第３１図は、この発明が適用される非接触ＩＣカードの一実施例を示すブロック図であり、
第３２図は、この発明に係る真性乱数発生回路で生成された真性乱数の２次元散布図であり、
第３３図は、第４図の真性乱数発生回路の変形例を示す具体的回路図であり、
第３４図は、第１図に示した真性乱数発生回路の基本概念の変形例を示す回路図であり、
第３５図は、第１図に示した真性乱数発生回路の基本概念のさらに別の変形例を示す回路図である。

【発明を実施するための最良の形態】

この発明をより詳細に説述するために、添付の図面に従ってこれを説明する。
第１図には、この発明に係る半導体集積回路装置に搭載される真性乱数発生回路の基本概念の回路図が示されている。第１図に示されたＣＭＯＳインバータ回路ＩＮＶ１～ＩＮＶ４は、半導体集積回路装置の設計及び製造の上では、現実的に制御可能な範囲内において、互いに同じ特性を持つように構成される。複数のインバータを互いに同じ特性にするため技術について、以下に概略的に説明する。
ＣＭＯＳインバータ回路において、その特性は、概略的には、それを構成するＰチャン

ネル型ＭＯＳＦＥＴとＮチャンネル型ＭＯＳＦＥＴとの相対的なコンダクタンスによって決まると理解されているであろう。その観点ではチャンネル幅Ｗとチャンネル長Ｌとの比Ｗ／Ｌは同じであるがサイズが異なるＭＯＳＦＥＴによっても同じ特性のＣＭＯＳインバータを構成できると理解され得る。しかしながら、半導体集積回路装置の製造バラツキによる電気特性への影響は、異なったサイズの素子に対しては異なったものとなる。

この実施例では、かかる複数のＣＭＯＳインバータＩＮＶ１～ＩＮＶ４のそれぞれは、好適には、それぞれを構成する素子の相互、すなわちＰチャンネル型ＭＯＳＦＥＴの相互、及びＮチャンネル型ＭＯＳＦＥＴの相互が互いに同じ構造、同じサイズを持って構成される。言うまでもなくそれら素子は、同じ素子は同じプロセスの下で一括製造されると言う半導体集積回路装置の特徴に従って製造される。これによって複数のＣＭＯＳインバータＩＮＶ１～ＩＮＶ４は、半導体集積回路装置の製造上の加工寸法のバラツキ、各種層の厚さバラツキ、不純物濃度バラツキ等々の製造バラツキによる影響を均等に受けるようにされる。

第１図のように入出力が短絡させられたＣＭＯＳインバータ回路ＩＮＶ１の出力電圧は、論理しきい値電圧に到達する。全てのＣＭＯＳインバータ回路が、完全に同じ電気的特性を持っていれば、４つのインバータ回路ＩＮＶ１～ＩＮＶ４の論理しきい値電圧は等しくなる。しかし、これは理想的な状態であり実際の半導体素子においては、僅かな特性の違いが存在するため、各インバータ回路ＩＮＶ１～ＩＮＶ４の論理しきい値電圧に差が生じる。

ＣＭＯＳインバータ回路の論理しきい値のバラツキの要因としては、ＭＯＳトランジスタ特性のバラツキが支配的であると捉えてよい。そして、ＭＯＳトランジスタ特性のバラツキの原因としては、ＭＯＳトランジスタのゲート幅や、ゲート絶縁膜膜厚、導電決定不純物濃度とその分布などを挙げることができる。これらのバラツキはマクロ的な部分とミクロ的とに分けることができる。マクロ的な部分としては、同一ロット内の複数のウェハ間のゲート幅バラツキなどである。

本願発明においては、主としてミクロ的な部分のバラツキを考慮するものであり、比較的に近接した位置に配置された素子間におけるバラツキについて検討した。このようなミクロ的なバラツキは、比較的に近接した素子間にランダムに発生するものとして観測される。

すなわち、第１図のインバータ回路ＩＮＶ１、ＩＮＶ２の論理しきい値のバラツキもランダムであると考えられる。この論理しきい値のバラツキは、後述するように真性乱数を発生させる上で好ましいことではない反面、別の観点では半導体素子の持つ特徴的な特性のバラツキが固有の識別情報として利用できる。つまり、ＣＭＯＳインバータ回路を用いた場合には、論理しきい値に生じるバラツキがＮチャンネル型ＭＯＳトランジスタの持つバラツキにＰチャンネル型ＭＯＳトランジスタの持つバラツキが加えられたものと見做すことができ、バラツキ範囲が広くなり識別番号ないし識別情報の発生を効果的に行うようにすることができる。しかし、このことは半導体素子の各ノードで発生する雑音に応答した真性乱数を発生させる上では好ましくないものとなる。

第１図に示した概念図では、４つのインバータ回路ＩＮＶ１～ＩＮＶ４を基本回路（又は単位回路）ＵＣ０として、ＣＭＯＳインバータ回路ＩＮＶ１の入力と出力とを短絡して、インバータ回路ＩＮＶ１の論理しきい値電圧ＶＬＴ１を形成する。この論理しきい値電圧ＶＬＴ１はインバータ回路ＩＮＶ２の入力に供給される。かかるインバータ回路ＩＮＶ２においては、そのしきい値電圧ＶＬＴ２を参照電圧として上記論理しきい値電圧ＶＬＴ１との電圧比較と増幅動作を行う。そして、かかるインバータ回路ＩＮＶ２の出力信号は、縦列接続されたインバータ回路ＩＮＶ３とＩＮＶ４からなる増幅回路により更に増幅されて２値信号に変換される。

理想的な条件においては、基本回路の第１のインバータ回路ＩＮＶ１の短絡された入出力ノードの電圧（論理しきい値電圧ＶＬＴ１）と第２のインバータ回路ＩＮＶ２の論理しきい値電圧ＶＬＴ２とは等しくなるように設計、製造されるが、実際には前記のようなプロセスバラツキが存在するため一致するとは限らない。

半導体内を電子が移動する際、不規則な動きをするため僅かであるが電気信号ノイズを発生させる。その現象は、第１のインバータ回路ＩＮＶ１にも第２のインバータ回路ＩＮＶ２にも発生するが、上記のようにＶＬＴ１＝ＶＬＴ２のような理想的な条件においては、第１のインバータ回路ＩＮＶ１の電気信号ノイズが第２のインバータ回路ＩＮＶ２により増幅され、第２のインバータ回路の出力信号は電気信号ノイズを反映して振幅する。電気信号ノイズは完全に無秩序な動きをするため、第２のインバータ回路ＩＮＶ２から得られる出力信号は真性乱数といえる。

つまり、第２図（ａ）に示すように、単位回路ＵＣ０の第１のインバータ回路ＩＮＶ１と第２のインバータ回路ＩＮＶ２の論理しき値電圧ＶＬＴ１，ＶＬＴ２とが一致している場合、電気信号ノイズＶｎｚが反転増幅されて出力信号Ｖｏｕｔとして取り出すことができる。なお、同図では第２のインバータ回路ＩＮＶ２の電気信号ノイズは省略し第１のインバータ回路ＩＮＶ１の電気信号ノイズＶｎｚに含めている。このようにして、第１のインバータ回路ＩＮＶ１の電気信号ノイズＶｎｚは第２のインバータ回路ＩＮＶ２により反転増幅される。さらに第２のインバータ回路ＩＮＶ２の出力信号Ｖｏｕｔは、第３および第４のインバータ回路ＩＮＶ３，ＩＮＶ４によりさらに増幅され、第４のインバータ回路ＩＮＶ４の出力では最終的に電源電圧レベルの振幅の論理レベルの情報が取り出せる。

しかし、電気信号ノイズＶｎｚは極めて小さく、また実際には各インバータ回路ＩＮＶ１、ＩＮＶ２を構成するＭＯＳトランジスタの特性は前記のような要因によってバラツキがあるため、基本回路ＵＣ０の第１および第２のインバータ回路ＩＮＶ１，ＩＮＶ２の論理しきい値電圧ＶＬＴ１，ＶＬＴ２は必ずしも等しいとはいえない。

つまり、第２図（ｂ）に示すように、単位回路ＵＣ０の第１のインバータ回路ＩＮＶ１と第２のインバータ回路ＩＮＶ２の論理しき値電圧ＶＬＴ１，ＶＬＴ２との間にΔＶのようなプロセスバラツキによる差電圧ΔＶが存在し、上記電気信号電圧ノイズＶｎｚの振幅より、上記第２のインバータ回路ＩＮＶ２の論理しきい値電圧ＶＬＴ２が常に大きい場合には、第２のインバータ回路ＩＮＶ２の出力信号Ｖｏｕｔは常にハイレベルとなってしまう。したがって、上記単位回路ＵＣ０を単独で見た場合には、第２のインバータ回路ＩＮＶ２の出力信号Ｖｏｕｔが上記の電気信号ノイズＶｎｚを反映すると常に保証されるものではない。

そこで、一般的には上記２つの論理しきい値電圧ＶＬＴ１，ＶＬＴ２の上記のようなプロセスバラツキを補正する方向にトリミングや補償回路を付加することが考えられるが、回路が複雑になったり、消費電流が増大するなどの問題を有するものとなる。

本願発明者においては、トランジスタの特性のバラツキはランダムな正規分布であることに着目し、第１図の示したように、数多くの基本回路を観察すれば、第１インバータ回路ＩＮＶ１と第２のインバータ回路ＩＮＶ２の特性が極めて等しい組み合わせがある確率で存在し、そのような基本回路は第２図（ａ）に示したように電気ノイズＶｎｚに敏感に反応するものとなることを見出した。

つまり、第２図（ｃ）のしきい値電圧分布図に示したように、インバータ回路ＩＮＶ１，ＩＮＶ２の論理しきい値電圧ＶＬＴ１，ＶＬＴ２は、正規分布となることが知られている。２つのインバータ回路ＩＮＶ１とＩＮＶ２を組み合わせると、その差ＶＬＴ１－ＶＬＴ２はもとの論理しきい値電圧ＶＬＴ１，ＶＬＴ２の分散の２倍の正規分布となる。電気信号ノイズ電圧Ｖｎｚの振幅より、第１のインバータ回路と第２のインバータ回路の論理しきい値電圧の差ＶＬＴ１－ＶＬＴ２が小さい基本回路が存在する確率は、インバータ回路の論理しきい値電圧ＶＬＴの分散と、電気信号ノイズ電圧の振幅Ｖｎｚで決まる。基本回路群中に含まれるノイズを電気信号のノイズを反映する基本回路の平均数は、基本回路群を構成する基本回路の数に、前記の確率を乗じた数である。

第１図において、ＵＣ０～ＵＣｎのような複数の基本回路の出力Ｄ０～Ｄｎを排他論理和回路に代表されるような信号変化検出回路ＥＸＯＲに入力すると、その出力Ｒは接続された基本回路ＵＣ０～ＵＣｎの出力信号Ｄ０～Ｄｎの変化のいずれにも反応して反転する。

上記複数の基本回路ＵＣ０～ＵＣｎの中に、第１インバータ回路と第２のインバータの

特性が極めて等しい組み合わせの基本回路が少なくとも１つ以上存在するように決められた複数からなる基本回路群の各出力を、信号変化検出回路ＥＸＯＲに入力する。すると、排他論理和回路のような信号変化検出回路ＥＸＯＲの出力Ｒは、基本回路ＵＣ０～ＵＣ１の出力Ｄ０～Ｄｎのうちのいずれか１つが変化すると反転する。すなわち、信号変化検出回路ＥＸＯＲの入力が基本回路の出力である場合、出力はかかる基本回路の電気ノイズを反映した真性乱数となる。基本回路群に、第１インバータ回路と第２のインバータ回路の特性が極めて等しい組み合わせの基本回路が複数存在しても、各基本回路どうしの電気信号ノイズに相関はないため、信号変化検出回路ＥＸＯＲの出力Ｒは同様に乱数であり、より品位の高い真性乱数を得ることができる。第１図に示した論理式Ｒ＝Ｄ０＊Ｄ１＊…＊Ｄｎにおいて、＊の記号は排他的論理和記号を表す。

図３には、この発明に係る乱数発生回路の一実施例の基本的回路図が示されている。この実施例では、前記図１のインバータ回路ＩＮＶ１～ＩＮＶ４が、２入力のナンド（ＮＡＮＤ）ゲート回路Ｇ１～Ｇ４に置き換えられる。上記ゲート回路Ｇ１は、一方の入力と出力とが結合される。このゲート回路Ｇ１の共通化された入出力がゲート回路Ｇ２の一方の入力と接続される。ゲート回路Ｇ２の出力はゲート回路Ｇ３の一方の入力に接続される。ゲート回路Ｇ３の出力はゲート回路Ｇ４の一方の入力に接続される。そして、これらのゲート回路Ｇ１～Ｇ４の他方の入力には、動作制御信号ＡＣＴが共通に供給される。

第１図のインバータ回路ＩＮＶ１～ＩＮＶ４は、上記ナンドゲート回路Ｇ１～Ｇ４のような論理ゲート回路の一種と見做すことができる。すなわち、入力信号を反転させる論理動作を行うものであるからである。第１図のようにインバータ回路ＩＮＶ１～ＩＮＶ４を用いた場合には、インバータ回路ＩＮＶ１とＩＮＶ２のように初段側においては論理しきい値電圧ＶＬＴ付近で動作するものであり、電源電圧ＶＤＤと回路の接地電位との間に直流電流を流すものとなる。本願発明では、前記のように素子のプロセスバラツキによる論理しきい値電圧の正規分布を利用するものであり、そのために比較的多数からなる単位回路を動作させる必要があるので、上記インバータ回路ＩＮＶ１とＩＮＶ２での直流電流は低消費電力化を実現する上では無視できない。

