(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4982750号
(P4982750)
(45)発行日　平成24年7月25日(2012.7.25)　(24)登録日　平成24年5月11日(2012.5.11)

(51)Int.Cl.			F I		
G06F	7/58	(2006.01)	G06F	7/58	A
H03K	3/84	(2006.01)	H03K	3/84	Z
G09C	1/00	(2006.01)	G09C	1/00	650B

請求項の数 4　(全 17 頁)

(21)出願番号　特願2007-11347(P2007-11347)
(22)出願日　平成19年1月22日(2007.1.22)
(65)公開番号　特開2008-176698(P2008-176698A)
(43)公開日　平成20年7月31日(2008.7.31)
審査請求日　平成22年1月21日(2010.1.21)

(73)特許権者　504133110
国立大学法人電気通信大学
東京都調布市調布ケ丘一丁目５番地１
(74)代理人　100083806
弁理士　三好　秀和
(74)代理人　100101247
弁理士　高橋　俊一
(74)代理人　100120455
弁理士　勝　治人
(72)発明者　渡部　信吾
東京都調布市調布ヶ丘１丁目５番地１　国立大学法人　電気通信大学内
(72)発明者　阿部　公輝
東京都調布市調布ヶ丘１丁目５番地１　国立大学法人　電気通信大学内
最終頁に続く

(54)【発明の名称】乱数発生器及び乱数発生器の作成方法

(57)【特許請求の範囲】
【請求項１】
複数の論理素子で構成されるリングオシレータの当該論理素子間のいずれか又は全てに少なくとも一個以上の配線資源からなる遅延回路が設けられているリングオシレータと、
前記リングオシレータの出力に接続され、所定のサンプリング周波数でジッター出力を抽出するサンプリング回路とを備え、
前記論理素子は、プログラム可能な集積回路内に設けられるロジックエレメントで構成され、前記配線資源は、前記集積回路において、前記ロジックエレメント近傍に配置されるローカルインターコネクト、カラム方向に延伸するカラムインターコネクト、及び／又はロウ方向に延伸するロウインターコネクトで構成されることを特徴とする乱数発生器。
【請求項２】
複数の論理素子で構成されるリングオシレータの当該論理素子間のいずれか又は全てに少なくとも一個以上の配線資源からなる遅延回路が設けられている複数のリングオシレータと、
前記複数のリングオシレータの出力に接続され,前記複数のリングオシレータの排他的論理和出力を発生する排他的論理和回路と、
前記排他的論理和回路の出力に接続され,所定のサンプリング周波数でジッター出力を抽出するサンプリング回路とを備え、
前記論理素子は、プログラム可能な集積回路内に設けられるロジックエレメントで構成され、前記配線資源は、前記集積回路において、前記ロジックエレメント近傍に配置され

るローカルインターコネクト、カラム方向に延伸するカラムインターコネクト、及び／又はロウ方向に延伸するロウインターコネクトで構成されることを特徴とする乱数発生器。
【請求項３】
前記サンプリング回路の出力に接続され,前記ジッター出力を加工処理する後処理回路を更に備えることを特徴とする請求項１又は請求項２に記載の乱数発生器。
【請求項４】
複数のロジックエレメントと，当該ロジックエレメントを電気的に接続する配線資源と、当該配線資源の交差点に設けられ、配線切り替えを行うスイッチング素子を少なくとも備えるプログラム可能な集積回路内に乱数発生器を設ける乱数発生器の作成方法において、
前記複数のロジックエレメントを用いて少なくとも一つのリングオシレータを形成するリングオシレータ形成ステップと、
前記リングオシレータを構成する一のロジックエレメントと他のロジックエレメントの間に、少なくとも一つ以上のスイッチング素子を含む一定長の配線資源を設けるジッター生成ステップと、
前記リングオシレータ形成ステップ及びジッター生成ステップにより生成された出力信号を所定のサンプリング周波数でサンプリング抽出するサンプリング抽出ステップと
を有する乱数発生器の作成方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、乱数発生器に関し、特にリングオシレータを基本構成とする真の乱数発生を可能とする乱数発生器及び乱数発生器の作成方法に関する。
【背景技術】
【０００２】
モンテカルロ法などのシミュレーション分野や、暗号およびセキュリティー分野における鍵生成、鍵交換、回路のマスクなどでは、大量の乱数やよく散らばった，乱数性のよい乱数が必要とされることが多い。
【０００３】
乱数には大きく分けて真の乱数と疑似乱数がある。真の乱数とは、予測が不可能で再現性のない乱数のことである。通常は、熱雑音や核分裂などの本質的にランダムな物理的現象を基に乱数を生成し、離散化・符号化の後に後処理をする。このため、アナログ回路を必要とするので、外部回路を付加することが多い。外部に特別な回路が必要となることから、実装の高密度化や低消費電力化，耐タンパー性などの点で問題がある。そのため、外部回路によらず、ＦＰＧＡ（Field Programmable Gate Array）のみを用いて真の乱数を生成する試みがなされている。
【０００４】
例えば、アナログＰＬＬ（Phase locked Loop）を用いて乱数を生成する例では、アナログＰＬＬを搭載しているある特定のＦＰＧＡのみでしか構成できない。
【０００５】
又、ＦＰＧＡの外部に抵抗とコンデンサからなる外部回路を付加して乱数を生成する例では、ＦＰＧＡの製造元やその種類に依存せず乱数を発生することができるが、乱数の生成が外部の回路に依存するため、付加回路が除去されれば乱数の生成が止まること、及び生成する乱数が外部からサンプリング可能であることから、セキュリティーの面で問題点がある。
【０００６】
一方、プログラマブルなデジタル回路であるＦＰＧＡを用い外部回路を要しない真の乱数の生成手法が提案されている（例えば、非特許文献１及び２参照。）。ＦＰＧＡの内部で閉じた回路が構成できるので、耐タンパー性，コストの削減，ＩＰ(Intellectual Property)コアとしての回路の面で有用である。非特許文献１においては、デジタル回路のみ

を用い、複数のリングオシレータによるジッターを基にした乱数生成器を理論的な立場から検討している。非特許文献１においては、ＣＰＬＤ（Complex Programmable Logic Device）やＦＰＧＡも検討しているが実際の評価は行っていない。又、非特許文献２においては、特定の条件に限定した実装を行い評価を行っている。

【０００７】

一方、縦続接続された複数段の論理ゲート出力の一部を帰還抵抗を介して入力側に帰還させて発振する発振部を備え、論理ゲートには、所定の抵抗を介して電源電圧が供給され、所定の抵抗は絶縁層を介して信号線に積層されていることを特徴とする乱数発生集積回路については、既に開示されている（例えば、特許文献１参照。）。

【特許文献１】特許第３６５０８２６号公報

【非特許文献１】ビー・スーナー，ダブリュー・ジェイ・マーティン，及びデイー・アール・スティンソン（B. Suner, W.J.Martin, and D.R.Stinson）著，“証明可能な安全性を有し攻撃耐性を内蔵する真の乱数生成器（A Provably Secure True Random Number Generator with Built-in Tolerance to Active Attacks）”，March 29, 2006,http://www.cacr.math.uwaterloo.ca/~dstinson/papers/rng-IEEE.pdf

【非特許文献２】ディー・シェレケンス,ビィー・プレニール，及びアイ・ベルボウヘーデ（D.Schellekens, B. Preneel, and I. Verbauwhede）著，“ＦＰＧＡベンダーに依存しない真の乱数生成器（FPGA vendor agnostic True Random Number Generator）”，Proc. 16th International Conference on Field Programmable Logic and Applications (FPL 2006), August 28-30, セッションM3.A Cryptographic Applications , http://www.cosic.esat.kuleuven.be/publications/article-790.pdf

