

(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2008-176698
(P2008-176698A)

(43) 公開日 平成20年7月31日(2008.7.31)

(51) Int.Cl.			F I			テーマコード (参考)		
G06F	7/58	(2006.01)	G06F	7/58	A	5J049		
H03K	3/84	(2006.01)	H03K	3/84	Z	5J104		
G09C	1/00	(2006.01)	G09C	1/00	650B			

審査請求 未請求 請求項の数 5 O L (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)

(71) 出願人 504133110
国立大学法人 電気通信大学
東京都調布市調布ヶ丘1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

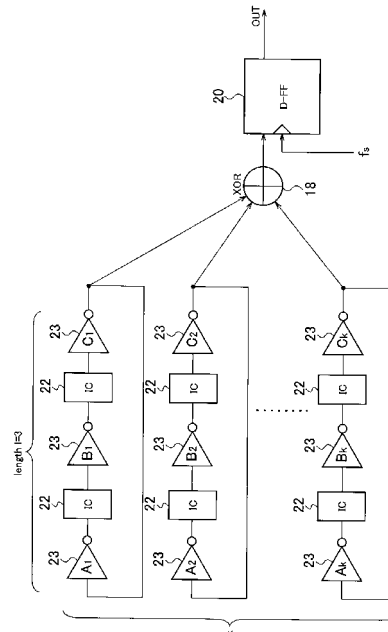
(54) 【発明の名称】 乱数発生器及び乱数発生器の作成方法

(57) 【要約】

【課題】リングオシレータ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して、真の乱数を発生する乱数発生器及び乱数発生器の作成方法を提供する。

【解決手段】複数の論理素子23で構成されるリングオシレータの当該論理素子23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(インターコネクト)22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18と、排他的論理和回路18の出力に接続され、所定のサンプリング周波数 f_s でジッター出力をサンプリング抽出するサンプリング回路12とを備える。

【選択図】 図7



【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

を備えることを特徴とする乱数発生器。

【請求項 3】

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請求項 1 又は請求項 2 に記載の乱数発生器。

【請求項 4】

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 乃至請求項 3 のいずれかに記載の乱数発生器。

【請求項 5】

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氣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

10

20

30

40

50

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

10

20

30

40

50

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ることを特徴とする。

10

【0012】

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。

20

【0013】

本発明の請求項4に記載の乱数発生器は、請求項1乃至請求項3のいずれか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5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。

30

【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。

40

【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

50

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 $Q_1, Q_2, \dots, Q_{2n+1}$ （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。

10

【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 $Q_1, Q_2, \dots, Q_{2n+1}$ 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。

20

【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。

30

【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。

40

【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】

50

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 $\dots, Q_{n-1}, Q_n, Q_{n+1}, \dots$ と各々のNOTゲートに対応する遅延回路 $\dots, D_{n-1}, D_n, D_{n+1}, \dots$ 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 $\dots, Q_{n-1}, Q_n, Q_{n+1}, \dots$ 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 $\dots, D_{n-1}, D_n, D_{n+1}, \dots$ が接続されている。

10

【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 $Q_1, Q_2, \dots, Q_{2n+1}$ 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。

20

【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。

30

【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】

40

[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。

50

【 0 0 3 7 】

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 1 8 で束ねる。更に、排他的論理和回路 1 8 の出力信号を、D タイプフリップフロップ回路 (D - F F) 2 0 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 1、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。

【 0 0 3 8 】

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。

10

【 0 0 3 9 】

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 1 8 で束ねる。更に、排他的論理和回路 1 8 の出力信号を、D タイプフリップフロップ回路 (D - F F) 2 0 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、 $A_1, A_2, \dots, A_k, B_1, B_2, \dots, B_k$ 、及び C_1, C_2, \dots, C_k と表示する 2 3 は、いずれも NOT ゲートを示す。I C と表示する 2 2 は、インターコネクトであり、配線資源を示す。

20

【 0 0 4 0 】

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 1 8 で束ねる。更に、排他的論理和回路 1 8 の出力信号を、D タイプフリップフロップ回路 (D - F F) 2 0 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、 $N_{11}, N_{21}, \dots, N_{k1}, N_{12}, N_{22}, \dots, N_{k2}, \dots$ 及び $N_{1n}, N_{2n}, \dots, N_{kn}$ と表示する 2 3 は、いずれも NOT ゲートを示す。I C と表示する 2 2 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。