これに対して、この実施例のようにゲート回路Ｇ１～Ｇ４を用いた場合には、各ゲート回路Ｇ１～Ｇ４は、動作制御信号ＡＣＴをロウレベル（論理０）のような非活性化レベルとしたとき、上記動作制御信号ＡＣＴとは異なる他方の入力信号に無関係に出力信号をハイレベル（論理１）にし、各ゲート回路Ｇ１，Ｇ２においても直流電流が発生しない。すなわち、この実施例回路では、乱数を必要とするタイミングで上記動作制御信号ＡＣＴをハイレベル（論理１）のような活性化レベルとする。これにより、各ゲート回路Ｇ１～Ｇ４は、上記動作制御信号ＡＣＴとは異なる他方の入力信号に応答して反転信号を形成するというインバータ回路としての動作を行う。これにより、上記動作制御信号ＡＣＴをハイレベルにすることにより、第１図の基本回路図と同様の動作を行うものとなる。

第４図には、第３図の真性乱数発生回路の一実施例の具体的回路図が示されている。ゲート回路Ｇ１は、出力ノードＮ１と回路の接地電位ＶＳＳとの間に直列形態にされたＮチャネルＭＯＳＦＥＴＱ１とＱ３、上記出力ノードＮ１と電源電圧ＶＤＤとの間に並列形態にされたＰチャネルＭＯＳＦＥＴＱ２とＱ４から構成される。上記ＭＯＳＦＥＴＱ１とＱ３のゲートが共通に接続されて第１の入力とされる。上記ＭＯＳＦＥＴＱ２とＱ４のゲートが共通に接続されて第２の入力とされる。他のゲート回路Ｇ２～Ｇ４も上記と同様な回路により構成される。

上記ゲート回路Ｇ１～Ｇ４は、半導体集積回路装置の設計及び製造の上では、現実的に制御可能な範囲内において、互いに同じ特性を持つように構成される。複数のゲート回路を互いに同じ特性とする技術について、以下に概略的に説明する。ゲート回路Ｇ１～Ｇ４において、その特性である論理しきい値は、概略的には、それを構成するＰチャネルＭＯＳＦＥＴとＮチャネルＭＯＳＦＥＴとに決まると理解されているであろう。その観点ではチャネル幅Ｗとチャネル長Ｌとの比Ｗ／Ｌは同じであるがサイズが異なるＭＯＳＦＥＴによっても同じ特性のＣＭＯＳゲート回路を構成できると理解され得る。しかしながら、半導体集積回路装置の製造バラツキによる電気特性への影響は、異なったサイズの素子に対

しては異なったものとなる。

この実施例では、かかる複数のゲート回路Ｇ１～Ｇ４のそれぞれは、好適には、それぞれを構成する素子の相互、すなわちＰチャネル型ＭＯＳＦＥＴの相互、及びＮチャネル型ＭＯＳＦＥＴの相互が互いに同じ構造、同じサイズを持って構成される。言うまでもなくそれら素子は、同じ素子は同じプロセスの元で一括製造されると言う半導体集積回路装置の特徴に従って製造される。これによって複数のゲート回路Ｇ１～Ｇ４は、半導体集積回路装置の製造上の加工寸法のバラツキ、各種層の厚さバラツキ、不純物濃度バラツキ等々の製造バラツキによる影響を均等に受けるようにされ、かつ、論理しきい値電圧も正規分布を持つようにされる。

第３図に示した実施例では、２つのゲート回路Ｇ１とＧ２の論理しきい値の大きさの判定出力がゲート回路Ｇ２から出力される。かかる信号伝達及び増幅経路に前記のような電気信号ノイズが重畳することにより、かかる電気信号ノイズに反映した出力信号を得る。つまり、ゲート回路Ｇ１の短絡された入出力ノードの電圧（論理しきい値に相当する）をゲート回路Ｇ２の入力バイアスとして供給し、上記電気信号ノイズに反映した出力信号を後段のゲート回路Ｇ３、Ｇ４により増幅してＣＭＯＳレベルの２値信号を得るものである。したがって、厳密にはゲート回路Ｇ３とＧ４は、単に増幅動作を行うものであるからゲート回路Ｇ１とＧ２のようにＰチャネル型ＭＯＳＦＥＴの相互、及びＮチャネル型ＭＯＳＦＥＴの相互が互いに同じ構造、同じサイズを持って構成される必要は無いが、この実施例では主に回路設計の観点から同じ構造、同じサイズを持って構成される。

第５図には、上記第３図の真性乱数発生回路の動作の一例を説明するための波形図が示されている。同図では、信号伝達経路での電気信号ノイズは省略されている。動作制御信号ＡＣＴをロウレベルからハイレベルに変化させると、上記各ゲート回路Ｇ１～Ｇ４が実質的に動作状態となり、ゲート回路Ｇ１の出力ノードＮ１がその論理しきい値に対応した電圧にされる。なお、これに必要な時間を収束時間と呼ぶことにする。ゲート回路Ｇ２は、その論理しきい値によってノードＮ１の電圧を判定し、その出力ノードＮ２の電位を決める。この例では、ゲート回路Ｇ１の論理しきい値が、ゲート回路Ｇ２の論理しきい値によりも僅かに大きいので、ゲート回路Ｇ２での増幅動作によってノードＮ２の電位が上記ノードＮ１に対して小さい電圧にされる。このノードＮ２の電圧は、ゲート回路Ｇ３により増幅されてノードＮ３のようにハイレベルに大きくされる。そして、ゲート回路Ｇ４により更に増幅されてノードＮ４のように回路の接地電位ＶＳＳに到達する。

上記ノードＮ１とＮ２の電位差が僅かであり、そこに発生する電気信号ノイズがノードＮ２の電位以下になると、出力信号は反転するものとなる。つまり、前記第２図（ａ）と同様にノードＮ１とＮ２の電位差を反転させるような電気信号ノイズが発生した場合、逆にいうなら電気信号ノイズによりノードＮ１とＮ２の電位差関係が逆転してしまうような僅かの電圧差しかないゲート回路Ｇ１とＧ２の組み合わせを持つ基本回路では、出力はかかる基本回路の電気ノイズを反映した真性乱数を発生させることができる。当然のことであるが、上記の真性乱数を発生させることができるのは、収束時間を経過して後であることは言うまでもない。収束時間中であれば、各ナンドゲートのノードの過渡的な状態の影響を受け、本来の微小な電気ノイズを反映した真性乱数を得ることは難しい。

この実施例では、回路が停止状態すなわち動作制御信号ＡＣＴがロウレベルであるとき、第３図のＮチャネルＭＯＳＦＥＴＱ３、Ｑ７、Ｑ１１、Ｑ１５がオフ状態となり、前記のＣＭＯＳインバータ回路を用いた場合のような貫通電流が抑制される。また、ゲート回路としてナンド（ＮＡＮＤ）回路を用いた利点は、ＣＭＯＳ論理ＬＳＩの標準素子であるため、適用する製品を限定しないことである。つまり、完全論理記述型回路で構成されるため、回路設計が容易になるものである。

第４図の実施例では、動作制御信号ＡＣＴが直列のＮチャネルＭＯＳＦＥＴのＱ３、Ｑ７、Ｑ１１、Ｑ１５のゲートに接続されているが、ＮチャネルＭＯＳＦＥＴＱ１、Ｑ５、Ｑ９、Ｑ１３に接続されて、ノードＮ１、Ｎ２、Ｎ３はＮチャネルＭＯＳＦＥＴのＱ３、Ｑ７、Ｑ１１、Ｑ１５のゲートに接続されてもよい。

トランジスタレベル回路記述において重要なのは、個々のＮＡＮＤ素子中のＭＯＳＦＥ

Ｔの信号接続位置である。上記の停止状態では各ゲート回路Ｇ１～Ｇ４の出力すなわちノードＮ１、Ｎ２、Ｎ３の電位が自動的に電源電圧となるため、それら信号の接続先のＰチャネルＭＯＳＦＥＴのＮＢＴＩによる特性の変動を防止できる効果がある。

ＭＯＳトランジスタは、そのしきい値電圧が電界強度と温度とに依存するような電界ストレスによって不所望に変動することが有る。特にＮＢＴＩ（Ｎｅｇａｔｉｖｅ Ｂｉａｓ Ｔｅｍｐｅｒａｔｕｒｅ Ｉｎｓｔａｂｉｌｉｔｙ）と称される現象は、Ｐチャネル型ＭＯＳＦＥＴで顕著に現われる現象である。この防御策として、目的外の時間においてＰＭＯＳのゲートに印加される電圧を高い電圧にする方法がよく用いられる。この実施例では、上記動作制御信号ＡＣＴのハイレベルにより論理しきい値判定動作を行わせ、かかる論理しきい値判定動作以外の時には、動作制御信号ＡＣＴをロウレベルにしてＰチャネル型ＭＯＳＦＥＴのゲートには、電源電圧を供給するようにゲート電圧を固定電圧にするものである。これにより、Ｐチャネル型ＭＯＳＦＥＴは、ゲート、ドレイン及びソースと基板（チャネル）の全てが電源電圧に等しい同電位となり、上記ＭＯＳＦＥＴの経時変化による論理しきい値の変動が極力抑えられる。このことは、前記のように各単位回路の出力信号を組み合わせによって識別情報を得る上で特に有効なものとなる。

これに対して、乱数発生回路においては、上記のような素子特性の変動、あるいは電源電圧の変動等には基本的には影響されないという特徴を有している。この実施例の乱数発生回路では、前記説明したように比較的多数の単位回路の中で少なくとも１個、ゲート回路Ｇ１とＧ２の論理しきい値電圧が前記電気信号ノイズからみて等しいものと見做されるものが存在すればよい。上記素子特性の変動、あるいは電源電圧の変動等には上記多数からなる単位回路群の全てにおいて発生し、それによりある単位回路ではゲート回路Ｇ１とＧ２の論理しきい値電圧が前記電気信号ノイズからみて等しいものと見做されていたものが外れても、別の単位回路では逆にゲート回路Ｇ１とＧ２の論理しきい値電圧が前記電気信号ノイズからみて等しいものと見做されることになるからである。

第３３図には、第４図の真性乱数発生回路の変形例が示されている。第３３図（ａ）のナンドゲート回路Ｇ１とＧ２（前記第１図のインバータ回路ＩＮＶ１とＩＮＶ２に相当）の電気的特性バラツキを抑えるため、ＮＡＮＤを構成するトランジスタのチャネル長Ｌおよびチャネル幅Ｗをいずれも標準サイズ（通常プロセスの最小寸法）よりも大きくする。かかるトランジスタのＬおよびＷを大きくすることで、トランジスタのゲート電極の加工誤差に起因する特性のバラツキを抑えることができる。また、ＭＯＳトランジスタのゲート電極直下の不純物濃度の統計的変動に起因するバラツキ（これを、「ゆらぎ現象」という。）を抑えることができる。近年の先端プロセスでは、同一チップ上のＭＯＳトランジスタの電気的特性バラツキは、加工誤差よりのゆらぎ現象の影響が支配的であることが知られている。

ナンドゲート回路Ｇ１とＧ２を構成する各トランジスタ大きさは共通である必要はないが、回路動作時の状態に関わる、言い換えるならば上記活性状態での論理しきい値の決定に影響を及ぼすＰチャネルＭＯＳＦＥＴＱ２（Ｑ６）とＮチャネルＭＯＳＦＥＴＱ１，Ｑ３（Ｑ５，Ｑ７）を優先して大きくする。各ナンドゲート回路Ｇ１とＧ２の対応するＭＯＳＦＥＴは同じ形状である必要がある。

また、増幅回路として動作するゲート回路Ｇ３及びＧ４は、上記のように設定することは必要ないが、回路設計上あるいは素子レイアウト上はゲート回路Ｇ１とＧ２と同様のものを用いるのが簡単となるし、後述するような乱数発生回路の存在を隠す上で有利なものとなる。

第３３図（ｂ）には、第３３図（ａ）と同様の効果が得られる別の実現方法の回路が示されている。すなわち、３入力ＮＡＮＤゲートを用いて、活性状態での論理しきい値の決定に影響を及ぼすＰチャネルＭＯＳＦＥＴとＮチャネルＭＯＳＦＥＴを各２個ずつとし、上記ゆらぎ現象の影響を抑えるものである。これは、特殊なサイズのＭＯＳトランジスタを特別に設計することなしに標準的なサイズのゲート部品で実現できるという利点がある。

なお、前記第３図、第４図及び第３３図はいずれもナンド（ＮＡＮＤ）ゲートを用いて

基本回路を構成したが、ナンドの代わりにノア（ＮＯＲ）ゲートであっても構わない。ただし、その場合にはかかる基本回路は、動作制御信号ＡＣＴがロウレベル（論理０）で活性化するものとなる。前記のように、ＮＢＴＩと称される電界ストレスに起因する劣化現象は特にＰチャネルＭＯＳＦＥＴで顕著である。しかし他の素子、例えばポリシリコンＦＥＴや有機トランジスタ等において、かかる劣化現象がＰチャネル型ではなくＮチャネル型で顕著である場合は、ノア（ＮＯＥ）ゲートを用いることが望ましい。

なお、第３図に示される実施例において、各単位回路ＵＣ０～ＵＣｎ内のナンドゲートＧ２，Ｇ３，Ｇ４については、それぞれに接続された共通制御信号ＡＣＴを電源ＶＤＤに接続して常にハイレベル（論理１）としてもよく、それによって本実施例の持つ基本的機能は変らない。

第６図には、第３図の真性乱数発生回路の信号変化検出回路ＥＸＯＲの一実施例の具体的回路図が示されている。この実施例では、排他的論理和回路ＥＸ０～ＥＸｎが縦列接続されて上記信号変化検出回路ＥＸＯＲが構成される。単位回路ＵＣ０の出力信号Ｄ０を受ける排他的論理和回路ＥＸ０の他方の入力には、特に制限されないが、ロウレベル（論理０）のような固定値が与えられる。次段の単位回路ＵＣ１の出力信号Ｄ０を受ける排他的論理和回路ＥＸ１の他方の入力には、上記排他的論理和回路ＥＸ０の出力信号が供給される。以下、ｎ＋１番目の単位回路ＵＣｎの出力信号Ｄｎを受ける排他的論理和回路ＥＸｎの他方の入力には、図示しないが１つ前の排他的論理和回路ＥＸｎ－１の出力信号が供給される。