【発明の開示】

【発明が解決しようとする課題】

【０００８】

本発明は、積極的に配線資源による遅延回路 を導入し、配線資源のジッターも利用するリングオシレータによる真の乱数発生器及び乱数発生器の作成方法を提供することを目的とする。

【０００９】

また本発明は、プログラム可能な集積回路において、積極的に配線資源による遅延回路 を導入し、配線資源のジッターも利用するリングオシレータによる真の乱数発生器及び乱数発生器の作成方法を提供することを目的とする。

【課題を解決するための手段】

【００１０】

上記目的を達成するための本発明の請求項１に記載の乱数発生器は、 複数の論理素子で構成されるリングオシレータの当該論理素子間のいずれか又は全てに少なくとも一個以上の配線資源からなる遅延回路が設けられているリングオシレータと、前記リングオシレータの出力に接続され、所定のサンプリング周波数でジッター出力を抽出するサンプリング回路とを備え、前記論理素子は、プログラム可能な集積回路内に設けられるロジックエレメントで構成され、前記配線資源は、前記集積回路において、前記ロジックエレメント近傍に配置されるローカルインターコネクト、カラム方向に延伸するカラムインターコネクト、及び／又はロウ方向に延伸するロウインターコネクトで構成されることを特徴とする。

【００１１】

本発明の請求項２に記載の乱数発生器は、複数の論理素子で構成されるリングオシレータの当該論理素子間のいずれか又は全てに少なくとも一個以上の配線資源からなる遅延回路が設けられている複数のリングオシレータと、前記複数のリングオシレータの出力に接続され,前記複数のリングオシレータの排他的論理和出力を発生する排他的論理和回路と、前記排他的論理和回路の出力に接続され,所定のサンプリング周波数でジッター出力を抽出するサンプリング回路とを備え、前記論理素子は、プログラム可能な集積回路内に設けられるロジックエレメントで構成され、前記配線資源は、前記集積回路において、前記

ロジックエレメント近傍に配置されるローカルインターコネクト、カラム方向に延伸するカラムインターコネクト、及び／又はロウ方向に延伸するロウインターコネクトで構成されることを特徴とする。

【００１３】

本発明の請求項３に記載の乱数発生器は、請求項１又は請求項２に記載の乱数発生器において、前記サンプリング回路の出力に接続され,前記ジッター出力を加工処理する後処理回路を更に備えることを特徴とする。

【００１４】

本発明の請求項４に記載の乱数発生器の作成方法は、複数のロジックエレメントと，当該ロジックエレメントを電気的に接続する配線資源と，当該配線資源の交差点に設けられ，配線切り替えを行うスイッチング素子を少なくとも備えるプログラム可能な集積回路内に乱数発生器を設ける乱数発生器の作成方法において、前記複数のロジックエレメントを用いて少なくとも一つのリングオシレータを形成するリングオシレータ形成ステップと、前記リングオシレータを構成する一のロジックエレメントと他のロジックエレメントの間に、少なくとも一つ以上のスイッチング素子を含む一定長の配線資源を設けるジッター生成ステップと、前記リングオシレータ形成ステップ及びジッター生成ステップにより生成された出力信号を所定のサンプリング周波数でサンプリング抽出するサンプリング抽出ステップとを有する乱数発生器の作成方法。

【発明の効果】

【００１５】

本発明の乱数発生器及び乱数発生器の作成方法によれば、真の乱数を発生することができる。

【発明を実施するための最良の形態】

【００１６】

次に、図面を参照して、本発明の実施の形態を説明する。以下の図面の記載において、同一又は類似の部分には同一又は類似の符号を付している。ただし、図面は模式的なものであり、現実のものとは異なることに留意すべきである。又、図面相互間においても互いの寸法の関係や比率が異なる部分が含まれていることはもちろんである。

【００１７】

また、以下に示す実施の形態は、この発明の技術的思想を具体化するための装置や方法を例示するものであって、この発明の技術的思想は、各構成部品の配置などを下記のものに特定するものでない。この発明の技術的思想は、特許請求の範囲において、種々の変更を加えることができる。

【００１８】

[第１実施形態]

本発明の第１の実施の形態に係る乱数発生器は、複数の論理素子で構成されるリングオシレータの当該論理素子間のいずれか又は全てに少なくとも一個以上の配線資源からなる遅延回路が設けられているリングオシレータと、リングオシレータの出力に接続され、所定のサンプリング周波数でジッター出力を抽出するサンプリング回路とを備える。

【００１９】

リングオシレータとは、複数のゲートをリング状につなぎ発振させる回路である。通常、奇数段のＮＯＴゲートQ_1，Q_2,…，Q_{2n+1}（ここで、ｎは、１以上の整数）を図1（ａ）のように構成する。リングオシレータによる発振器は温度や外部の状況などの影響を強く受け、水晶発振器などと比べると不安定であり、ジッターが大きい。

【００２０】

本発明の第１の実施の形態に係る乱数発生器においては、図1（ｂ）に示すように、奇数段のＮＯＴゲートQ_1，Q_2,…，Q_{2n+1}に加えて、このジッターの発生源として、積極的に配線資源による遅延回路D_nを導入し、乱数発生に利用する。

【００２１】

本発明の第１の実施の形態に係るリングオシレータによる真の乱数発生回路は、図１（

ｃ）に示すように、ノイズソース部１４とノイズソースの偏りやビットレートの調整などを行う後処理部１６からなる。

【００２２】

ノイズソース部１４は、単位時間当たりのジッターの割合を増やすために複数のリングオシレータの出力を排他的論理和で束ねてもよく、そのため、図１（ｃ）に示す構成例では、排他的論理和リングオシレータ１０を備える。更に、一定時間間隔で乱数を発生するため、一定周波数で排他的論理和リングオシレータ１０出力をサンプリングするためのサンプリング回路１２を備える。複数のリングオシレータの代わりに、図1（ｂ）に示すように、単一のリングオシレータを用いてもよい。

【００２３】

図２は、リングオシレータによる真の乱数発生回路において、図1（ａ）に示すように、積極的に配線資源による遅延回路D_nを導入しない場合のリングオシレータ（タイプＡ：比較例）の発振波形と、図1（ｂ）に示すように、積極的に配線資源による遅延回路D_nを導入した場合のリングオシレータ（タイプＢ：本発明）の発振波形との比較を模式的に示す。

【００２４】

図２中には、サンプリング波形も示されている。本発明の第１の実施の形態に係るリングオシレータによる真の乱数発生回路においては、積極的に配線資源による遅延回路D_nを導入することによって、ジッター間隔を、$j_1 > j_0$と増大するとともに、発振周期も$T_1 > T_0$と増加し、発振周期に対するジッター間隔の割合も、$j_1 / T_1 > j_0 / T_0$となり増大する。

【００２５】

図３は、本発明の第１の実施の形態に係る乱数発生器において、単位時間当たりのジッターの割合を増やすためにノイズソース部１４において、３個のリングオシレータの出力を排他的論理和回路１８で束ねて、全信号中のジッターの割合を増加する波形例を模式的に示す。図３（ａ）乃至図３（ｃ）に示す個々のリングオシレータの出力を、排他的論理和回路１８で束ねて図３（ｄ）に示すように、ジッター間隔、ジッター割合の増大した出力波形を得ることができる。

【００２６】

図４乃至図５は本発明の第１の実施の形態に係る乱数発生回路において、リングオシレータの構成の各種変形例を示す。

【００２７】

図４（ａ）は、３段のＮＯＴゲートQ_1，Q_2，Q_3と遅延回路D_1からなるリングオシレータを示す。図４（ｂ）は、３段のＮＯＴゲートQ_1，Q_2，Q_3と遅延回路D_1，D_2からなるリングオシレータを示す。図４（ｃ）も、３段のＮＯＴゲートQ_1，Q_2，Q_3と遅延回路D_1，D_2からなるリングオシレータを示し、遅延回路D_1，D_2の配置を変更した例を示す。