30

【 0 0 4 1 】

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。

【 0 0 4 2 】

[第 3 実施形態]

(F P G A)

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。

40

【 0 0 4 3 】

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 (L E) 2 4 が 1 0 個まとまったロジックアレイブロック (L A B) 2 5 と、L A B 2 5 の周囲に配置されるローカルインターコネクト 2 6 と、ローカルインターコネクト 2 6 及び L A B 2 5 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 (C L) 2 7 と、同じくローカルインターコネクト 2 6 及び L A B 2 5 の周囲に配置

50

され、ロウ方向に延伸するロウインターコネクタ(RL)28とを備える。

【0044】

ローカルインターコネクタ26、カラムインターコネクタ(CL)27及びロウインターコネクタ(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タ(CL)27及びロウインターコネクタ(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タ26、カラムインターコネクタ(CL)27及びロウインターコネクタ(RL)28などによって構成される配線資源(インターコネクタ)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(インターコネクタ)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(インターコネクタ)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(インターコネクタ)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、インターコネクタ(IC)22を2箇所に入れ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タ $\dots, CL_{i-4}, CL_{i-3}, CL_{i-2}, CL_{i-1}, CL_i, CL_{i+1}, CL_{i+2}, \dots$ と、ロウ方向に延伸する複数のロウインターコネクタ $\dots, RL_{i-1}, RL_i, RL_{i+1}, \dots$ を備える。従って、NOTゲート間の配線資源(インターコネクタ)は、FPGA上のカラムインターコネクタ、ロウインターコネクタ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タ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(インターコネクタ)による遅延回路を積極的に導入しない場合には、 $k=110\sim 210$ であるのに対して、配線資源(インターコネクタ)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(インターコネクタ)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 $f_s=50\text{MHz}$ 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

10

20

30

40

50

、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1.365 nsの配線遅延をもつインターコネクトを、B - C間に1.334 ns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、0.367 ns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

10

【0054】

複数のLE24と、当該LE24を電氣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。

20

【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、NIST SP 800 - 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、

30

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 $l = 3$ 、 $k = 20$ 、 $f_s = 50 \text{ MHz}$ 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NIST SP 800 - 22にかけ、統計的性質を調べた。

40

【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 $f_s = 50 \text{ MHz}$ より 50 Mbps 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

50

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から明らかのように、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。

10

【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から明らかのように、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Serial 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。

20

【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。

30

【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。

40

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

50

トアレイ内，或いは F P G A 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。

【 0 0 6 8 】

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 A S I C として構成することもできる。

【 0 0 6 9 】

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。

【 0 0 7 0 】

[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。

【 0 0 7 1 】

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 】

【 0 0 7 2 】

【 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 F P G A の内部回路構成図。

【 図 1 0 】 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 F P G A の内部回路構成例。

【 図 1 1 】 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 F P G A の L A B の配

10

20

30

40

50

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、NIST SP 800 - 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、NIST SP 800 - 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 Temp late検定の結果。 10

【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

Q₁, Q₂, ..., Q_{n-1}, Q_n, Q_{n+1}, ..., Q_{2n+1}...、A₁, A₂, ..., A_k、B₁, B₂, ..., B_k、及びC₁, C₂, ..., C_k、N₁₁, N₂₁, ..., N_{k1}、N₁₂, N₂₂, ..., N_{k2}、... 及びN_{1n}, N_{2n}, ..., N_{kn}... NOTゲート 30