これにより、排他的論理和回路ＥＸｎの出力信号Ｒは、上記ｎ＋１個の単位回路ＵＣ０～ＵＣｎの出力信号Ｄ０～Ｄｎの中のいずれか１つでも変化すると、それに対応してそれに対応した排他的論理和回路ＥＸの出力信号が変化し、上記直列形態にされた排他的論理和回路によって出力信号Ｒが変化するものとなる。つまり、上記出力信号Ｒは、単位回路（基本回路）の電気ノイズを反映した真性乱数となる。

上記信号変化検出回路ＥＸＯＲとしては、論理ゲート回路で構成する場合には上記のような複数個の排他的論理和回路を用いるものが便利であるが、それに限定されず、出力信号Ｄ０～Ｄｎの論理レベルの変化を検出するものであれば何であってもよい。例えば、出力信号Ｄ０～Ｄｎと、その遅延信号により１シッョトパルスを形成するもの等種々の実施形態を採ることができる。

第７図には、この発明に係る真性乱数発生回路の他の一実施例の回路図が示されている。この実施例では、単位回路ＵＣ０～ＵＣｎがデコーダＤＥＣを用いて時間的に分散して動作させられる。そして、１つの排他論理和回路ＥＸと、１つのフリップフロップ回路ＦＦとを用いて、複数の単位回路ＵＣ０～ＵＣｎの出力の排他論理を累算することにより真性乱数ＲＲを得るものである。なお、排他論理和を複雑な論理に変更することで、発生パターンをより解読され難い真性乱数を得ることができる。

上記デコーダＤＥＣは、特に制限されないが、カウンタとデコーダにより構成される。つまり、クロックＣＬＫをカウンタで計数して、その計数出力をデコードして単位回路ＵＣ０～ＵＣｎを順次動作状態にする動作制御信号ＤＥＣ０～ＤＥＣｎを生成するものである。あるいは、シフトレジスタを用い、選択信号に対応した初期値をクロックＣＬＫにより順次にシフトして単位回路ＵＣ０～ＵＣｎを順次に動作状態にする動作制御信号ＤＥＣ０～ＤＥＣｎを形成するようにされる。

このように単位回路ＵＣ０～ＵＣｎを順次に動作状態にするために、単位回路ＵＣ０を例にして説明すると、ゲート回路Ｇ１とＧ２に対して動作制御信号としてのデコード出力ＤＥＣ０が供給される。増幅回路としてのゲート回路Ｇ３とＧ４は、上記ゲート回路Ｇ１とＧ２が動作制御信号ＤＥＣ０により動作状態とされたときには、それに対応した出力信号の増幅動作を行い、上記ゲート回路Ｇ１とＧ２が動作制御信号ＤＥＣ０により非動作状態とされたときには、前段の単位回路の出力信号をスルして伝達する動作を行う。

ゲート回路Ｇ３の一方の入力には、それに対応したゲート回路Ｇ２の出力信号が伝えられ、他方の入力には前段の単位回路の出力信号が伝えられる。ゲート回路Ｇ４は、一方の入力にはそれに対応したゲート回路Ｇ３の出力信号が供給され、他方の入力には電源電圧

に対応されたハイレベルが固定的に供給される。これにより、ゲート回路Ｇ４は実質的にはインバータ回路として動作する。初段の単位回路ＵＣ０のゲート回路Ｇ３の他方の入力には、電源電圧に対応されたハイレベルが固定的に供給される。

第８図には、第７図の真性乱数発生回路の動作の一例を説明するための概念的な波形図が示されている。デコーダＤＥＣにより、初段の単位回路ＵＣ０に対応した動作制御信号ＤＥＣ０がハイレベルの選択レベルにされると、ゲート回路Ｇ１とＧ２による出力信号が形成されてゲート回路Ｇ３，Ｇ４により増幅されて出力信号Ｄ０が形成される。単位回路ＵＣ１～ＵＣｎにおいては、上記動作制御信号ＤＥＣ１～ＤＥＣｎがロウレベルの非選択レベルであるので、ゲート回路Ｇ２に相当するゲート回路の出力信号は全てハイレベルにされる。それ故、ゲート回路Ｇ３に相当するゲート回路はインバータ回路としての動作を行い、前段回路からの出力信号を増幅するのみとなる。この結果、上記初段の単位回路ＵＣ０の出力信号Ｄ０は、上記単位回路ＵＣ１～ＵＣｎのゲート回路を通して排他的論理和回路ＥＸに伝えられる。つまり、Ｄ１～Ｄｎは、Ｄ０に従ったレベルにされる。

デコーダＤＥＣにより、第２番目の単位回路ＵＣ１に対応した動作制御信号ＤＥＣ１がハイレベルの選択レベルにされると、上記同様にゲート回路Ｇ１とＧ２に対応した２つのゲート回路による出力信号が形成されてゲート回路Ｇ３，Ｇ４に対応したゲート回路により増幅されて出力信号Ｄ１が形成される。つまり、上記初段の単位回路では、選択信号ＤＥＣ０のロウレベルによりゲート回路Ｇ２の出力信号がハイレベルとなり、出力信号Ｄ０をハイレベルに固定する。したがって、上記のようにの単位回路ＵＣ１においては、上記のようにゲート回路Ｇ３，Ｇ４に対応したゲート回路による増幅動作が行われる。以下、その出力信号Ｄ１は、前記同様に後段側の単位回路における増幅回路としてのゲート回路を通して排他的論理和回路ＥＸに伝えられる。つまり、Ｄ２～Ｄｎは、Ｄ１に従ったレベルにされる。第３番目以降の単位回路ＵＣ２～ＵＣｎの選択動作も前記同様である。

第７図の実施例回路の実際の波形は、第８図とは異なる。つまり、単位回路ＵＣ０において非選択状態のときには、出力信号Ｄ０がハイレベルにされる。つまり、上記ＤＥＣ１が非選択レベルになると同時に出力信号Ｄ０は非選択状態に対応したハイレベルの出力信号を形成するものとなる。このことは、単位回路ＵＣ１～ＵＣｎが非選択レベルにされたときに、各出力信号Ｄ１～Ｄｎも一斉にハイレベルにされる。このような非選択状態に対応して出力信号Ｄ０～Ｄｎのレベルを忠実に表現すると、上記単位回路ＵＣ０～ＵＣｎが順序動作し、その出力が順次（シリアル）に出力されることが解り難くなるので、単位回路ＵＣ０～ＵＣｎにおける非選択状態での出力レベルの変化を無視して第８図のように表すものである。

第７図の実施例回路において、（ｎ＋１）個の単位回路（基本回路）を含む単位回路群が例示されており、（ｎ＋１）個の基本回路の中に、第１ゲート回路Ｇ１（第１インバータ回路ＩＮＶ１）と第２ゲート回路Ｇ２（第２のインバータ回路ＩＮＶ２）の特性が極めて等しい組み合わせの単位回路が少なくとも１つ以上存在する。前述のように、単位回路群中に含まれる第１ゲート回路Ｇ１と第２ゲート回路Ｇ２の特性が極めて等しい組み合わせの単位回路の数が多いほど、得られる乱数の品位は高くなる。単位回路群に含まれる第１ゲート回路Ｇ１と第２ゲート回路Ｇ２の特性が極めて等しい組み合わせの単位回路の数を十分な数にするためには、第１ゲート回路Ｇ１と第２ゲート回路Ｇ２の特性が極めて等しい組み合わせの単位回路が存在する確率を上げ、単位回路群に含まれる単位回路数を、かかる確率に見合う適正な数にすることが必要である。第１ゲート回路Ｇ１と第２ゲート回路Ｇ２の特性が極めて等しい組み合わせの単位回路が存在する確率は、当該回路の製造プロセスと設計手法等に依存する要素が高い（出来高次第）ため、単位回路群に含まれる単位回路数の最適化が重要である。

また、乱数の品位を向上させる別の手段として、排他論理和回路ＥＸとフリップフロップ回路ＦＦを用いた累算の回数を増やすことも有効である。具体的には、第８図例示された動作波形において、（ｎ＋１）個の単位回路の累算を、例えば（ｎ＋１）×ｍとｍ倍に延長する。つまり、単位回路ＵＣ０～ＵＣｎの前出力Ｄ０～Ｄｎをｍ回にわたって読み出して１ビットの乱数Ｒ（ＲＲ）を決定するものである。

第９図には、この発明に係る真性乱数発生回路とその要素回路の一実施例の回路図が示されている。第９図（ａ）に示される真性乱数発生回路では、第９図（ｂ）に示されるような単位回路（要素回路）がＭ×Ｎ個のようにマトリックス配置される。

１つの行が前記第７図の回路のように接続され、その出力部に行選択信号により選択されるナンドゲート回路Ｇ０とクロックドインバータ回路ＣＮ０が設けられる。Ｍ個からなる各行を構成する単位回路は、対応するもの同士が列デコーダにより形成された列選択信号Ｃ０～ＣＭ－１により共通に選択される。上記Ｎ個の行方向に配置された単位回路は、行デコーダにより形成された行選択信号Ｒ０～ＲＮ－１により１つが選択される。かかる行選択信号Ｒ０～ＲＮ－１は、上記ナンドゲート回路Ｇ０とクロックドインバータ回路ＣＮ０からなる行選択回路の選択信号としても用いられる。選択回路を構成するクロックドインバータ回路ＣＮ０は、それが非動作状態のときに出力ハイインピーダンス状態になるので、上記Ｎ個のクロックドインバータ回路の出力信号が共通に接続され、選択された１つの行に対応したクロックドインバータ回路の出力号がナンドゲート回路Ｇ１１に伝達される。

動作制御信号ＡＣＴによりゲートが制御されるナンドゲート回路Ｇ１０とインバータ回路ＩＮＶ１０を通してクロックＣＬＫがＭ進カウンタに供給される。これにより、Ｍ進カウンタでは動作制御信号ＡＣＴが活性状態のときにクロックＣＬＫに対応して０～Ｍ－１の計数動作を行い、列デコーダによりＣ０～ＣＭ－１の選択信号が形成されて単位回路の出力信号が第７図の実施例と同様にシリアルに出力される。

上記Ｍ進カウンタのキャリー信号がＮ進カウンタに供給されるので、Ｎ進カウンタはＭ進カウンタの１回りに対応して計数動作を行う。これにより、上記行方向に配置されたＭ個の単位回路の読み出しが行われると、行選択の切替が行われて０行目からＲＮ－１行目まで、それぞれＮ個の単位回路の読み出しが実施される。

本実施例において、Ｍ×Ｎサイクルで全ての単位回路の読み出しが行われるから、Ｍ×Ｎサイクルにより出力ＲＲから１ビットの真性乱数を生成することができる。これをＫ回繰り返すことによりＫビットの真性乱数を得ることができる。この構成では、Ｍ×Ｎ個の単位回路の中に少なくとも１つだけ前記のような電気信号ノイズに応答する単位回路が存在するようにＭ×Ｎの数を選ぶものである。なお、上記Ｋ回の繰り返しの間にＪ個（０＜Ｊ＜Ｋの整数）の乱数を取り出してもよい。ただしその場合は、各乱数ビットの取り出しサイクルはＭ×Ｎサイクル以上離れていなければならない。また、上記Ｍ個からなる単位回路の中に、前記真性乱数を発生させるものが少なくとも１つ存在するようにＭの数を選ぶものとすると、Ｍサイクル毎（各行毎）に１ビットの真性乱数ＲＲを取得することができるので、Ｍ×ＮサイクルによりＮビットの真性乱数を発生させる真性乱数発生回路を構成することができる。

第９図（ｂ）には、前記第９図（ａ）における回路要素の一実施例の具体的回路図が示されている。単位回路は、前記第７図に示したゲート回路Ｇ１～Ｇ４に、行／列選択機能を設けるためのゲート回路Ｇ５とＧ６が追加される。ナンドゲート回路Ｇ５の２つの入力には、列選択信号Ｃｉと、行選択信号Ｒｉが供給される。ゲート回路Ｇ３には、前記第７図の単位回路と同様にその行における１段前の単位回路の出力信号Ｄｉが供給される。これにより、行及び列が選択状態にされた１つの単位回路のみが前記のような動作状態にされる。

第９図（ｃ）には、前記第９図（ｂ）における回路要素の他の一実施例の具体的回路図が示されている。単位回路は、第９図（ｂ）および前記第７図に示したゲート回路Ｇ１～Ｇ４を３入力ナンドゲートにして、行／列選択機能を合わせ持たせている。ナンドゲート回路Ｇ５およびＧ６の３つの入力のうち２つの入力には、列選択信号Ｃｉと、行選択信号Ｒｉが供給される。ゲート回路Ｇ７には、第９図（ｂ）および前記第７図の単位回路と同様にその行における１段前の単位回路の出力信号Ｄｉが供給される。これにより、行及び列が選択状態にされた１つの単位回路のみが前記のような動作状態にされる。

第９図（ａ）におけるクロックドインバータ回路ＣＮは、第９図（ｄ）に示すように、電源電圧ＶＤＤと回路の接地電位ＶＳＳとの間に直列接続されたＰチャネルＭＯＳＦＥＴ

Ｑ１、Ｑ２とＮチャネルＭＯＳＦＥＴＱ４、Ｑ３から構成される。ＰチャネルＭＯＳＰＥＴＱ１とＮチャネルＭＯＳＦＥＴＱ３のゲートが共通に接続されて入力端子Ａとされる。ＰチャネルＭＯＳＦＥＴＱ２とＮチャネルＭＯＳＦＥＴＱ４のドレインが共通に接続されて出力端子Ｂとされる。そして、端子Ｃから供給される制御信号は、ＮチャネルＭＯＳＦＥＴＱ４のゲートに供給され、上記制御信号がインバータ回路ＩＮＶ１２によって反転されてＰチャネルＭＯＳＦＥＴＱ２のゲートに供給される。