【００２８】

図５（ａ）は、複数の奇数段のＮＯＴゲート・・・Q_{n-1}，Q_n，Q_{n+1}，・・・と各々のＮＯＴゲートに対応する遅延回路・・・D_{n-1}，D_n，D_{n+1}，・・・からなるリングオシレータを示す。図５（ｂ）は、図５（ａ）のＮＯＴゲート・・・Q_{n-1}，Q_n，Q_{n+1}，・・・の各々をｐチャネルトランジスタQ_A、及びｎチャネルトランジスタQ_BからなるＣＭＯＳインバータによって構成した例を示す。各々のＣＭＯＳインバータは電源電圧V_{DD}と接地電位間に接続され、かつ各々のＣＭＯＳインバータ間には、遅延回路・・・D_{n-1}，D_n，D_{n+1}，・・・が接続されている。

【００２９】

ここで、配線資源とは、集積回路内の配線のみならず、バッファ回路、ＮＯＴゲート間のルート選択により、中間に介在する複数の論理素子（ロジックエレメント）、スイッチ回路なども含まれる。

【００３０】

又、ＮＯＴゲートQ_1，Q_2,…，Q_{2n+1}は単なるインバータのみならず、ロジックアレイ内，ゲートアレイ内，プログラマブルゲートアレイ内，或いは図９乃至図１６において詳述するＦＰＧＡ内などの論理素子（ロジックエレメント）も含まれる。

【００３１】

又、ＮＯＴゲートには、単純な１入力１出力のＮＯＴゲート以外にも、２入力１出力のＮＡＮＤゲートの入力をつなげて１入力として用いた場合なども含まれ、更に又、排他的論理和（ＸＯＲ）ゲートなども利用可能である。

【００３２】

従って、配線資源には、これらの集積回路内の配線のみならず、このようなロジックアレイ内，ゲートアレイ内，プログラマブルゲートアレイ内，或いはＦＰＧＡ内などの論理素子（ロジックエレメント）間のルート選択により、中間に介在する複数のバッファ回路、複数の論理素子、スイッチ回路なども含まれる。

【００３３】

従って、本発明の実施の形態に係る乱数発生器に適用されるリングオシレータは、単なるインバータチェーンのみならず、積極的に配線資源を介在し、ロジックアレイ内，ゲートアレイ内，プログラマブルゲートアレイ内，或いはＦＰＧＡ内などの論理素子（ロジックエレメント）間をリング状に接続した回路構成も含まれる。

【００３４】

本発明の第１の実施の形態に係る乱数発生器によれば、積極的に配線資源による遅延回路 を導入し、配線資源のジッターも利用するリングオシレータによる真の乱数発生器を提供することができる。

【００３５】

[第２実施形態]

本発明の第２の実施の形態に係る乱数発生器は、複数の論理素子で構成されるリングオシレータの当該論理素子間のいずれか又は全てに少なくとも一個以上の配線資源からなる遅延回路が設けられている複数のリングオシレータと、複数のリングオシレータの出力に接続され,複数のリングオシレータの排他的論理和出力を発生する排他的論理和回路と、排他的論理和回路の出力に接続され,所定のサンプリング周波数でジッター出力を抽出するサンプリング回路とを備える。

【００３６】

図６は、本発明の比較例に係る乱数発生器の模式的回路構成を示す。ノイズソース部について示されており、後処理部については、省略している。

【００３７】

図６に示す比較例に係る乱数発生器では、図１（ａ）に示すリングオシレータの基本回路構成例を複数配置し、複数のリングオシレータの出力を排他的論理和回路１８で束ねる。更に、排他的論理和回路１８の出力信号を、Ｄタイプフリップフロップ回路（Ｄ－ＦＦ）２０に入力し、一定時間間隔で乱数を発生させるため、一定の周波数でサンプリングし、乱数出力を得る。ここで、図６に示すように、リングオシレータの長さをｌ、リングオシレータの数をｋ、サンプリング周波数をf_Sと定義する。

【００３８】

図７は、本発明の第２の実施の形態に係る乱数発生器の模式的回路構成を示す。ノイズソース部について示されており、後処理部については、省略している。

【００３９】

図７に示す本発明の第２の実施の形態に係る乱数発生器では、図４（ｃ）に示す本発明の第１の実施の形態に係る乱数発生器に適用したリングオシレータと同様の構成例をｋ個配置し、ｋ個のリングオシレータの出力を排他的論理和回路１８で束ねる。更に、排他的論理和回路１８の出力信号を、Ｄタイプフリップフロップ回路（Ｄ－ＦＦ）２０に入力し、一定時間間隔で乱数を発生させるため、サンプリング周波数f_Sでサンプリングし、乱数出力を得る。図７において、A_1，A_2，…，A_k、B_1，B_2，，B_k、及びC_1，C_2，…，C_kと表示する２３は、いずれもＮＯＴゲートを示す。ＩＣと表示する２２は、インタ

ーコネクトであり、配線資源を示す。

【００４０】

図８は、本発明の第２の実施の形態の変形例に係る乱数発生器の模式的回路構成を示す。図８に示す例では、図５（ａ）に示す本発明の第１の実施の形態に係る乱数発生器に適用したリングオシレータと同様の構成例をｋ個配置し、ｋ個のリングオシレータの出力を排他的論理和回路１８で束ねる。更に、排他的論理和回路１８の出力信号を、Ｄタイプフリップフロップ回路（Ｄ－ＦＦ）２０に入力し、一定時間間隔で乱数を発生させるため、サンプリング周波数f_Sでサンプリングし、乱数出力を得る。図８において、N_{11}，N_{21}，…，N_{k1}、N_{12}，N_{22}，…，N_{k2}、…及びN_{1n}，N_{2n}，…，N_{kn}と表示する２３は、いずれもＮＯＴゲートを示す。ＩＣと表示する２２は、インターコネクトであり、配線資源を示すことは図７と同様である。

【００４１】

本発明の第２の実施の形態に係る乱数発生器によれば、積極的に配線資源による遅延回路 を導入し、配線資源のジッターも利用するリングオシレータを並列化構成して、ジッター量を増加した真の乱数発生器を提供することができる。

【００４２】

[第３実施形態]

（ＦＰＧＡ）

本発明の第３の実施の形態に係る乱数発生器は、ＦＰＧＡのみを用いる例を示す。ＦＰＧＡのみを用いて真の乱数を生成するには、第１の実施の形態に係る乱数発生器に示すように、リングオシレータを用いる。しかも、必要とされる乱数性を得るために多数のリングオシレータを必要とするが、回路コストの増加を抑制するために、本発明の第３の実施の形態に係る乱数発生器においては、リングオシレータの一部に、乱数の基となるジッターを発生させる配線資源（インターコネクト）による遅延回路を積極的に導入し、真の乱数発生に利用する。

【００４３】

ＦＰＧＡの資源はルックアップテーブルやレジスタを含む論理素子資源と配線資源からなる。例えば、ＦＰＧＡの基本単位は、図９に示すように、最小の回路単位であるロジックエレメント（ＬＥ）２４が１０個まとまったロジックアレイブロック（ＬＡＢ）２５と、ＬＡＢ２５の周囲に配置されるローカルインターコネクト２６と、ローカルインターコネクト２６及びＬＡＢ２５の周囲に配置され，カラム方向に延伸するカラムインターコネクト（ＣＬ）２７と、同じくローカルインターコネクト２６及びＬＡＢ２５の周囲に配置され，ロウ方向に延伸するロウインターコネクト（ＲＬ）２８とを備える。