Q_A... pチャンネルMOSトランジスタ

Q_B... nチャンネルMOSトランジスタ

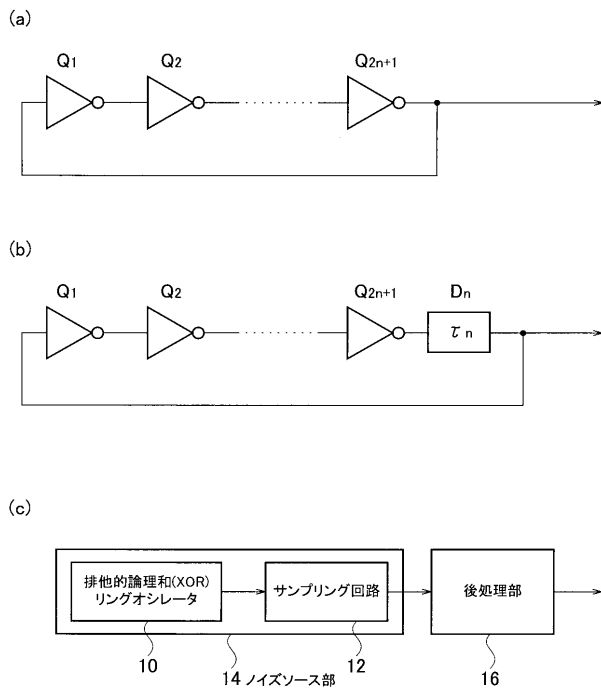
D₁, D₂, ..., D_{n-1}, D_n, D_{n+1}... 遅延回路