端子Ｃから供給される行選択信号のような選択信号がハイレベルのときにＮチャネルＭＯＳＦＥＴＱ４とＰチャネルＭＯＳＦＥＴＱ２がオン状態となり、入力端子Ａからの入力信号を受けるＮチャネルＭＯＳＦＥＴＱ３とＰチャネルＭＯＳＦＥＴＱ１のオン／オフに対応した出力信号が出力端子Ｂから出力される。端子Ｃから供給される行選択信号のような選択信号がハイレベルのときにＮチャネルＭＯＳＦＥＴＱ４とＰチャネルＭＯＳＦＥＴＱ２が同時にオン状態となり、入力端子Ａからの入力信号によりＮチャネルＭＯＳＦＥＴＱ３又はＰチャネルＭＯＳＦＥＴＱ１が相補的にオン状態となり、ロウレベル又はハイレベルが出力端子Ｂから出力される。

また、第９図（ａ）におけるクロックドインバータ回路ＣＮは、第９図（ｅ）に示されるようなトランスファゲート回路であってもよい。クロックドインバータ回路ＣＮは、第９図（ｅ）に示すように、入力端子Ａと出力端子Ｂとの間に直列接続されたＰチャネルＭＯＳＦＥＴＱ５と、ＮチャネルＭＯＳＦＥＴＱ６から構成される。端子Ｃから供給される制御信号は、ＮチャネルＭＯＳＦＥＴＱ６のゲートに供給され、上記制御信号がインバータ回路ＩＮＶ１４によって反転されてＰチャネルＭＯＳＦＥＴＱ５のゲートに供給される。端子Ｃから供給される行選択信号のような選択信号がハイレベルのときにＰチャネルＭＯＳＦＥＴＱ５とＮチャネルＭＯＳＦＥＴＱ６がオン状態となり、入力端子Ａからの入力信号が出力端子Ｂから出力される。端子Ｃから供給される行選択信号のような選択信号がハイレベルのときにＮチャネルＭＯＳＦＥＴＱ４とＰチャネルＭＯＳＦＥＴＱ２が同時にオン状態となり、入力端子Ａからの入力信号によりＮチャネルＭＯＳＦＥＴＱ３又はＰチャネルＭＯＳＦＥＴＱ１が相補的にオン状態となり、ロウレベル又はハイレベルが出力端子Ｂから出力される。また、端子Ｃから供給される行選択信号のような選択信号がロウレベルのときにＮチャネルＭＯＳＦＥＴＱ４とＰチャネルＭＯＳＦＥＴＱ２が同時にオフ状態となり、出力端子Ｂはハイインピーダンスとなる。

第１０図には、この発明に係る真性乱数発生回路とその要素回路の他の一実施例の回路図が示されている。第１０図（ａ）に示される真性乱数発生回路では、第１０図（ｂ）に示される単位回路がＭ（列）×Ｎ（行）個のようにマトリックス配置される。１つの行が前記第７図の回路のように接続され、その出力部にナンドゲート回路Ｇ０と排他的論理和回路ＥＸ０が設けられる。ナンドゲート回路Ｇ０の他方の入力は電源ＶＤＤが接続され常にハイレベル（論理１）状態である。Ｍ個からなる各行を構成する単位回路は、対応するもの同士が列デコーダにより形成された列選択信号Ｃ０～ＣＭ－１により共通に選択される。

動作制御信号ＡＣＴによりゲートが制御されるナンドゲート回路Ｇ１０とインバータ回路ＩＮＶ１０を通してクロックＣＬＫがＭ進カウンタに供給される。これにより、Ｍ進カウンタでは動作制御信号ＡＣＴが活性状態のときにクロックＣＬＫに対応して０～Ｍ－１の計数動作を行い、列デコーダによりＣ０～ＣＭ－１の選択信号が形成されて、Ｎ行で構成されるＣｉを共通とする各行の単位回路の出力信号が第７図の実施例と同様にシリアルに出力される。

ナンドゲート回路Ｇ０の出力は、排他的論理和回路ＥＸ０に接続され、ＥＸ０の他方の入力はに接続される。さらに排他的論理和回路ＥＸ０の出力は、となりの行の排他的論理和回路へ接続され、全ての行の排他的論理和回路の出力は順次となりの行へ縦列接続される。排他的論理和回路ＥＸ０の他方の入力には、特に制限されないが、ハイレベル（論理１）のような固定値が与えられる。これにより、縦列接続された排他的論理和回路の出力信号ＲＡは、上記選択されたＣｉを共通とするＮ行の単位回路から生成されるＮ個の出力信号の中のいずれか１つでも変化すると、それに対応して各行のた排他的論理和回路の各

出力信号が変化し、上記縦列形態にされた排他的論理和回路によって出力信号ＲＡが変化するものとなる。つまり、上記出力信号ＲＡは、１サイクルの動作でＮ個の単位回路（基本回路）の電気ノイズを反映した値となる。

本実施例において、Ｍサイクルで全ての単位回路の読み出しが行われるから、Ｍサイクルにより出力ＲＲから１ビットの真性乱数を生成することができる。これをＫ回繰り返すことによりＫビットの真性乱数を得ることができる。この構成では、Ｍ×Ｎ個の単位回路の中に少なくとも１つだけ前記のような電気信号ノイズに応答する単位回路が存在するようにＭ×Ｎの数を選ぶものである。なお、上記Ｋ回の繰り返しの間にＪ個（０＜Ｊ＜Ｋの整数）の乱数を取り出してもよい。ただしその場合は、各乱数ビットの取り出しサイクルはＭサイクル以上離れていなければならない。

第１０図（ｂ）には、前記第１０図（ａ）の真性乱数発生回路における回路要素の一実施例の具体的回路図が示されている。ナンドゲート回路Ｇ１とＧ２の２つの入力の一方には、列選択信号Ｃｉが供給される。ゲート回路Ｇ３には、前記第７図の単位回路と同様にその行における１段前の単位回路の出力信号Ｄｉが供給される。これにより、列が選択状態にされた１つの単位回路のみが前記のような動作状態にされる。

第１１図には、第９図の真性乱数発生回路の動作の一例を説明するための概略波形図が示されている。動作制御信号ＡＣＴがハイレベルの活性化レベルにされた状態で、クロックＣＬＫを入力すると、それに対応して列選択信号Ｃ０～ＣＭ－１が列デコーダから出力される。このとき、Ｎ進カウンタは計数値がゼロであるから０行目の行選択信号Ｒ０を選択レベルにするので、第０行目の単位回路の出力信号が列選択信号Ｃ０～ＣＭ－１に対応してシリアルに出力される。０行目の単位回路の読み出しが行われると、そのキャリー信号によりＮ進カウンタが＋１の計数動作を行い、上記第０行目Ｒ０を非選択にして代わって第１行目Ｒ１を選択状態にする。このようにして、Ｎ－１行目までの単位回路の読み出しが順次に行われる。真性乱数ＲＲは、上記単位回路のシリアル出力Ｒと、１つ前の出力との排他的論理和により決定される。なお、第１０図の真性乱数発生回路の動作波形図は、第９図と類似しているので省略する。第９図と異なる点は、選択信号Ｒ０～ＲＮ－１がないことである。それによってＮ進カウンタを進行させるための動作が不要となり、Ｍ×Ｎ個の単位回路（基本回路）を全て選択するために必要なサイクルがＭ回となる。

第１２図には、この発明に係る真性乱数発生回路の他の一実施例の概念図が示されている。この実施例では、算術方式の乱数発生回路と、本発明にかかる物理現象を利用した真性乱数発生回路を組み合わせた方法によって、乱数を発生させるものである。前述のように算術方式の乱数発生回路は、回路が比較的小規模であるが、得られる乱数の品位は高くない。特に、無数の乱数を取得した場合、周期性が表れるという本質的な欠点がある。そこで、算術方式のアルゴリズム中に、この発明に係る真性乱数発生回路での電気信号ノイズに応答した不規則な要素を初期値として挿入することで、周期性を低減することが可能である。

第１３図には、第１２図の初期値発生回路の一実施例の回路図が示されている。この実施例は、基本的には前記第６図の実施例と同様である。異なる点は、排他的論理和ＥＸ０～ＥＸｎに代えてフリップフロップ回路ＦＦ０～ＦＦｎが設けられ、かかるフリップフロップ回路ＦＦ０～ＦＦｎからＤ０～Ｄｎのような初期値を得るものである。

上記信号Ｄ０～Ｄｎは、そのうちの大半が前記のようなプロセスバラツキによって固定値となるが、そのうちのいずれか１ないし数ビットが電気信号ノイズに応答した乱数となるので、上記算術方式乱数発生回路の初期値としての機能を十分に発揮させることができる。

第１４図には、第１２図の初期値発生回路の他の一実施例の回路図が示されている。この実施例は、基本的には前記第６図の実施例と同様である。異なる点は、活性化信号ＡＣＴによって１ビットの乱数をフリップフロップ回路ＦＦから出力させるものである。つまり、この実施例では１ビットの乱数を前記算術方式乱数発生回路の初期値としての用いるものである。

第１５図には、第１３図と第１４図の初期値発生回路の動作を説明するための波形図が

示されている。動作制御信号ＡＣＴをハイレベルにすると、第１３図の回路では各単位回路ＵＣ０～ＵＣｎから出力信号Ｒ０～Ｒｎが出力される。この出力信号Ｒ０～Ｒｎは、前記のように固定値となるものや電気信号ノイズに対応して変化するものが存在する。動作制御信号ＡＣＴをハイレベルからロウレベルにすると、そのときの上記出力信号Ｒ０～Ｒｎに対応した乱数Ｄ０～Ｄｎがフリップフロップ回路ＦＦ０～ＦＦｎに取り込まれて、固定値を含むＤ０～Ｄｎからなる複数ビットからなる乱数が出力される。

第１４図の回路では、上記各単位回路ＵＣ０～ＵＣｎの出力信号Ｒ０～Ｒｎが排他的論理和回路ＥＸ０～ＥＸｎに供給され、そのときどきの信号Ｒ０～Ｒｎに対応した１ビットの乱数が排他的論理和回路ＥＸ０～ＥＸｎを通して出力されている。したがって、動作制御信号ＡＣＴをハイレベルからロウレベルにすると、そのときのに生成されている乱数がフリップフロップ回路ＦＦに取り込まれて、１ビットからなる乱数ＤＭが出力される。

第１６図には、この発明に係る真性乱数発生回路の他の一実施例の回路図が示されている。この実施例は、前記第９図に示した真性乱数発生回路に識別情報Ｆを出力させる出力端子が設けられる。つまり、Ｍ×Ｎ個の単位回路から出力されるＭ×Ｎ個の出力信号が識別情報Ｆとして出力される。上記識別情報Ｆは、適当な記憶回路に保持されて管理システムに登録される。この識別情報Ｆの照合方法としては、登録時と照合時の環境や条件の違いの他に前記のように電気信号ノイズに応答する真性乱数に対応した識別番号の変動を許容する必要がある。上記真性乱数発生回路を搭載した半導体集積回路装置に電源投入等を行った際、あるいは前記動作活性化信号ＡＣＴを活性化した直後の識別信号Ｆを適当な記憶回路に記憶させて、これを被識別番号とする。管理システムから登録識別番号を順次取り出す。登録識別番号と被識別番号を比較する。

登録識別番号と被識別番号の比較結果の違いが小さいものを一致候補にする。この動作を管理システムに登録されている登録識別番号について繰り返すことで、最終的に全ての登録識別番号の中で最も違いが小さいものが同一最有力候補となる。

登録識別番号と被識別番号を比較において、対応するビットの”０”、”１”出力パターンは、個々の登録識別番号に特有であり、同一の半導体集積回路装置から出力された識別番号であるかは、パターンを構成するビット数の一致の割合で判定できる。登録時と照合時の環境や前記乱数ビットでの違いによる識別番号の変動を許容するため、被識別番号と登録済みの識別番号とのずれの合計がもつとも小さいものを一致の候補とすることによりチップ識別が可能となる。

第１７図には、この発明に係る真性乱数発生回路の一実施例の回路図が示されれている。この実施例は、基本構成は前記第９図の実施例と同様である。本願においては、ＭＯＳＦＥＴの特性のバラツキはランダムな分布であることに着目し、数多くの単位回路を観察すれば、第１インバータ回路ＩＮＶ１と第２のインバータ回路ＩＮＶ２又は第１ゲート回路Ｇ１と第２ゲート回路Ｇ２の特性が極めて等しい組み合わせがある確率で存在することを利用するものである。このために、半導体集積回路装置に真性乱数発生回路を製造した場合に、実際に電気信号ノイズを反映させる単位回路が存在するか否かの検査を行うことが不可欠となる。

この実施例では、真性乱数発生回路に自身を試験するテスト回路が付加される。このテスト回路での検査方法は、単位回路群中に含まれる第１ゲート回路Ｇ１（第１インバータ回路ＩＮＶ１）と第２ゲート回路Ｇ２（第２インバータ回路ＩＮＶ２）の特性が極めて等しい組み合わせの単位回路の数を判定し、物理現象に基づく電気信号ノイズを確実に捉えることを保証するものである。