【００４４】

ローカルインターコネクト２６、カラムインターコネクト（ＣＬ）２７及びロウインターコネクト（ＲＬ）２８によって、ＦＰＧＡにおけるプログラマブルな配線を実現することができる。カラムインターコネクト（ＣＬ）２７及びロウインターコネクト（ＲＬ）２８の交点には、トランジスタによるスイッチが配置されており、そこにはジッターが存在し得る。

【００４５】

本発明の第３の実施の形態に係る乱数発生器は、ＦＰＧＡの最小の回路単位であるロジックエレメント（ＬＥ）２４をＮＯＴゲートとし、リングオシレータのＮＯＴゲートの間に、ローカルインターコネクト２６、カラムインターコネクト（ＣＬ）２７及びロウインターコネクト（ＲＬ）２８などによって構成される配線資源（インターコネクト）を挿入する。このように構成することで、発振波形のジッターを増加することができる。

【００４６】

例えば、配線資源（インターコネクト）を積極的に導入しない場合には、ＬＡＢ２５内のＬＥ２４を個々のＮＯＴゲートとして構成し、それぞれをリング状に接続したものを並列化することで、図６に示す比較例に係る乱数発生器と同様の乱数発生器を構成することができる。

【００４７】
一方、配線資源（インターコネクト）を積極的に導入する場合には、例えば、図１０に示すように、ＩＮＶ１、ＩＮＶ２、及びＩＮＶ３で示される別々のＬＡＢ２５内のＬＥ２４を個々のＮＯＴゲートとして構成し、その間を点線及び実線で示すように、配線資源（インターコネクト）でリング状に接続したものを並列化することで、図７に示すに本発明の第２の実施の形態に係る乱数発生器と同様の乱数発生器をＦＰＧＡ上において構成することができる。すなわち、図７に示すように、リングオシレータの長さｌ＝３とし、インターコネクト（ＩＣ）２２を２箇所に挿入したリングオシレータを並列化した構成例を、ＦＰＧＡを用いて実現することができる。ＦＰＧＡは、図１１に示すように、マトリックス状に配置された複数のＬＡＢ２５と、カラム方向に延伸する複数のカラムインターコネクト…，CL_{i-4}，CL_{i-3}，CL_{i-2}，CL_{i-1}，CL_{i}，CL_{i+1}，CL_{i+2}，…と、ロウ方向に延伸する複数のロウインターコネクト…，RL_{i-1}，RL_{i}，RL_{i+1}，…を備える。従って、ＮＯＴゲート間の配線資源（インターコネクト）は、ＦＰＧＡ上のカラムインターコネクト、ロウインターコネクトの経路選択により任意に選定することができる。図１１においては、ローカルインターコネクト２６については省略されている。

【００４８】
リングオシレータの数ｋは、例えば、配線資源（インターコネクト）による遅延回路を積極的に導入しない場合には、ｋ＝１１０～２１０であるのに対して、配線資源（インターコネクト）による遅延回路を積極的に導入した場合には、例えば、ｋ＝１１０よりも減少することができる。

【００４９】
比較例に係る乱数発生器と配線資源（インターコネクト）を有効活用する本発明の第３の実施の形態に係る乱数発生器を比較する。

【００５０】
比較例に係る乱数発生器は、図６に示すようにリングオシレータを構成し、各リングオシレータの長さをｌ＝３、リングオシレータの数をｋ＝２０としたものである。２０個のリングオシレータの出力の排他的論理和をサンプリング周波数f_S＝５０ＭＨｚでサンプリングし、乱数生成器の出力を得る。

【００５１】
本発明の第３の実施の形態に係る乱数発生器の具体的な配置構成例を図１２及び図１３に示す。図１３は、図１２の経路選択を説明するために、ＦＰＧＡ上における詳細な配置構成例を示す。図１２及び図１３中のＡ，Ｂ，Ｃはそれぞれ１つのＮＯＴゲートに対応し、Ｂをひとつだけ離すことで、Ａ－Ｂ間、Ｂ－Ｃ間にインターコネクトを挿入している。

【００５２】
図１２及び図１３の例では、Ａ－Ｂ間に１．３６５ｎｓの配線遅延をもつインターコネクトを、Ｂ－Ｃ間に１．３３４ｎｓの配線遅延をもつインターコネクトを挿入している。この配線遅延は、図１３に示すように、ロウインターコネクト３単位分、カラムインターコネクト３単位分の和に相当する。Ｃ－Ａ間の配線遅延は、同一のＬＡＢ２５内であることから、０．３６７ｎｓと小さい。

【００５３】
（乱数発生器の作成方法）
本発明の第３の実施の形態に係る乱数発生器の作成方法は、例えば、以下の通りである。

【００５４】
複数のＬＥ２４と,当該ＬＥ２４を電気的に接続する配線資源（インターコネクト）と，当該配線資源（インターコネクト）の交差点に設けられ，配線切り替えを行うスイッチング素子を少なくとも備えるプログラム可能な集積回路内に乱数発生器を設ける乱数発生器の作成方法において、（ａ）複数のＬＥ２４を用いて少なくとも一つのリングオシレータを形成するリングオシレータ形成ステップと、（ｂ）リングオシレータを構成する一のＬＥ２４と他のＬＥ２４の間に、少なくとも一つ以上のスイッチング素子を含む一定長の

配線資源を設けるジッター生成ステップと、（ｃ）リングオシレータ形成ステップ及びジッター生成ステップにより生成された出力信号を所定のサンプリング周波数f_Sでサンプリング抽出するサンプリング抽出ステップとを有する。

【００５５】

（乱数性評価の方法）

乱数発生器の評価は、回路面積や生成速度、生成される乱数の乱数性により行うことができる。回路面積は、ＦＰＧＡの必要とされるＬＥ２４によって決定され、生成速度は、回路動作周波数によって決定される。乱数性は、種々の統計テストから評価される。

【００５６】

本発明の第３の実施の形態に係る乱数発生器の評価においては、ＮＩＳＴＳＰ８００－２２（http://csrc.nist.gov/publications/nistpubs/index.html: A Statistical Test Suite for Random and Pseudo-random Number Generators for Cryptographics Applications）に示される１５種類の検定を行った。検定には、図６と同様に比較例の回路構成の場合と、

図７と同様に本発明の実施の形態に係る回路構成の場合を、それぞれについて１０００サンプル（１サンプル当たり１，０００，０００ビット）で比較した。乱数テストで用いたパラメータは、図１４に示すとおりである。パラメータｌ＝３，ｋ＝２０，f_S＝５０ＭＨｚは同一とした。

【００５７】

通常、真の乱数生成器は、より乱数性のよい乱数を生成するために、図１（ｃ）に示したように、後処理部１６を用いるが、ここでは、配線資源（インターコネクト）を追加したことによる乱数性の違いを見るために、後処理部１６を介さず、乱数生成出力をそのまま直接ＮＩＳＴＳＰ８００－２２にかけ、統計的性質を調べた。

【００５８】

（乱数性評価結果）

回路面積については、比較例に係る乱数発生器、本発明の第３の実施の形態に係る乱数発生器ともに、ＬＥ数６７であった。生成速度については、比較例に係る乱数発生器、本発明の第３の実施の形態に係る乱数発生器ともに、サンプリング周波数f_S＝５０ＭＨｚより５０Ｍｂｐｓであった。

【００５９】

乱数性の評価結果を図１５に示す。図１５はそれぞれの検定項目に対して有意確率（p-value）を計算し、その値の分布度合い（一様性）と検定合格率（比率）をまとめたものである。図１５において、各検定につき、○は合格、×は不合格を意味する。Non-overlapping Template検定については、テンプレートサイズが９の時、１４８種のテンプレートに対して行った結果を合格、不合格の個数で表している。