t₁, t₂, ..., t_{n-1}, t_n, t_{n+1}... 遅延時間

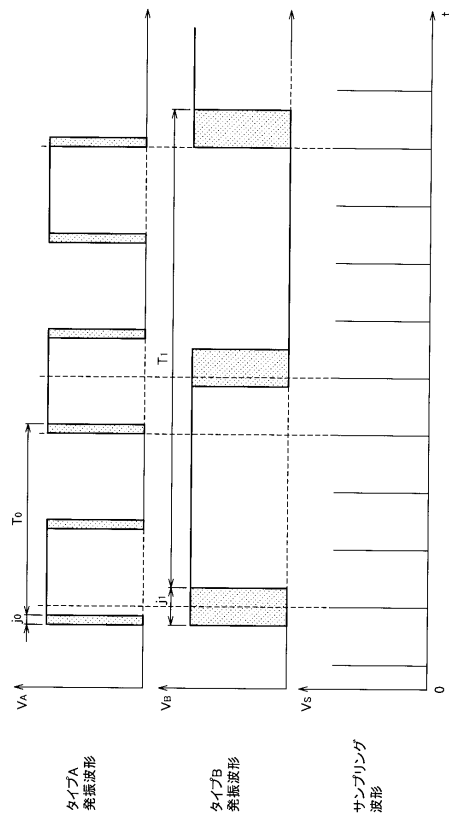
T₀, T₁... 周期

j₀, j₁... ジッター間隔

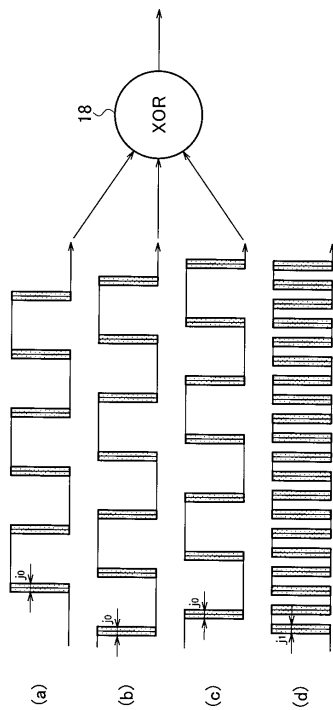
【 図 1 】



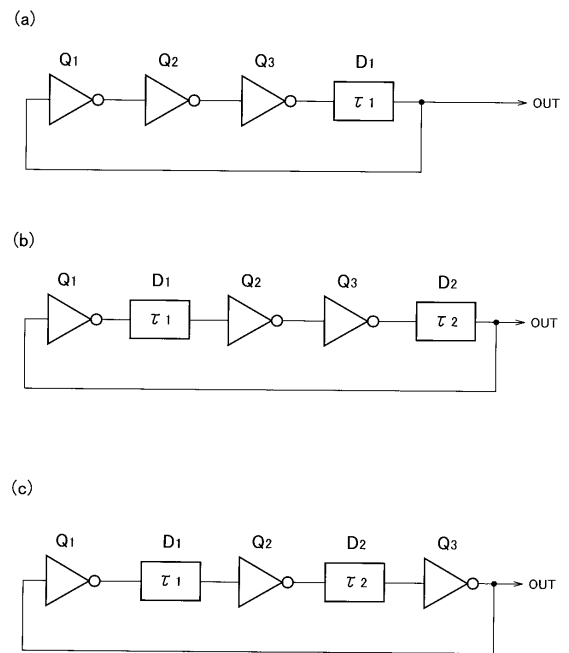
【 図 2 】



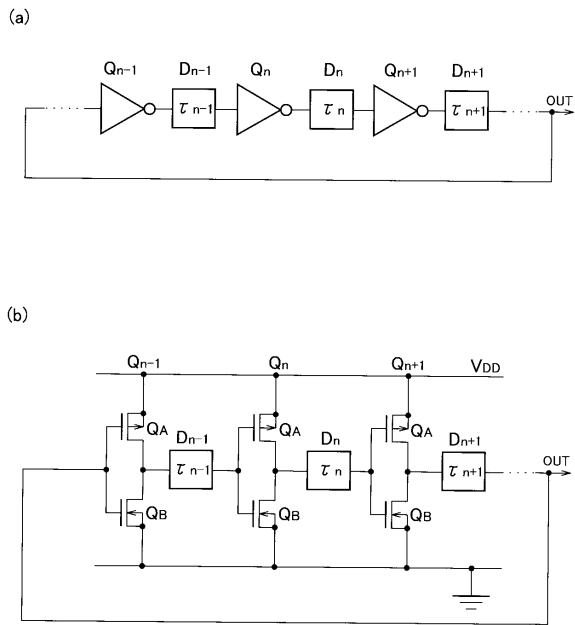
【 図 3 】