前記第１６図において識別情報Ｆを取り出したように、各単位回路からの出力信号を得られる回路ノード、つまりはインバータ回路ＩＮＶ１１の出力端子（排他的論理和回路ＥＸの一方の入力）の信号Ｒを反転検出器に供給し、この検出信号Ｈを計数器により計数する。この計数出力Ｃを比較器で比較し、判定結果Ｍを得るものである。また、上記テスト動作のために（４＋Ｍ）進カウンタにより列選択信号を形成するようにされる。（４＋Ｍ）進カウンタは、同じ単位回路を４回連続して選択すると、次の単位回路の選択動作に移るという動作を繰り返して行う。

第１８図には、上記テスト回路の動作の一例を説明するためのタイミング図が示されている。テスト信号ＴＳをハイレベルにして（４＋Ｍ）進カウンタ動作を指示する。また、反転検出器と計数器を初期状態又は初期値とする。動作制御信号ＡＣＴをハイレベルにして乱数発生回路を動作状態にする。クロックＣＬＫの供給して最初の単位回路からの順次の読み出し動作を行う。このとき、（４＋Ｍ）進カウンタは、クロックＣＬＫ１～４に対して同じ単位回路を４回連続して選択する。これにより、前記第２図（ｂ）のように固定値を出力するものは、４回とも同じ信号Ｒが出力される。

このように固定値を出力させるものは反転検出器は反転検出を行わないので、計数器の計数値は増加しない。これに対して、第２図（ａ）のように電気信号ノイズＶｎｚに応答した出力信号Ｒを形成するものが存在すると、４回のアクセス中での反転回数は最大で３回であるが、１回以上の反転した場合には検出結果は真とする。同図では、２サイクル目と４サイクル目で出力信号Ｒが変化し、このように反転検出器では出力Ｈのレベルがその都度変化する。

このように１回でも出力Ｈが変化すると、結果が真であるとき計数器の値Ｃ０をロウレベルからハイレベルに変化させて計数値を１増やす。単位回路群中の次の単位回路の選択に移り、最後の単位回路まで上記同様な検出動作を繰り返して行う。計数器の数が規定値より大きい時、検査結果Ｍの値を真（ハイレベル）とする。真性乱数を得る場合には基本的には上記規定値は１であればよいが、安全性を考慮して２又は３以上の複数にすることが望ましい。

例えば、第１８図に示したように計数器を２ビット出力のバイナリカウンタとしたとき、クロックＣＬＫのＫ－１サイクル目で計数出力Ｃ０とＣ１が共にハイレベルになることを比較器が検出して上記検査結果Ｍをハイレベルにように決めれば、第２図（ａ）のように電気信号ノイズＶｎｚに応答した出力信号Ｒを形成するものが４個以上存在することが確かめられたことになる。

１つの単位回路を検査に対してＣＬＫパルスの４個で４回アクセスしたが、最低２回以上であっても構わない。２回アクセスする時は、（２＋Ｍ）進カウンタを用いるものである。検査以外のときには、上記テスト信号ＴＳのロウレベルの応じて前記のようにＭ進カウンタとして動作するようにされる。あるいは、そのまま（４＋Ｍ）進カウンタや（２＋Ｍ）進カウンタとして動作させてもよい。この場合には、読み出しサイクルが４倍又は２倍に増加する。

セキュリティ製品における政府機関の規定として、ＮＩＳＴ（米国標準技術研究所）が策定したＦＩＰＳ１４０－２がある。この中には、政府の購入品が備える暗号モジュールが満たすべきセキュリティ要件（ＦＩＰＳ　ＰＵＢ　１４０－２，ＳＥＣＵＲＩＴＹ　ＲＥＱＵＩＲＥＭＥＮＴＳ　ＦＯＲ　ＣＲＹＰＴＯＧＲＡＰＨＩＣ　ＭＯＤＵＬＥＳ）が規定されており、乱数については統計的手法による、品位の検定合格基準が示されている。当該方法を用いた方法では、それを実現するための専用の回路の規模が比較的大きいことや、半導体試験装置で検査する場合に比較的時間がかかるという短所がある。

これに対して、この発明に係る乱数発生回路に設けられたテスト回路では、半導体ウェハ上に回路が完成した時点で、上記テスト機能を備えたテスタに接続することなく、自身で判定を行うことができる。また、半導体集積回路装置として出荷時にも自身で判定することが可能である。更に、必要ならシステムに搭載された時点で、必要に応じてあるいは定期的に上記真性乱数発生回路が正常に動作可能な状態であるか否かの確認を行うことができる。これによって、信頼性の高い真性乱数発生が可能となるものである。いずれも、本方式が統計に裏付けられたものであることにより可能である。

すなわち、真性乱数発生回路の診断（試験）は、その乱数の品位の評価に等しく、ある種の統計的処理が必要である。そのため、試験装置、試験時間、長期信頼度保証などの大きな課題がある。特に、真性乱数発生器がＬＳＩや最終システムに搭載された以降、回路自体が正常に動作しているか重要な問題である。何故なら、品位の高い真性乱数が得られなければ、セキュリティが危ぶまれることになるからである。しかし、真性乱数発生回路を試験あるいはモニタすることは稼動中のシステムとしては大きな負荷である。このよう

な技術的課題に対して、本願発明の真性乱数発生回路では、上記のように簡単な構成でこれらの問題を解決することができる。

第１９図には、この発明に係る真性乱数発生回路の一実施例の回路図が示されている。この実施例は、基本構成は前記第９図の実施例と同様である。この実施例では、クロックとして発振器で形成した発振パルスＯＳＣを用いるようにするものである。

第２０図には、第１９図の真性乱数発生回路の動作波形図が示されている。活性化信号ＡＣＴにより、発振器が特定の周期Ｔｏｓｃのパルスを発生する。パルスＯＳＣを受けて、単位回路群中の単位回が順次選択され、ＲＲ信号に乱数が生成される。スタート信号ＳＴをハイレベルに遷移させると、ＲＲ信号の乱数が出力ＲＹから取り出される。スタート信号ＳＴの周期Ｔｃと発振器の周期Ｔｏｓｃの関係は、全ての単位回路からの出力信号の読み出しを必要とするから、［Ｔｃ］≧［Ｔｏｓｃ］×［ｎ］である。ここで、上記の［ｎ］は、単位回路群中の単位回路数（Ｍ×Ｎ）である。発振器出力パルスＯＳＣは、かかる真性乱数発生回路が搭載されたＬＳＩのシステムクロック等であってもよい。

第２１図には、この発明に係る真性乱数発生回路の一実施例の回路図が示されている。この実施例は、基本構成は前記第１９図の実施例と同様である。この実施例では、スタート信号ＳＴが省略されて、動作制御信号ＡＣＴより動作状態となり、シフトレジスタが出力の直前に設けられて並列ビットからなる乱数ＲＡｉを生成するようにされる。

第２２図には、この発明に係る乱数発生回路の出力部の他の一実施例の回路図が示されている。この実施例は、前記第２１図の実施例のシフトレジスタをメモリに変更している。同図で用いたメモリは、いわゆるシリアル入力／パラレル出力型のメモリである。制御信号ＡＣＴがハイレベルの時、真性乱数発生回路からクロックのＭ×Ｎサイクル毎にＲＲから１ビットずつ真性乱数発生し、また同時に当該メモリはシリアル入力モードであって、入力ＳＩから真性乱数を取り込み蓄積する。制御信号がロウレベルの時、真性乱数発生回路は停止し、同時に当該メモリはパラレル出力モードであって、入力ＡＤのアドレス情報に対応したメモリ空間に蓄積された真性乱数を出力ＤＴから出力する。なお、当該メモリの各入出力の意味は、ＳＥはこのメモリのモードを切り替えるための制御入力であって、ハイレベルの時シリアル入力モード、ロウレベルの時パラレル出力モードであり、ＳＩはシリアルデータ入力であり、ＣＫはシリアル入力を取り込む時の同期信号入力であり、ＡＤはパラレル出力モードの時メモリ空間を選択するアドレス入力であり、ＤＴはパラレルデータ出力である。

第２２図に示されたメモリは、ＦＩＦＯ（Ｆｉｒｓｔ　Ｉｎ　Ｆｉｒｓｔ　Ｏｕｔ）型メモリや、シリアル入力とパラレル出力を同時に行える非同期型メモリであっても構わない。

第２３図には、前記第２１図に示した真性乱数発生回路の動作波形図が示されている。動作制御信号ＡＣＴにより回路が動作状態となり、Ｎ進カウンタのキャリー信号ＣＡによってシフトレジスタが１ビットのシフト動作を行い生成された真性乱数ＲＲの取り込みを行う。この実施例では、０ないし７からなる８回の前単位回路群の読み出しによって、８ビットからなる乱数Ｄ０～Ｄ７をパラレルに出力させることができる。

第２４図には、この発明に係る真性乱数発生回路の一実施例のチップ構成図が示されている。この実施例では、真性乱数発生回路を１つのＩＣで構成するものである。外部端子として電源端子ＶＣＣ、ＶＳＳ、クロック入力端子ＣＬＫ、動作制御信号ＲＳＴ及び真性乱数出力端子ＲＲから構成される。前記のように発振器を搭載したものでは、クロック端子ＣＬＫが省略される。また、テスト回路を備えたものでは、判定出力端子、テストモード入力端子等が付加される。判定出力端子は、乱数出力端子ＲＲと許容することもできる。かかるＩＣチップを１つのパッケージに封止しても、他のＩＣと同じ実装基板に搭載して封止（マルチチップＩＣ）しても、また、そのままシステムに実装しても構わない。

第２５図には、この発明に係る半導体集積回路装置の一実施例のブロック図が示されている。この実施例の各回路ブロックは、実際の半導体基板上における幾何学的な回路配置に合わせて描かれている。この実施例の半導体集積回路装置は、特に制限されないが、複数の回路機能ブロックが組み合わされて特定の信号処理機能を持つようにされる。このよ

うな回路ブロックを有する半導体集積回路装置に真性乱数発生回路が搭載される。真性乱数発生回路に必要とされるクロックは、かかる半導体集積回路装置に設けられたクロック発生回路で形成されたクロック又は外部端子からクロック供給を受けるものではそのクロックが用いられる。また、第１９図や第２１図の乱数発生回路のように発振器を持つものでは、上記のようなクロックの供給は不要である。

第２６図には、この発明に係る半導体集積回路装置の他の一実施例のブロック図が示されている。この実施例の各回路ブロックも、実際の半導体基板上における幾何学的な回路配置に合わせて描かれている。この実施例は、ＭＰＵ（マイクロプロセッシングユニット）を中心とした１チップのマイクロコンピュータに向けられている。このマイクロコンピュータでは、バスＢＵＳ（アドレスバス、データバス及びコントロールバス）上に上記ＭＰＵの他に、ＲＡＭ（ランダム・アクセス・メモリ）、ＲＯＭ（リード・オンリー・メモリ）、ＤＭＡＣ（ダイレクト・メモリ・アクセス・コントローラ）、ＴＩＭ（タイマー）及びＡＤＣ（アナログ・デジタル・コンバータ）、ＤＡＣ（デジタル・アナログ・コンバータ）と、この前記の真性乱数発生回路が接続される。

本発明に係る真性乱数発生回路は、全て標準ＣＭＯＳ論理回路のみで実現される。このことは、複雑なアナログ回路設計やＬＳＩ実装に掛かる負荷を軽減し、製品の価格を低減し、信頼性性の向上に寄与することになる。また、セキュリティ問題において最大の課題である、クラッキングに対して強固なモジュールを提供できる。何故なら、標準論理回路のみで構成することで、ＬＳＩの中でアタックの標的から逃れる、迷彩（ステルス）効果が得られるからである。つまり、アナログ回路を用い場合のように回路パターンに特徴がなく、しかも上記のようにバスＢＵＳを介して乱数の取り出しを行うようにした場合には、上記迷彩（ステルス）効果をいっそう高くすることができる。

第２７図には、この発明に係る真性乱数発生回路の他の一実施例の構成図が示されている。第２７図（ａ）には、回路ブロック構成が示され、第２７図（ｂ）には、レイアウト構成が示されている。この実施例では、例えば前記第７図に示したような真性乱数発生回路がｎ個設けられる。つまり、０ないしｎ－１からなるｎ個の真性乱数発生回路が設けられ、それぞれの出力信号Ｒ０、Ｒ１～Ｒｎ－１はマルチプレクサＭＵＸを通して１つつの信号が選ばれて真性乱数ＲＭとして出力される。

第２７図（ｂ）のレイアウト構成に示すように、マルチプレクサを挟んで上下に真性乱数発生回路を設けることにより、効率よく回路配置を行うことができる。同図において、真性乱数発生回路の中の１つの回路ブロックは、例えば前記１つの単位回路を表している。この構成においては、２つの真性乱数発生回路に挟まれたマルチプレクサは２つのうちの１つを選択するというような比較的簡単な構成で良いから、マルチプレクサが配置される部分には前記デコーダ等の選択信号発生回路が配置される。

例えば、この実施例の真性乱数発生回路において乱数Ｒを得るのにｎ個の単位回路で構成される場合、１ビットの乱数Ｒを得るためには前記のように全ての単位回路からの出力信号を得る必要からにｎサイクルを費やすことになる。そこで、上記１つの乱数を得るに必要なｎサイクルに対応してこの実施例のようにｎ個の乱数発生回路を設けた場合には、クロックＣＬＫに同期した高い周波数で乱数を発生させることができる。ただし、動作制御信号により動作を開始したときからｎサイクルからなるダミーサイクルを必要とする。

第２８図には、第２７図に示した真性乱数発生回路の動作の一例を示すタイミング図が示されている。第２７図の真性乱数発生回路では、最初の乱数発生回路の読み出しのためにｎサイクル（ｎクロック）後から各真性乱数発生回路から乱数Ｒ０～Ｒｎ－１が出力されるから、マルチプレクサＭＰＸによりクロックＣＬＫに同期して１個ずつ選ぶようすることにより、クロックＣＬＫに同期した真性乱数ＲＭ（Ｒ０、Ｒ１、Ｒ２…Ｒｎ－１、Ｒ０’Ｒ１’Ｒ２’…のようにクロックＣＬＫに同期した高ビットレートな真性乱数を得ることができる。