【００６０】

図１５から明らかなように、比較例に係る乱数発生器、本発明の第３の実施の形態に係る乱数発生器ともに多くの検定に合格していない。これは前述のように、リングオシレータの個数ｋは２０個であり、生成されるジッターの割合が少ないためである。しかしながら、配線資源（インターコネクト）を用いる本発明の第３の実施の形態に係る乱数発生器においては、明らかに比較例に係る乱数発生器よりも乱数性は増加していることがわかる。

【００６１】

本発明の第３の実施の形態に係る乱数発生器において、Non-overlapping Template検定の結果の詳細は、図１６に示すように表される。図１６は、同検定の１４８種類のテンプレートの内、異なる検定結果をもたらす場合を抜き出したものである。図１６から明らかなように、比較例に係る乱数発生器においては合格しなかった多くのテンプレート検定が、本発明の第３の実施の形態に係る乱数発生器においては合格していることがわかる。

【００６２】

又、図１６において、離散フーリエ変換（ＤＦＴ：Discrete Fourier transform）やSe

rial 2の検定では、比較例に係る乱数発生器、本発明の第３の実施の形態に係る乱数発生器ともに合格しなかったが、本発明の第３の実施の形態に係る乱数発生器の合格比率（PROPORTION）は向上していることがわかる。

【００６３】

アプリケーションによっては、ＦＰＧＡ上の配線資源（インターコネクト）に余剰が生ずる場合もある。このため、この余剰の配線資源（インターコネクト）を有効に活用することで、回路設計の自由度を向上することができる。

【００６４】

本発明の第３の実施の形態に係る乱数発生器によれば、ＦＰＧＡ上において、配線資源（インターコネクト）を積極的に活用し、リングオシレータによる真の乱数発生器を構成することができる。

【００６５】

[その他の実施の形態]

上記のように、本発明は第１乃至第３の実施の形態によって記載したが、この開示の一部をなす論述及び図面はこの発明を限定するものであると理解すべきではない。この開示から当業者には様々な代替実施の形態、実施例及び運用技術が明らかとなろう。

【００６６】

特に、本発明の第３の実施の形態に係る乱数発生器においては、ＦＰＧＡを適用する例を開示しているが、ＦＰＧＡに限定されるものではない。ゲートアレイ、ロジックアレイ、プログラマブルロジックアレイ或いはＡＳＩＣなどを用いても、同様に配線資源（インターコネクト）を積極的に活用することで、ジッターの増大した真の乱数発生器を構成することができる。

配線資源（インターコネクト）には、集積回路内の配線のみならず、ＮＯＴゲート間のルート選択により、中間に介在する複数の論理素子、スイッチ回路なども含まれる。又、ＮＯＴゲートは単なるインバータのみならず、ロジックアレイ内，ゲートアレイ内，或いはＦＰＧＡ内のロジックエレメントなども含まれる。従って、配線資源（インターコネクト）には、これらの集積回路内の配線のみならず、このようなロジックアレイ内，ゲートアレイ内，或いはＦＰＧＡ内のロジックエレメント間のルート選択により、中間に介在する複数の論理素子、スイッチ回路なども含まれる。

【００６７】

従って、本発明の実施の形態に係る乱数発生器に適用されるリングオシレータは、単なるインバータチェーンのみならず、積極的に配線資源を介在し、ロジックアレイ内，ゲートアレイ内，或いはＦＰＧＡ内のロジックエレメント間をリング状に接続した回路構成も含まれる。

【００６８】

従って、所望の長さｌ、所定の個数ｋ、所定のサンプリング周波数f_Sを有する本発明の実施の形態に係る真の乱数発生器を所望のＡＳＩＣとして構成することもできる。

【００６９】

このように、本発明はここでは記載していない様々な実施の形態などを含むことは勿論である。したがって、本発明の技術的範囲は上記の説明から妥当な特許請求の範囲に係る発明特定事項によってのみ定められるものである。

【００７０】

[乱数発生器の使用方法]

本発明の実施の形態に係る乱数発生器は、例えば、鍵生成、鍵交換、回路のマスク、パチンコの確率変動等に用いることが可能である。これら鍵生成等に本乱数発生器を用いることにより、プログラム可能な集積回路の限られた資源を有効利用しつつ、真の乱数による鍵生成、鍵交換、回路のマスク、パチンコの確率変動等を行うことができる。

【００７１】

又、本発明の実施の形態では乱数発生器として説明をしているが、この乱数発生器からサンプリング回路を除くことにより、単なるジッター発生器として利用することが可能で

ある。この場合、本ジッター発生器は、ジッターを測定するジッター測定装置において、測定精度を検査するために用いるサンプル用のジッター発生器として用いることが可能である。

【図面の簡単な説明】

【００７２】

【図１】（ａ）リングオシレータの基本回路構成例。（ｂ）本発明の第１の実施の形態に係る乱数発生器を構成するリングオシレータの基本回路構成例。（ｃ）本発明の第１の実施の形態に係る乱数発生器の模式的ブロック構成図。

【図２】リングオシレータによる真の乱数発生回路において、積極的に配線資源による遅延回路D_nを導入しない場合のリングオシレータ（タイプＡ：比較例）の発振波形図と、積極的に配線資源による遅延回路D_nを導入した場合のリングオシレータ（タイプＢ：本発明）の発振波形図、及びサンプリング波形図。

【図３】本発明の第１の実施の形態に係る乱数発生器において、単位時間当たりのジッターの割合を増やすためにノイズソース部において、３個のリングオシレータの出力を排他的論理和回路で束ねて、全信号中のジッターの割合を増加する波形例を模式的に示す図であって、図３（ａ）乃至図３（ｃ）：個々のリングオシレータの出力波形図、図３（ｄ）：排他的論理和回路出力波形図。

【図４】（ａ）本発明の第１の実施の形態に係る乱数発生器を構成するリングオシレータの別の構成例。（ｂ）本発明の第１の実施の形態に係る乱数発生器を構成するリングオシレータの更に別の構成例。（ｃ）本発明の第１の実施の形態に係る乱数発生器を構成する更に別のリングオシレータの構成例。

【図５】（ａ）本発明の第１の実施の形態に係る乱数発生器を構成する更に別のリングオシレータの構成例。（ｂ）本発明の第１の実施の形態に係る乱数発生器を構成する更に別のリングオシレータの構成例。