第２９図には、この発明が適用されるＩＣカードの一実施例の外観図が示されている。ＩＣカードは、プラスチックケースからなるカード１０１と、かかるカード１０１の内部に搭載された図示しない１チップのマイクロコンピュータ等からなるＩＣカード用チップ

を持つものである。上記ＩＣカードは、さらに上記ＩＣカード用チップの外部端子に接続されている複数の接点（電極）１０２を持つ。

複数の接点１０２は、後で第３０図によって説明するような電源端子ＶＣＣ、電源基準電位端子ＶＳＳ、リセット入力端子ＲＥＳバー、クロック端子ＣＬＫ、データ端子Ｉ／Ｏ－１／ＩＲＱバー、Ｉ／Ｏ－２／ＩＲＱバーとされる。ＩＣカードは、かかる接点１０２を通して図示しないリーダーライタのような外部結合装置から電源供給を受け、また外部結合装置との間でのデータの通信を行う。

第３０図には、この発明に係るＩＣカードに搭載されるＩＣカード用チップ（マイクロコンピュータ）の一実施例の概略ブロック図が示されている。同図の各回路ブロックは、公知のＭＯＳ集積回路の製造技術により、特に制限されないが、単結晶シリコンのような１個の半導体基板上において形成される。

この発明に係るＩＣカード用チップの構成は、基本的にマイクロコンピュータと同じような構成である。その構成は、クロック生成回路、中央処理装置（以下、単にＣＰＵという）、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）やＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）、不揮発性メモリ（ＥＥＰＲＯＭ）などの記憶装置、暗号化及び復号化処理の演算を行なうコプロセッサ（暗号化・復号化装置）、入出力ポート（Ｉ／Ｏポート）などからなる。

クロック生成回路は、図示しないリーダライタ（外部結合装置）から第２９図の接点１０２を介して供給される外部クロックＣＬＫを受け、かかる外部クロック信号に同期したシステムクロック信号を形成し、それをチップ内部に供給する回路である。

ＣＰＵは、論理演算や算術演算などを行う装置であり、システムコントロールロジック、乱数発生器及びセキュリィロジック及びタイマなどを制御する。ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭのような記憶装置は、プログラムやデータを格納する装置である。コプロセッサは、ＤＥＳ暗号法などに適合された回路から構成される。Ｉ／Ｏ（入出力）ポートは、リーダライタと通信を行う装置である。データバスとアドレスバスは、各装置を相互に接続するバスである。

上記記憶装置のうち、ＲＯＭは、記憶内容が不揮発的に固定されているメモリであり、主にプログラムを格納するメモリである。揮発性メモリ（以下、ＲＡＭという）は自由に記憶情報の書き換えができるメモリであるが、電源の供給が中断されると、記憶している内容が消えてなくなる。ＩＣカードがリーダライタから抜かれると電源の供給が中断されるため、上記ＲＡＭの内容は、保持されなくなる。

上記不揮発性メモリ（以下、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌ　Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）という）は、内容の書き換えが可能な不揮発性メモリであり、その中に一旦書き込まれた情報は、電源の供給が停止されてもその内部に保持される。このＥＥＰＲＯＭは、書き換える必要があり、かつＩＣカードがリーダライタから抜かれても保持すべきデータを格納するために使われる。例えば、ＩＣカードがプリペイドカードとして使用されるような場合、のプリペイドの度数などは、使用するたびに書き換えられる。この場合の度数などは、リーダライタか抜かれてもＩＣカード内で記憶保持する必要があるため、ＥＥＰＲＯＭで保持される。

ＣＰＵは、いわゆるマイクロプロセッサと同様な構成にされる。すなわち、その詳細を図示しないけれども、その内部に命令レジスタ、命令レジスタに書込まれた命令をデコードし、各種のマイクロ命令ないしは制御信号を形成するマイクロ命令ＲＯＭ、演算回路、汎用レジスタ（ＲＧ６等）、内部バスＢＵＳに結合するバスドライバ、バスレシーバなどの入出力回路を持つ。ＣＰＵは、ＲＯＭなどに格納されている命令を読み出し、その命令に対応する動作を行う。ＣＰＵは、Ｉ／Ｏポートを介して入力される外部データの取り込み、ＲＯＭからの命令や命令実行のために必要となる固定データのようなデータの読み出し、ＲＡＭやＥＥＰＲＯＭに対するデータの書き込みと読み出し動作制御等を行う。

上記ＣＰＵは、クロック生成回路から発生されるシステムクロック信号を受けそのシステムクロック信号によって決められる動作タイミング、周期をもって動作される。ＣＰＵは、その内部の主要部がＰチャンネル型ＭＯＳＦＥＴとＮチャンネル型ＭＯＳＦＥＴとか

らなるＣＭＯＳ回路から構成される。特に制限されないが、ＣＰＵは、ＣＭＯＳスタティックフリップフロップのようなスタティック動作可能なＣＭＯＳスタテック回路と、信号出力ノードへの電荷のプリチャージと信号出力ノードへの信号出力とをシステムクロック信号に同期して行うようなＣＭＯＳダイナミック回路とを含む。

コプロセッサは、内部で扱う平文データに符号ビットを付加し、ポジ／ネガの両方の状態を持つようにする。暗号化における繰り返し演算時に、データを符号ごとランダムに変更する。符号の影響を受けない演算（排他的論理和など）はそのまま符号を無視して演算する。符号の影響を受ける演算（変換表を用いた演算など）では、ポジ用の演算回路とネガ用の演算回路を用意し、データの符号によって演算回路の出力を選択する機構を用いる。

ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）は、広範に用いられている秘密鍵ブロック暗号である。ＤＥＳのアルゴリズムは、大きく平文のデータフローと鍵のデータフローに分割できる。平文データフローでは、ＩＰとよばれる転置（信号の入れ換え）を行った後、上位と下位それぞれ３２ビットずつにデータを分割し、転置・換字処理を１６回繰り返す。最後に上位と下位それぞれ３２ビットデータを統合し、IP^{-1}とよばれる転置を行い、暗号文を得る。

ＤＥＳでは、暗号化と復号化が同じ処理で実現できる。ただし暗号化と復号化では、鍵のスケジューリングが異なる。鍵のスケジューリング部分について、詳細は省略するが、鍵データを元に、各段に対して４８ビット鍵スケジューリングデータの出力を行う。

ＤＥＳアルゴリズムでは、同じ平文に対しては常に同じ内部動作を行う。その結果、内部信号が入力信号に依存して変化するので、ＤＰＡ（Ｄｉｆｆｒｅｎｔｉａｌ　Ｐｏｗｅｒ　Ａｎａｌｙｓｉｓ）法での統計処理を行いやすい。つまり、ＤＰＡ法では、消費電流波形を統計処理して暗号鍵を推定し、例えばＤＥＳのある部分に仮定した暗号鍵を当てはめて、平文を変化させながら消費電流波形を測定して統計する。暗号鍵を様々に変化させながらこの作業を繰り返し、正しい鍵のときには電流波形が大きなピークを示す。

上記のようなＤＰＡによるＤＥＳ解読に対する対策の例として、特開２０００－０６６５８５号公報がある。この公報に記載の技術では、マスクａのパターンと、そのビット反転のマスクパターンのペアを設け、暗号化を行う毎にこのペアの一方をスイッチによりランダムに選択して、装置内部の平文に依存したビットをマスクし、暗号文を出力する前に暗号文からマスクａの影響を除去するようにするものである。

ＤＰＡによる解読防止のためには、上記マスクが特定のパターンに偏らないようにする必要のあることは説明されているが、どのようにすれば複数ビットのパターンが偏らないようにするために、乱数発生器で生成された乱数が利用される。

第３１図には、この発明が適用される非接触ＩＣカードの一実施例のブロック図が示されている。同図には、非接触ＩＣカードに対して、外部装置として設けられるリード・ライト装置のコイル（アンテナ）も併記されている。非接触ＩＣカードに搭載されるＬＳＩは、図示されるブロックの他に、例えばメモリやマイクロコンピュータ等の機能ブロックを備えるが、それらを論理回路及び不揮発メモリとして表している。上記ＬＳＩの各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ＭＯＳＦＥＴ（金属酸化物半導体型電界効果トランジスタ。この明細書では、ＭＯＳＦＥＴをして絶縁ゲート型電界効果トランジスタの総称とする）集積回路の製造技術により、単結晶シリコンのような１個の半導体基板面上に形成される。また、このＬＳＩは、所定の保護膜によってラミネート処理された後、非接触ＩＣカードの基体となるカード面上に搭載され、さらに被膜処理が施される。

本実施例の非接触ＩＣカードは、特に制限されないが、いわゆる密着型の非接触ＩＣカードとされ、例えば銅箔等を用いてカード面上にコイル状に形成される受電コイル（カード側アンテナ）と、所定の配線層を介して上記受電コイルに結合されるＬＳＩとを備える。このＬＳＩは、４個のダイオードがブリッジ結合されてなる整理回路と、整流回路の整流電圧を平滑する平滑コンデンサと、安定化電源回路とによって、上記論理回路及び不揮発メモリ等を含む内部回路の動作電圧ＶＤＤが形成される。上記整流回路に対しては、実

質並列形態にクロック発生回路、データ受信回路及びデータ送信回路が設けられる。

上記ダオードブリッジ回路からなる整流回路は、リード・ライト装置の送電コイル（アンテナ）との電磁結合によって非接触ＩＣカードの受電コイルに電力源として伝達される交流信号つまりキャリアを整流し、上記平滑コンデンサで平滑した電圧を安定化電源により直流電源電圧ＶＤＤを生成し、ＬＳＩの各機能ブロックに動作電源として供給する。パワーオンリセット回路は、電源電圧ＶＤＤの立ち上がりを検知し、つまりは、リード・ライト装置との結合を検知して、データの受信や送信を正常に行うようにするために、論理回路のレジスタやラッチ回路等をリセットさせる。

データ受信回路は、リード・ライト装置から例えばキャリアを周波数変調することにより伝送されるデータを受信復調し、内部入力データとしてＬＳＩの内部回路に伝達する。内部回路で形成された出力データは、データ送信回路によりキャリアを周波数変調してリード・ライト装置に伝送する。

上記のような内部回路（論理回路）やデータ受信回路及びデータ送信回路では、上記動作電圧ＶＤＤの他に、動作シーケンス制御や信号の受信や送信のためにクロック信号を必要とする。この実施例では、クロック発生回路により上記交流信号をパルス信号とし、クロック信号を生成する。論理回路部には、乱数発生器が設けらており、外部とのデータ送信やデータ受信にかかる乱数が用いられる。

上記非接触ＩＣカードでは、直流電源電圧ＶＤＤの電流供給能力が小さいから、乱数発生器における消費電力も小さいことが必要とされる。前記のよう乱数発生器は、単位回路を順次に動作させるものであるために消費電流を小さくできる。それ故、この実施例の乱数発生器は、上記のような非接触ＩＣに搭載させるものとして好適なものとなる。

第３２図には、この発明に係る乱数発生回路で生成された乱数の乱数２次元散布図が示されている。同図においては、２００×２００ビットの乱数の０と１をドットの白と黒に対応して表示したものである。特に制限されないが、この実施例では、単位回路（基本回路）を１２８個設けて、通常のＣＭＯＳプロセスで回路を構成したものである。

同図は、図面の作成の関係で乱数２次元散布図を４００ｄｐｉでスキャナーで読み取り表示したものであるので、実際の乱数２次元散布図とは若干異なるが、おおよその乱数２次元散布を表しており、特有のパターンは存在しないことが判る。つまり、高い品位の乱数であることを表している。また、前記のＦＩＰＳ１４０－２での乱数検定結果は、次の通りである。１回の検定に使用される乱数の長さを２０，０００ビットとし、これを６００回行った結果、全てにおいてかかる検定をパスすることができた。

今日暗号やセキュリティが日常的に話題となるようになったのは、インターネットの普及が理由であろう。インターネットは遠く離れた機器をつなぐネットワーク技術である。インターネット上を往来するデータは、本質的に第三者の所有するコンピュータやセットワーク装置を通過するため盗聴や改竄の虞が常にある。インターネットをセキュリティやプライバシーが保証された安全なインフラとするために、暗号や認証が脚光を浴びている。現在、インターネット上で様々なセキュリティ技術が利用されているが、その代表的なものにＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔ Ｌａｙｅｒ）やＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ ｓｅｃｕｒｉｔｙ）技術などがある。これらの技術の詳細は記さないけれども、いずれも品位の高い乱数が必要である。特に、ＩＰｓｅｃは次世代のインターネット技術であるＩＰｖ６（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ Ｖｅｒｓｉｏｎ６）では必須条件として採用される。ＩＰｖ６は普及すると、個人の持つパーソナルコンピュータや携帯電話をはじめ、自動車や家電製品などにもＩＰ番号が割り当てらことも可能となる。そうなると、品位の高い乱数、つまり真性乱数をそれらの機器の中で容易に生成することが必要となる。

前述のように、本発明に係る真性乱数発生回路は、全て標準ＣＭＯＳ論理回路のみで実現される。このことは、複雑なアナログ回路設計やＬＳＩ実装に掛かる負荷を軽減し、製品の価格を低減し、信頼性性の向上に寄与することになる。

第３４図には、この発明に係る半導体集積回路装置に搭載される真性乱数発生回路の第１図に示された基本概念の応用概念の回路図が示されている。第１図では、真性乱数は複

数からなる各基本回路内のＩＮＶ１とＩＮＶ２に生じる電気信号ノイズを素にしているが、第３４図では、第１のインバータＩＮＶ１を共通とし第２のインバータを各基本回路に分散させる。つまり、１種類しか存在しない第１のインバータの論理しきい値ＶＬＴ１と各基本回路内の第２のインバータの論理しきい値ＶＬＴ２の差が極めて小さい組み合わせが存在する場合、第１のインバータおよび第２のインバータの電気信号ノイズの影響を反映して真性乱数を得ることができる。なお、第３のインバータ以後の動作は上記第１図で述べた内容と同じであるので省略する。