【図６】本発明の比較例に係る乱数発生器の構成例。

【図７】本発明の第２の実施の形態に係る乱数発生器の構成例。

【図８】本発明の第２の実施の形態の変形例に係る乱数発生器の構成例。

【図９】本発明の第３の実施の形態に係る乱数発生器に適用するＦＰＧＡの内部回路構成図。

【図１０】本発明の第３の実施の形態に係る乱数発生器に適用するＦＰＧＡの内部回路構成例。

【図１１】本発明の第３の実施の形態に係る乱数発生器に適用するＦＰＧＡのＬＡＢの配置構成図。

【図１２】本発明の第３の実施の形態に係る乱数発生器に適用するＦＰＧＡの中の回路位置図。

【図１３】本発明の第３の実施の形態に係る乱数発生器に適用するＦＰＧＡの中の詳細回路位置図。

【図１４】本発明の第３の実施の形態に係る乱数発生器において、ＮＩＳＴＳＰ８００－２２の統計テストで用いるパラメータ。

【図１５】本発明の第３の実施の形態に係る乱数発生器において、ＮＩＳＴＳＰ８００－２２による検査結果。

【図１６】本発明の第３の実施の形態に係る乱数発生器において、Non-overlapping Template検定の結果。

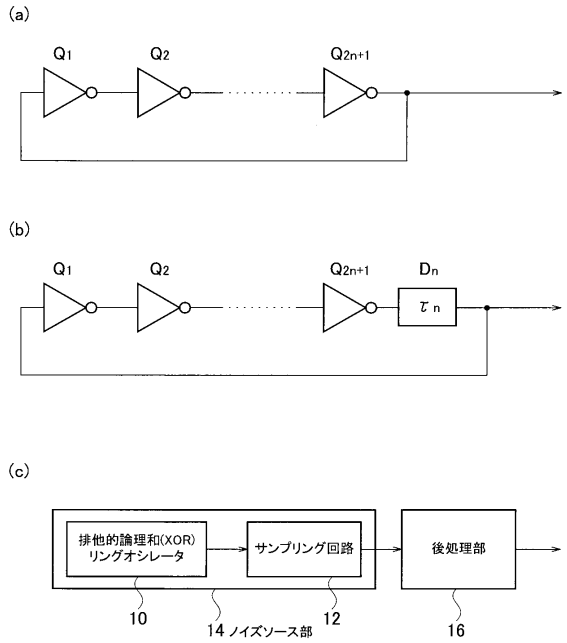
【符号の説明】

【００７３】

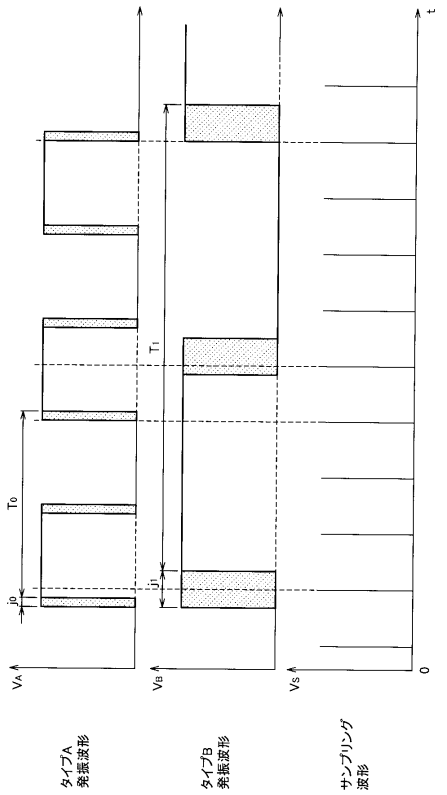
１０…排他的論理和リングオシレータ
１２…サンプリング回路
１４…ノイズソース部
１６…後処理部
１８…排他的論理和回路（ＸＯＲ）

２０…Ｄタイプフリップフロップ（Ｄ－ＦＦ）
２２…インターコネクト（ＩＣ）
２３…ＮＯＴゲート
２４…ロジックエレメント（ＬＥ）
２５…ロジックアレイブロック（ＬＡＢ）
２６…ローカルインターコネクト
２７，…，CL_{i-4}，CL_{i-3}，CL_{i-2}，CL_{i-1}，CL_i，CL_{i+1}，CL_{i+2}，……カラムインターコネクト
２８，…，RL_{i-1}，RL_i，RL_{i+1}，……ロウインターコネクト
Q_1，Q_2，…，Q_{n-1}，Q_n，Q_{n+1}，…，Q_{2n+1}…、A_1，A_2，…，A_k、B_1，B_2，，B_k、及びC_1，C_2，…，C_k、N_{11}，N_{21}，…，N_{k1}、N_{12}，N_{22}，…，N_{k2}、…及びN_{1n}，N_{2n}，…，N_{kn}…ＮＯＴゲート
Q_A…ｐチャネルＭＯＳトランジスタ
Q_B…ｎチャネルＭＯＳトランジスタ
D_1，D_2，…，D_{n-1}，D_n，D_{n+1}…遅延回路
τ_1，τ_2，…，τ_{n-1}，τ_n，τ_{n+1}…遅延時間
T_0，T_1…周期
j_0，j_1…ジッター間隔

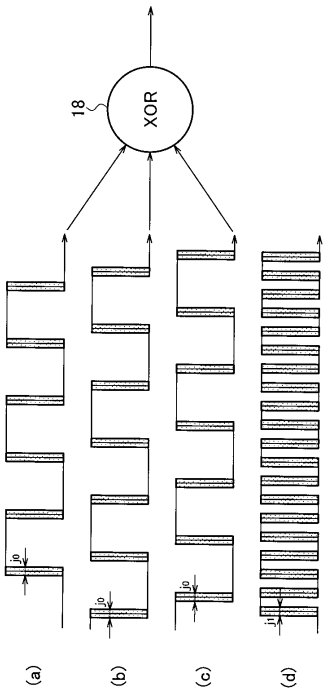
【図１】



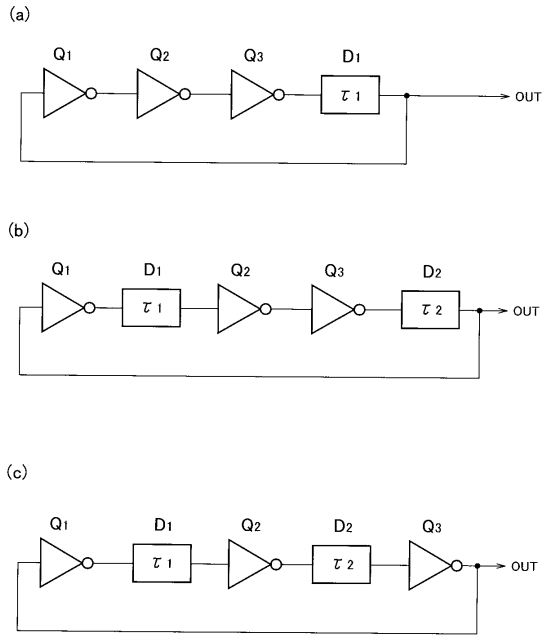
【図２】



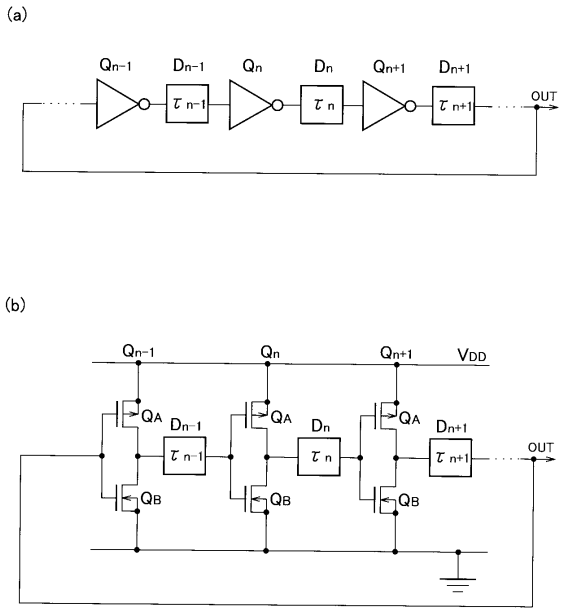
【図３】


18
XOR
(a)
(b)
(c)
(d)

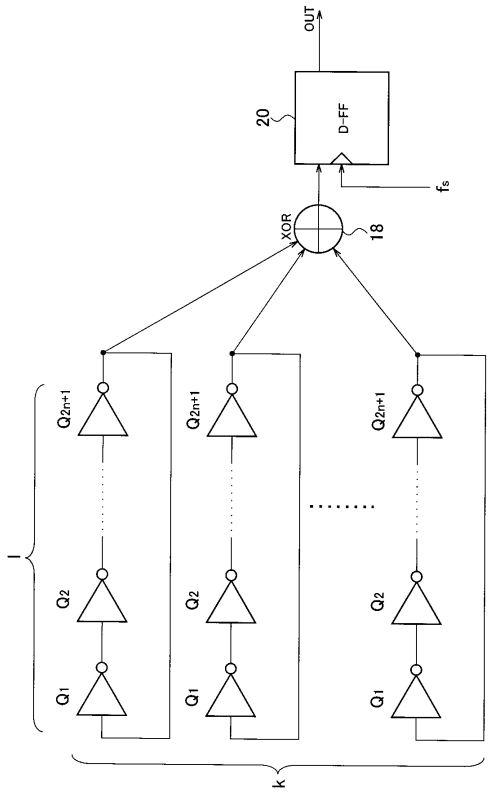
【図４】


(a)
Q1
Q2
Q3
D1
τ 1
OUT
(b)
Q1
D1
Q2
Q3
D2
τ 1
τ 2
OUT
(c)
Q1
D1
Q2
D2
Q3
τ 1
τ 2
OUT

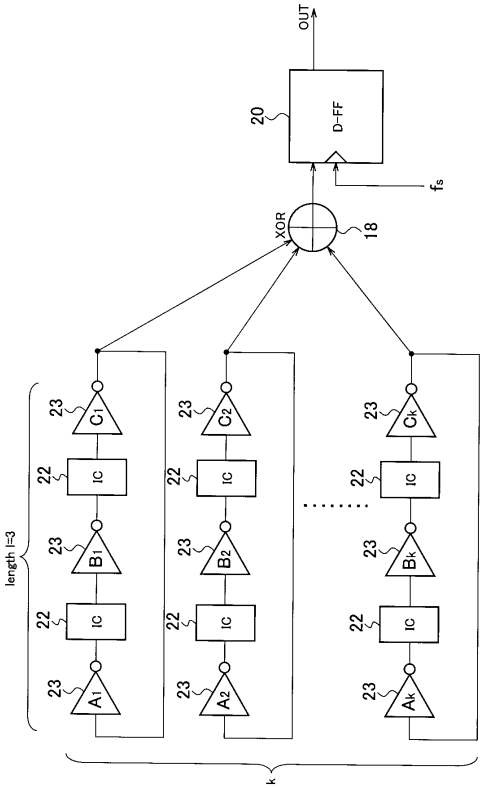
【図５】


(a)
Qn-1
Dn-1
Qn
Dn
Qn+1
Dn+1
τ n-1
τ n
τ n+1
OUT
(b)
Qn-1
Qn
Qn+1
VDD
QA
QB
Dn-1
Dn
Dn+1
τ n-1
τ n
τ n+1
OUT

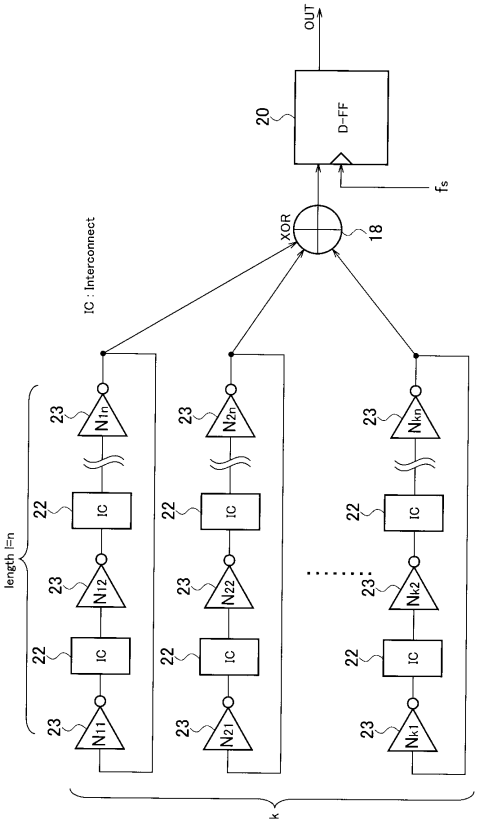
【図６】


OUT
20
D-FF
fs
XOR
18
Q2n+1
Q2
Q1
l
k

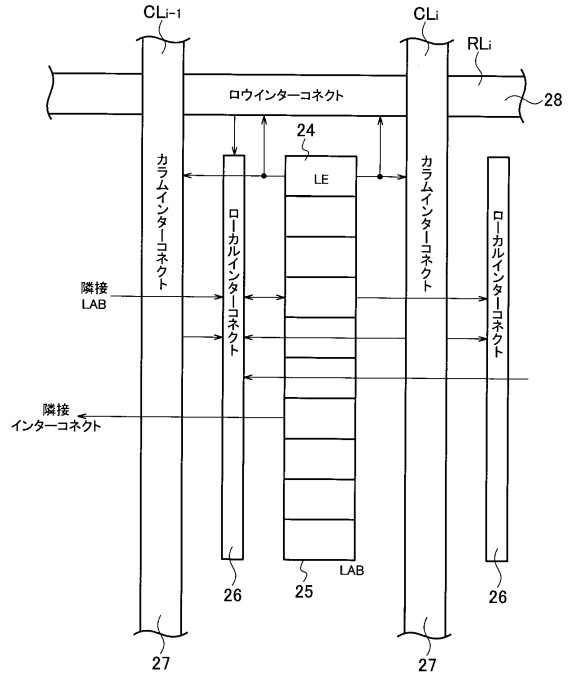
【図７】


OUT
20
D-FF
f_s
XOR
18
length l=3
IC
C_1
C_2
C_k
B_1
B_2
B_k
A_1
A_2
A_k
22
23
k

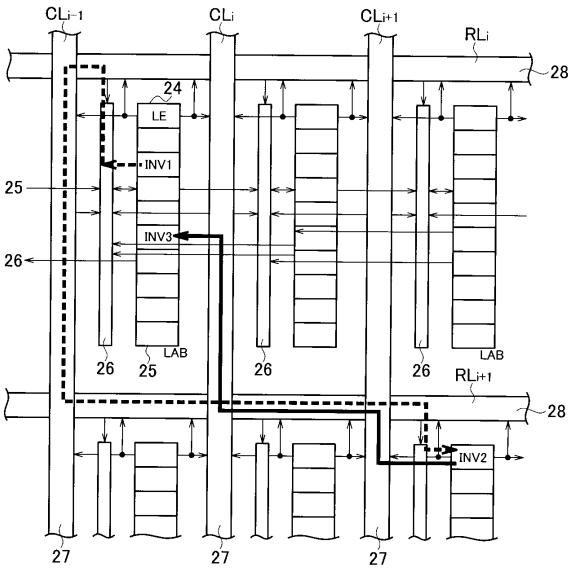
【図８】


OUT
20
D-FF
f_s
XOR
18
IC : Interconnect
length l=n
IC
N_{1n}
N_{2n}
N_{kn}
N_{12}
N_{22}
N_{k2}
N_{11}
N_{21}
N_{k1}
22
23
k

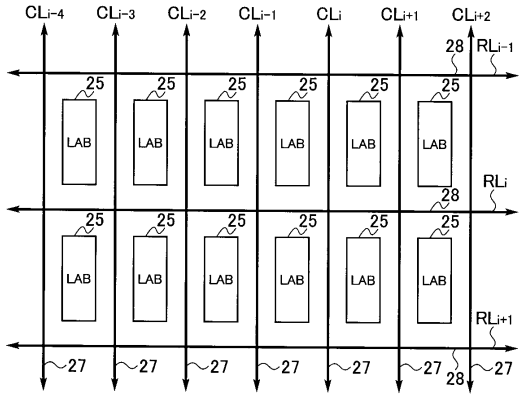
【図９】


CL_{i-1}
CL_i
RL_i
28
ロウインターコネクト
24
LE
カラムインターコネクト
ローカルインターコネクト
隣接
LAB
隣接
インターコネクト
LAB
26
25
27