第３５図には、この発明に係る半導体集積回路装置に搭載される真性乱数発生回路の第３４図に示された応用基本概念のさらに別の応用概念の回路図が示されている。この実施例では、前記図３４のインバータ回路ＩＮＶ１～ＩＮＶ１４が、２入力のナンド（ＮＡＮＤ）ゲート回路Ｇ１～Ｇ１４に置き換えられる。上記ゲート回路Ｇ１は、一方の入力と出力とが結合される。このゲート回路Ｇ１の共通化された入出力が基本回路内のゲート回路Ｇ０２の一方の入力と接続される。ゲート回路Ｇ０２の出力はゲート回路Ｇ０３の一方の入力に接続される。ゲート回路Ｇ０３の出力はゲート回路Ｇ０４の一方の入力に接続される。そして、これらのゲート回路Ｇ０２～Ｇ０４の他方の入力には、電源ＶＤＤに接続され常にハイレベル（論理１）とさる。

第３４図のインバータ回路ＩＮＶ１～ＩＮＶ１４は、上記ナンドゲート回路Ｇ１～Ｇ１４のような論理ゲート回路の一種と見做すことができる。すなわち、入力信号を反転させる論理動作を行うものであるからである。第３４図のようにインバータ回路ＩＮＶ１～ＩＮＶ１４を用いた場合には、インバータ回路ＩＮＶ１とＩＮＶ０２のように初段側においては論理しきい値電圧ＶＬＴ付近で動作するものであり、電源電圧ＶＤＤと回路の接地電位との間に直流電流を流すものとなる。本願発明では、前記のように素子のプロセスバラツキによる論理しきい値電圧の正規分布を利用するものであり、そのために比較的多数からなる単位回路を動作させる必要があるので、上記インバータ回路ＩＮＶ１とＩＮＶ０２での直流電流は低消費電力化を実現する上では無視できない。

これに対して、この実施例のようにゲート回路Ｇ１～Ｇ１４を用いた場合には、各ゲート回路Ｇ１～Ｇ１４は、動作制御信号ＡＣＴをロウレベル（論理０）のような非活性化レベルとしたとき、ゲート回路Ｇ１の出力は無条件にハイレベル（論理１）となり、例えばゲート回路Ｇ１の出力を入力とするゲート回路Ｇ０２の出力は無条件にロウレベル（論理０）となり、ゲート回路Ｇ０２の出力を入力とするゲート回路Ｇ０３の出力は無条件にハイレベル（論理１）となり、ゲート回路Ｇ０３の出力を入力とするゲート回路Ｇ０４の出力は無条件にハイレベル（論理１）となり、各ゲート回路Ｇ１，Ｇ０２、Ｇ０３、Ｇ０４およびそれと等価なな他の基本回路ないのゲート回路においても直流電流が発生しない。すなわち、この実施例回路では、乱数を必要とするタイミングで上記動作制御信号ＡＣＴをハイレベル（論理１）のような活性化レベルとする。これにより、各ゲート回路Ｇ１～Ｇ１４は、上記動作制御信号ＡＣＴとは異なる他方の入力信号に応答して反転信号を形成するというインバータ回路としての動作を行う。これにより、上記動作制御信号ＡＣＴをハイレベルにすることにより、第３４図の基本回路図と同様の動作を行うものとなる。

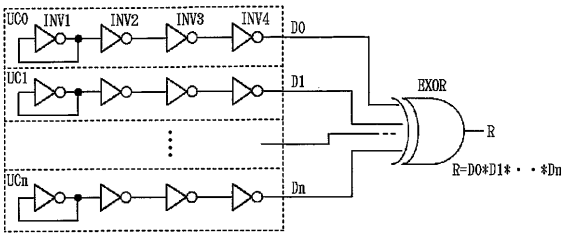
以上本発明者よりなされた発明を実施例に基づき具体的に説明したが、本願発明は前記実施例に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。例えば、抵抗素子を、インバータやゲート回路を構成する信号入力ＭＯＳＦＥＴに対する負荷素子とするような場合には、特性バラツキに応ずる情報は、抵抗素子の特性バラツキと信号入力ＭＯＳＦＥＴの特性バラツキとの両方を反映したものとなる。抵抗バラツキに対応する特定情報は、必ずしも半導体集積回路装置内のみで形成する必要は無く、外部端子を介して接続する構成とすることもできる。ただし、低消費電力化を図る上では、前記のようなＣＭＯＳゲート回路を用いることが望ましい。また、第１インバータ回路ＩＮＶ１と第２インバータ回路ＩＮＶ２は、その消費電流を低減させるために前記第１０図（ｂ）に示したようなクロックドインバータ回路ＣＮに置き換え、動作制御信号により活性化を行うようにするものであってもよい。

【産業上の利用可能性】

この発明は、ネットワーク機器に組込むもの、無線通信機器に組み込むもの、暗号化・複合化装置に組み込むもの、認証システムに組み込むもの、あるいは玩具系ロボットやゲームのキャラクタの「個性因子」や「気まぐれ因子」に組み込まれる乱数の乱数発生方法と半導体集積回路装置に広く利用することができる。

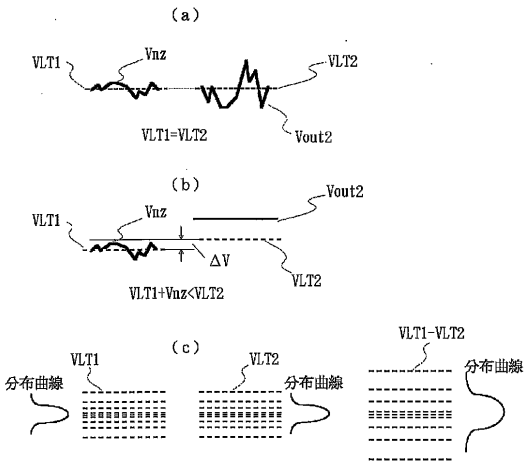
【図１】

第 1 図



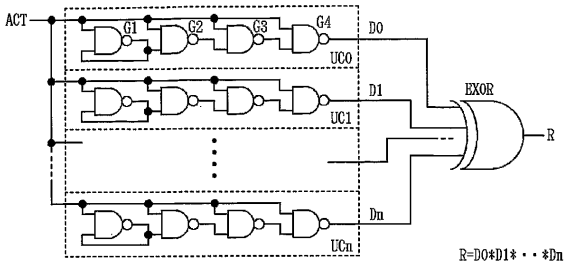
【図２】

第 2 図



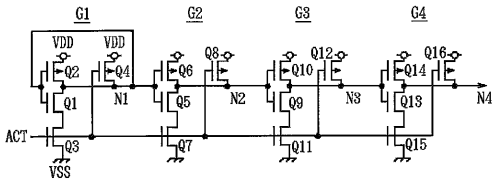
【図３】

第 ３ 図



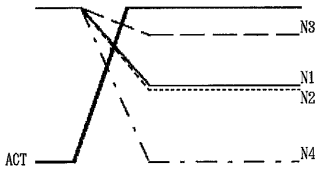
【図４】

第 ４ 図



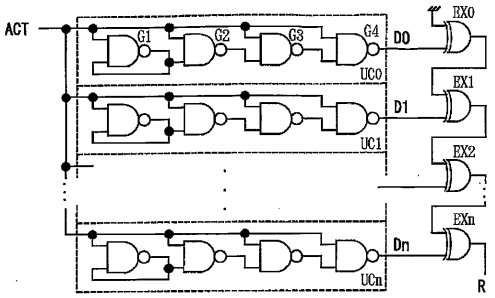
【図５】

第 ５ 図



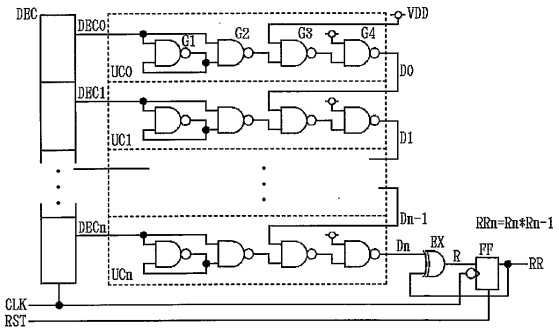
【図６】

第 ６ 図



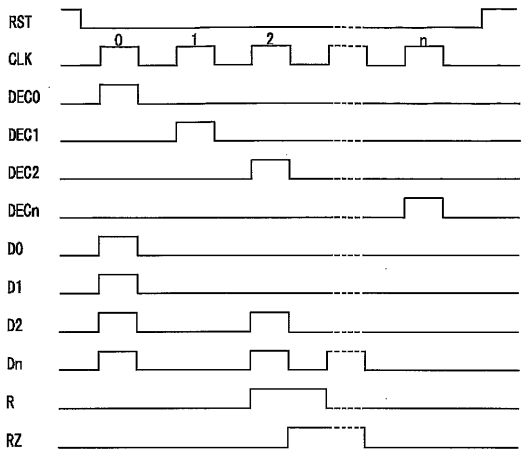
【図７】

第 ７ 図



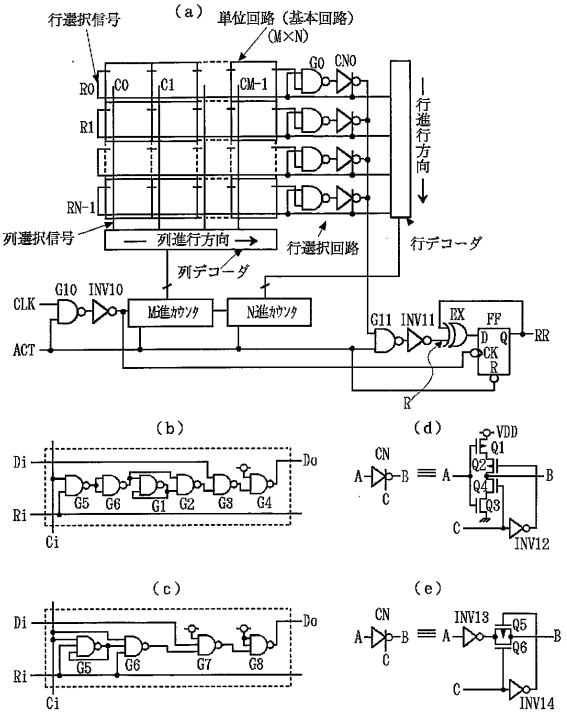
【図８】

第 ８ 図



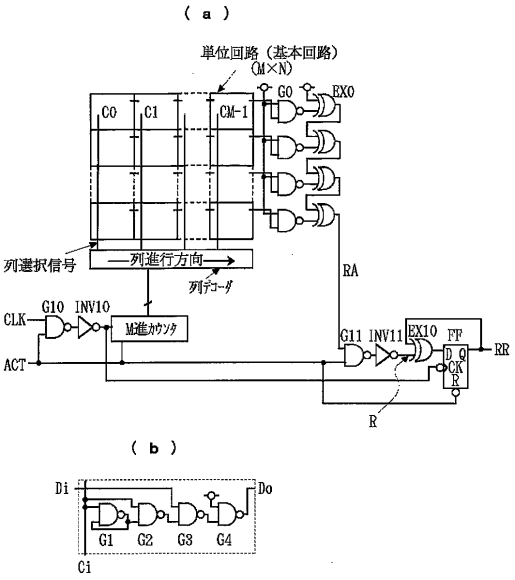
【図９】

第 ９ 図



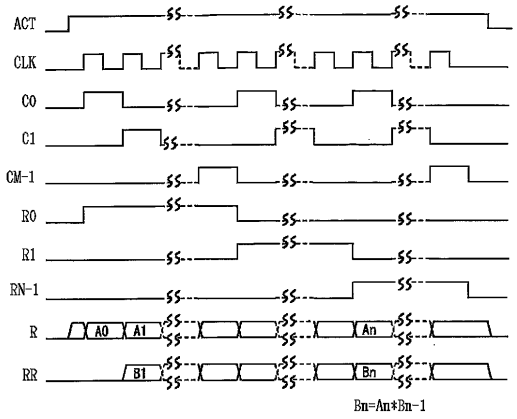
【図１０】

第 １０ 図



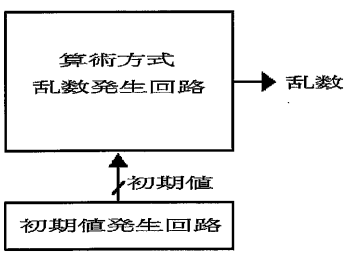
【図１１】

第 １１ 図



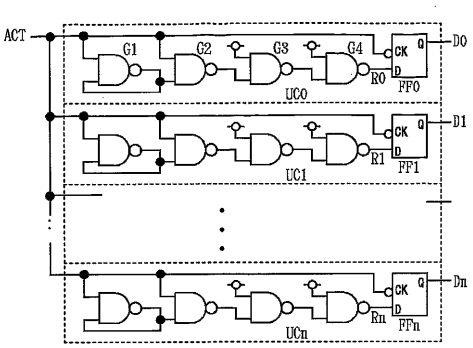
【図１２】

第 １２ 図



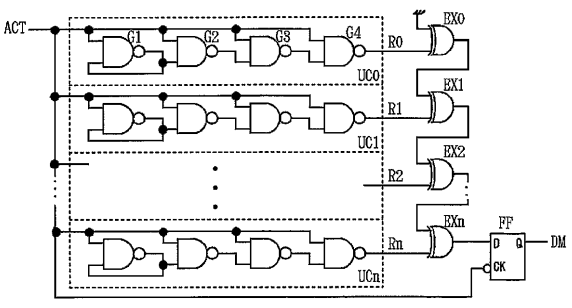
【図１３】

第 １３ 図



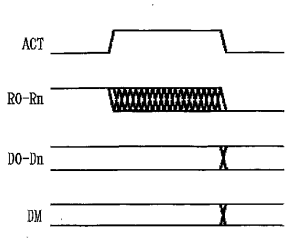
【図１４】

第 １４ 図



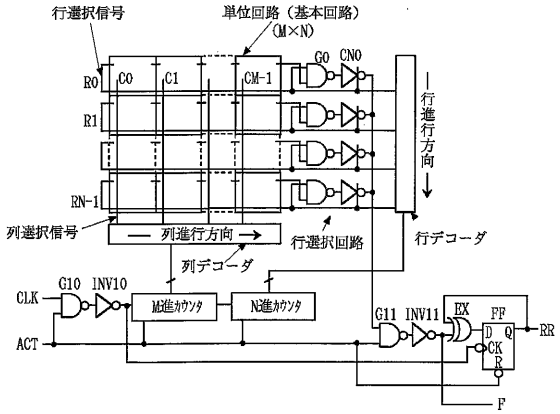
【図１５】

第　１５　図



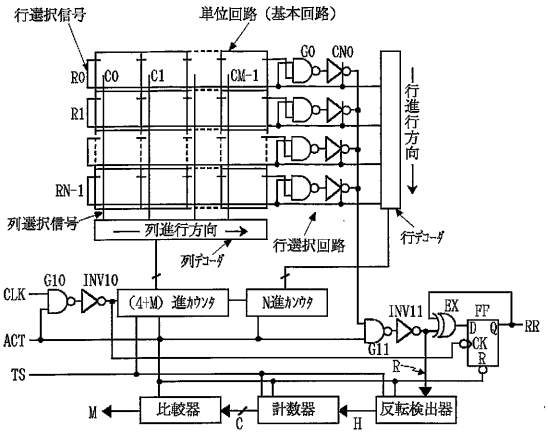
【図１６】

第　１６　図



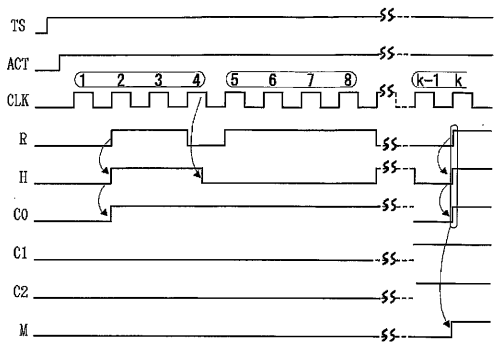
【図１７】

第　１７　図



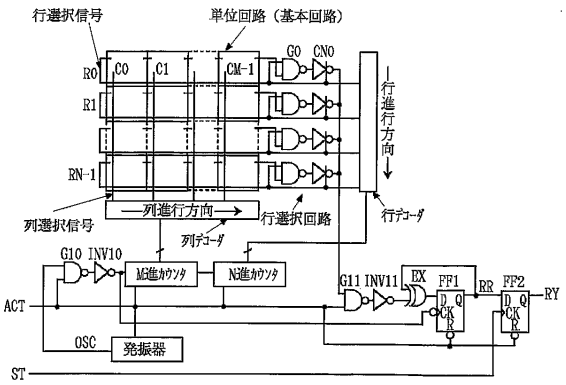
【図１８】

第　１８　図



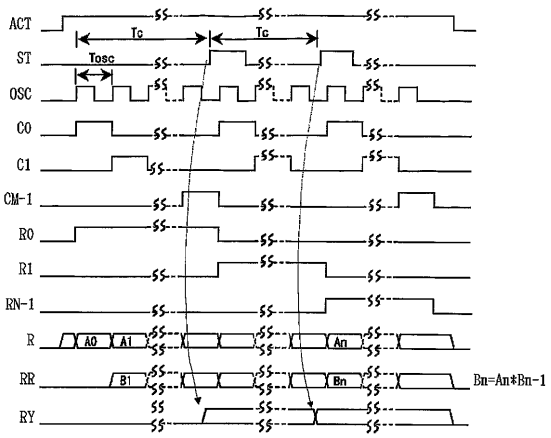
【図１９】

第　１９　図



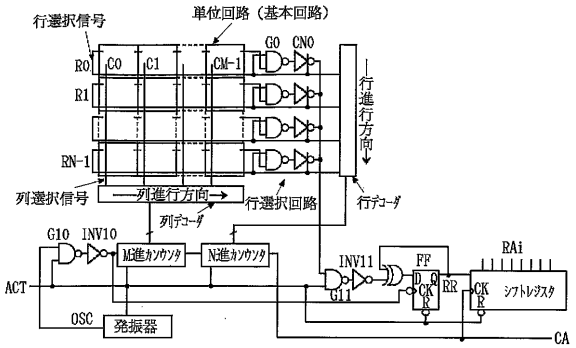
【図２０】

第　２０　図



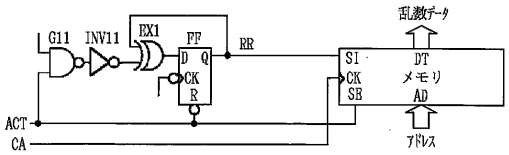
【図２１】

第　２１　図



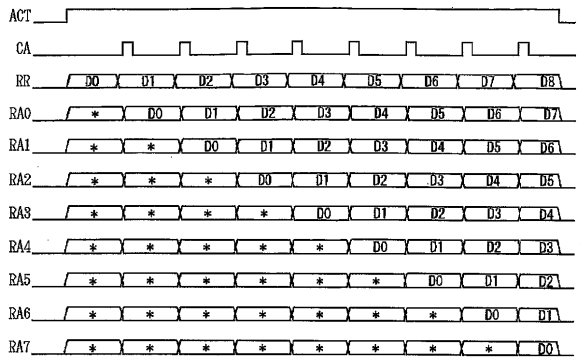
【図２２】

第　２２　図



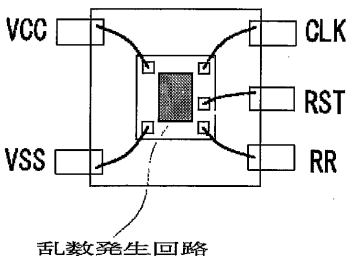
【図２３】

第　２３　図



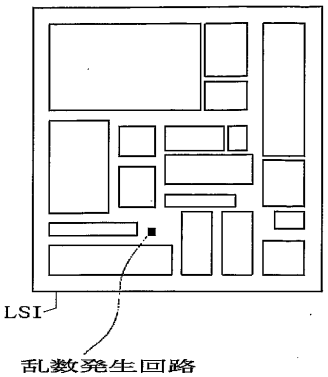
【図２４】

第　２４　図



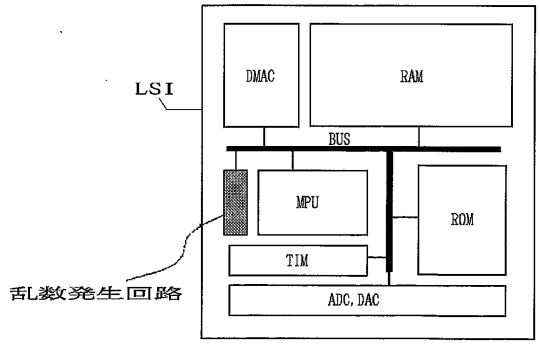
【図２５】

第　２５　図



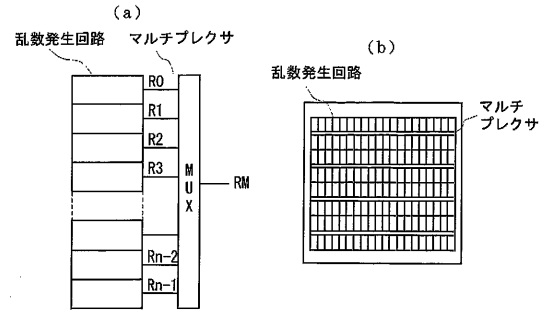
【図２６】

第　２６　図



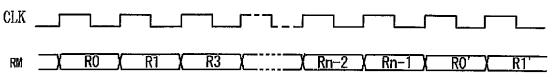
【図２７】

第　２７　図



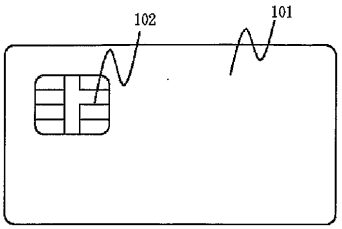
【図２８】

第　２８　図



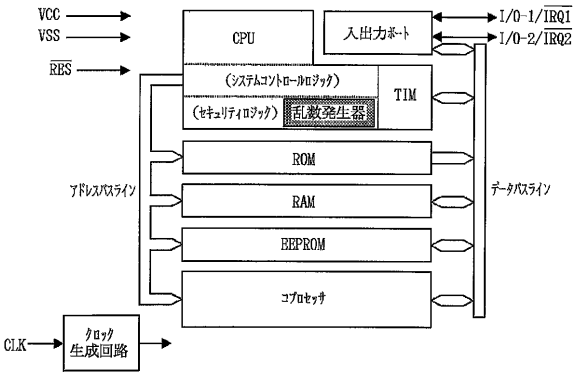
【図２９】

第　２９　図



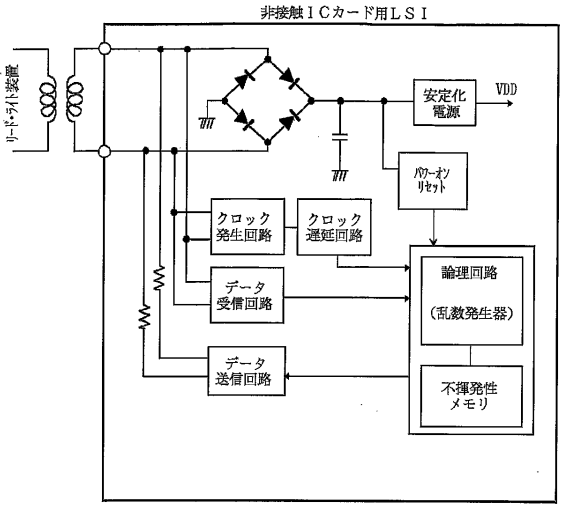
【図３０】

第　３０　図



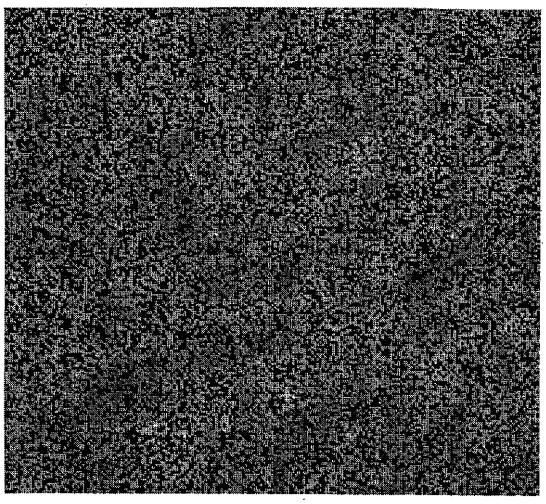
【図３１】

第　３１　図



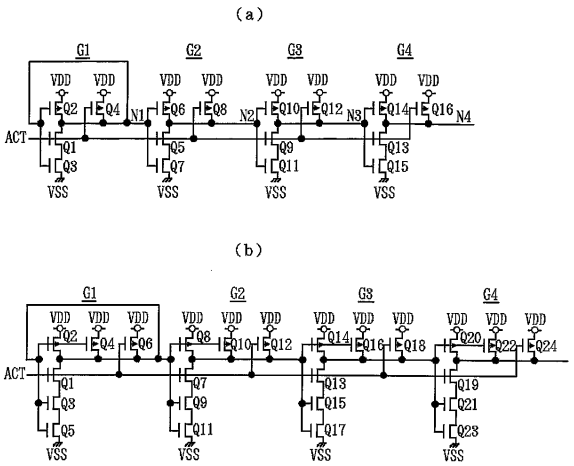
【図３２】

第 ３２ 図



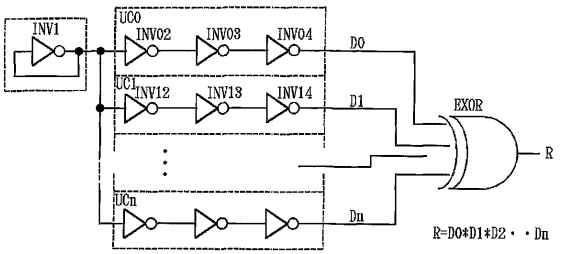
【図３３】

第 ３３ 図



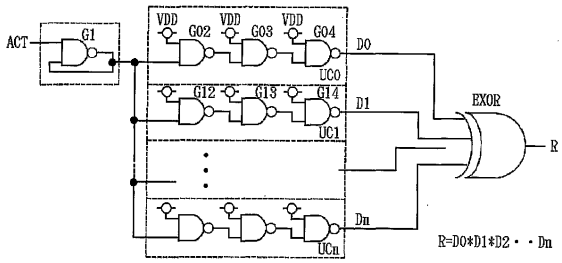
【図３４】

第 ３４ 図



【図３５】

第 ３５ 図



フロントページの続き

(56)参考文献 特開２００３－３３２４５２（ＪＰ，Ａ）
国際公開第０２／０４５１３９（WO，Ａ１）
米国特許第０５９６３１０４（ＵＳ，Ａ）
特開平０１－１１４２１１（ＪＰ，Ａ）
特開２００３－１０８３６３（ＪＰ，Ａ）
特開２００３－１７３２５４（ＪＰ，Ａ）
特表２００３－５２６１５１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 7/58