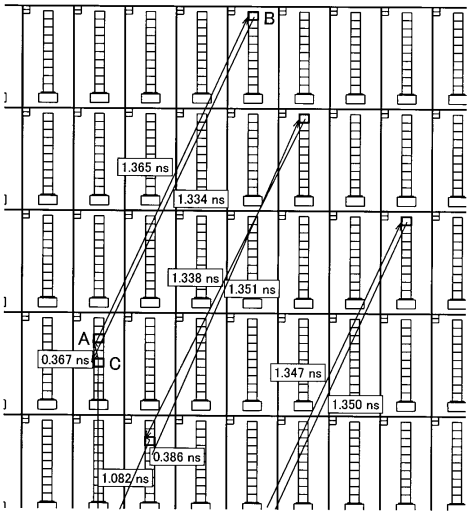
【図１０】


CL_{i-1}
CL_i
CL_{i+1}
RL_i
28
24
LE
INV1
INV3
INV2
25
26
LAB
RL_{i+1}
27

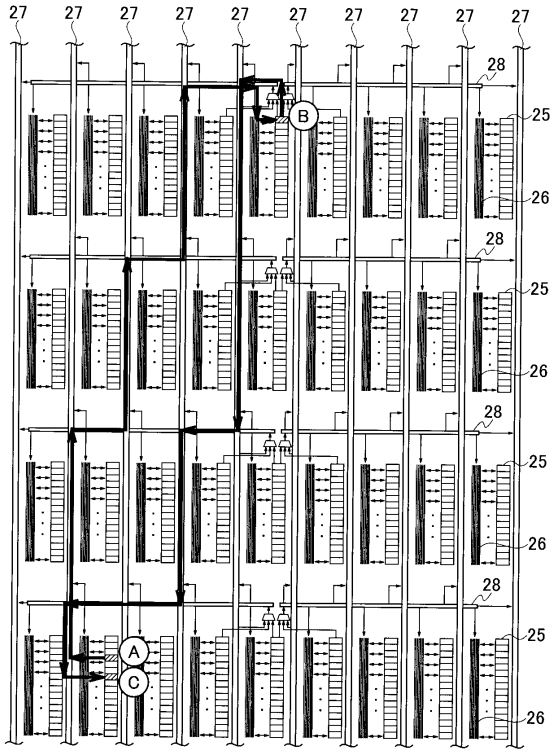
【図１１】



【図１２】



【図１３】



【図１４】

パラメータ	値
Bitstream Length	100000
Number of Bitstreams	1000
Block Frequency Test block length	128
Non Overlapping Template Test Block Length	9
Overlapping Template Test Block Length	9
Universal Test Block Length	1280
Universal Test Number Of Initialization Steps	7
Approximate Entropy Test Block Length	10
Serial Test Block Length	16
Linear Complexity Test Subsequence Length	500

【図１５】

検定種別	比較例				本発明			
	一様性		比率		一様性		比率	
Frequency	0.000000	×	0.000	×	0.000000	×	0.000	×
Block Frequency	0.000000	×	0.000	×	0.000000	×	0.000	×
Runs	0.000000	×	0.000	×	0.000000	×	0.000	×
LongRun	0.000000	×	0.000	×	0.000000	×	0.000	×
Matrix Rank	0.953089	○	0.993	○	0.150340	○	0.992	○
DFT	0.000000	×	0.688	×	0.000000	×	0.946	×
Non-overlapping Template	O:2 X:146		O:6 X:142		O:22 X:126		O:31 X:117	
Overlapping Template	0.000000	×	0.000	×	0.000000	×	0.000	×
Universal Statistical	0.000000	×	0.000	×	0.000000	×	0.000	×
Linear Complexity	0.385543	○	0.993	○	0.467322	○	0.990	○
Serial 1	0.000000	×	0.000	×	0.000000	×	0.000	×
Serial 2	0.000000	×	0.833	×	0.000000	×	0.955	×
Approximate Entropy	0.000000	×	0.000	×	0.000000	×	0.000	×
Cumulative Sums 1	0.000000	×	0.000	×	0.000000	×	0.000	×
Cumulative Sums 2	0.000000	×	0.000	×	0.000000	×	0.000	×
Random Excursions	0.000000	×	0.000	×	0.000000	×	0.000	×
Random Excursions Variant	0.000000	×	0.000	×	0.000000	×	0.000	×

【図１６】

テンプレート		比較例			本発明		
		一様性	比率		一様性	比率	
14	000011011	0.000000 ×	0.920	×	0.000000 ×	0.965	○
15	000011101	0.001866 ○	0.990	○	0.000000 ×	0.961	○
19	000100111	0.000000 ×	0.765	×	0.000000 ×	0.964	○
24	000110011	0.000000 ×	0.829	×	0.788728 ○	0.997	○
27	000111001	0.000000 ×	0.418	×	0.000184 ○	0.988	○
39	001010111	0.000000 ×	0.212	×	0.205531 ○	0.990	○
40	001011011	0.000000 ×	0.461	×	0.000643 ○	0.987	○
41	001011101	0.000000 ×	0.474	×	0.841226 ○	0.989	○
45	001101011	0.000000 ×	0.687	×	0.725829 ○	0.987	○
46	001101101	0.000000 ×	0.591	×	0.886162 ○	0.984	○
48	001110101	0.000000 ×	0.789	×	0.165340 ○	0.987	○
58	010010111	0.000000 ×	0.428	×	0.000000 ×	0.972	○
59	010011011	0.000000 ×	0.423	×	0.717714 ○	0.984	○
62	010100111	0.000000 ×	0.722	×	0.983938 ○	0.990	○
65	010110011	0.000000 ×	0.768	×	0.544254 ○	0.986	○
66	010110111	0.000000 ×	0.961	○	0.000000 ×	0.065	×
67	010111011	0.000000 ×	0.961	○	0.000000 ×	0.033	×
80	100111000	0.000000 ×	0.413	×	0.000047 ×	0.983	○
88	101011100	0.000000 ×	0.808	×	0.693142 ○	0.988	○
92	101101100	0.000000 ×	0.585	×	0.775337 ○	0.991	○
93	101110000	0.036833 ○	0.984	○	0.000000 ×	0.967	○
94	101110100	0.000000 ×	0.482	×	0.781106 ○	0.990	○
105	110011000	0.000000 ×	0.854	×	0.853049 ○	0.993	○
106	110011010	0.000000 ×	0.765	×	0.154629 ○	0.980	○
112	110101100	0.000000 ×	0.663	×	0.707513 ○	0.988	○
114	110110010	0.000000 ×	0.404	×	0.518106 ○	0.983	○
115	110110100	0.000000 ×	0.494	×	0.005638 ○	0.983	○
117	110111010	0.000000 ×	0.963	○	0.000000 ×	0.020	×
123	111001000	0.000000 ×	0.731	×	0.000000 ×	0.962	○
124	111001010	0.000000 ×	0.706	×	0.880145 ○	0.985	○
127	111010010	0.000000 ×	0.427	×	0.002949 ○	0.984	○
128	111010100	0.000000 ×	0.221	×	0.054314 ○	0.985	○
131	111011010	0.000000 ×	0.970	○	0.000000 ×	0.068	×

フロントページの続き

審査官　田中　友章

(56)参考文献　Schellekens,D. et al., “FPGA Vendor Agnostic True Random Number Generator”, International Conference on Field Programmable Logic and Applications, 2006. FPL'06., ２００６年　8月３０日, p.1-6
Suner,B. et al., “A Provably Secure True Random Number Generator with Built-in Tolerance to Active Attacks”, IEEE Transactions on Computers, ２００７年　1月, Vol.56, No. 1,, P.109-119
Kohlbrenner,P. et al., “An Embedded True Random Number Gererator for FPGAs”, FPGA '04 Proceedings of the 2004 ACM/SIGDA 12th International Symposium on Field Programmable Gate Arrays, ２００４年, p.71-78

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ　　７／５８
Ｇ０９Ｃ　　１／００
Ｈ０３Ｋ　　３／８４