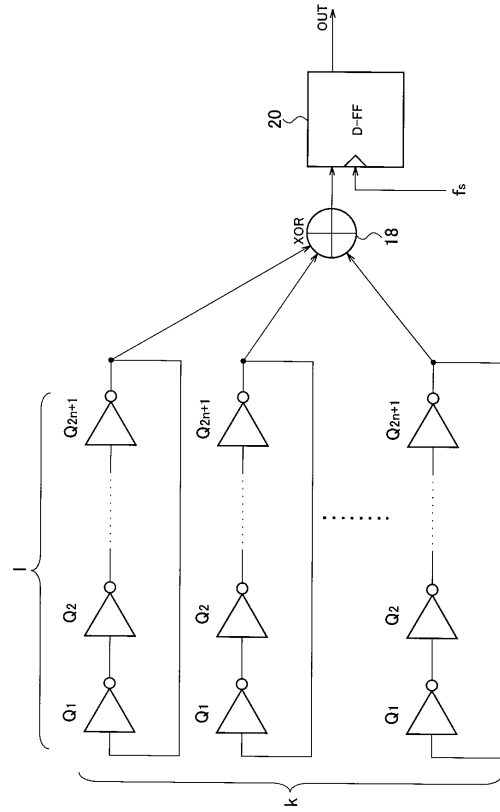
【 図 4 】



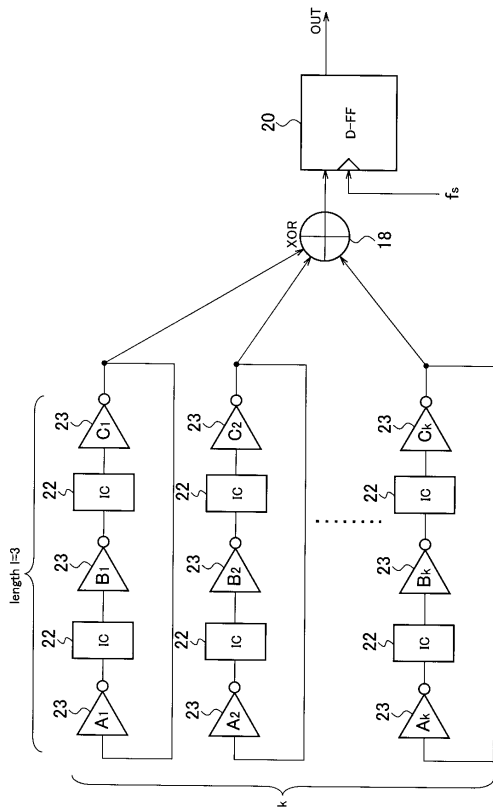
【 図 5 】



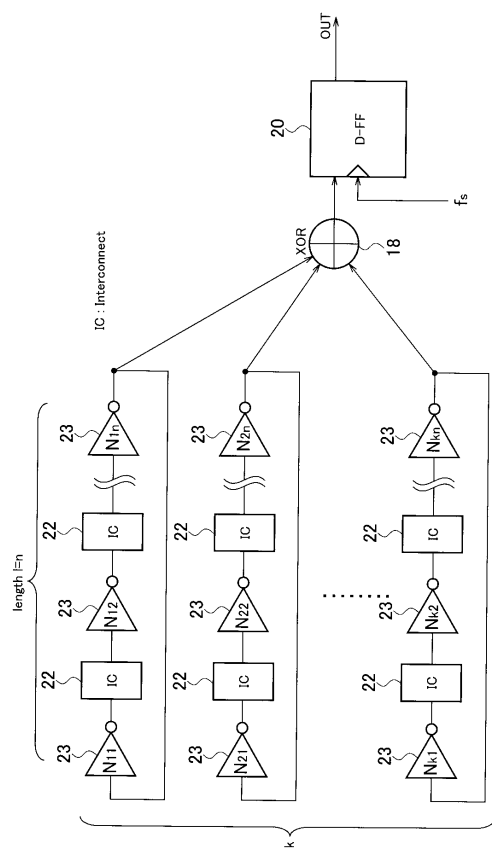
【 図 6 】



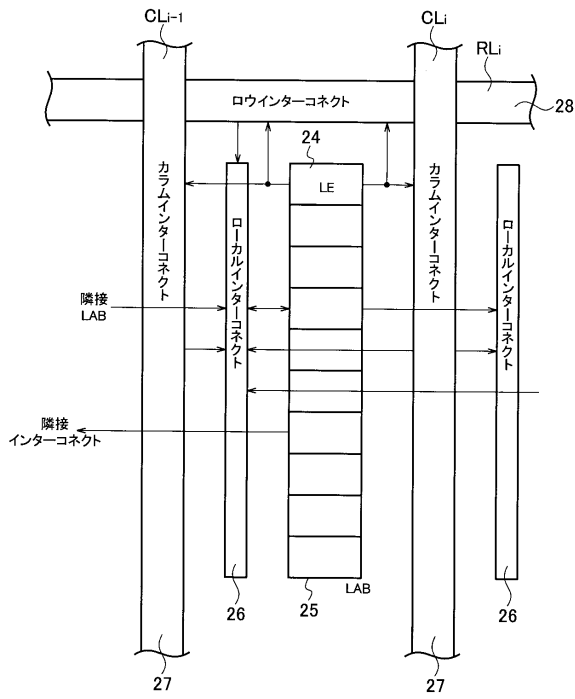
【 図 7 】



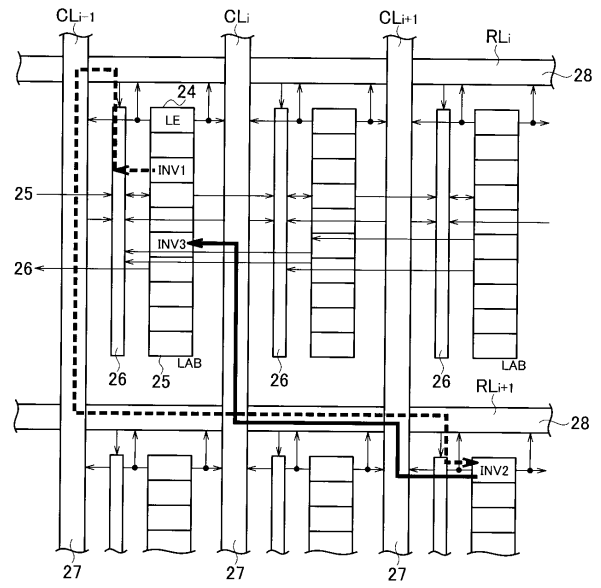
【 図 8 】



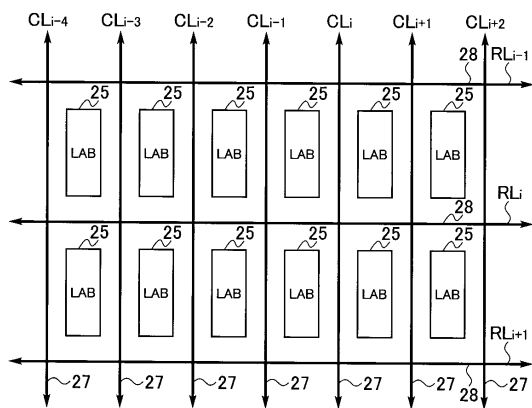
【 図 9 】



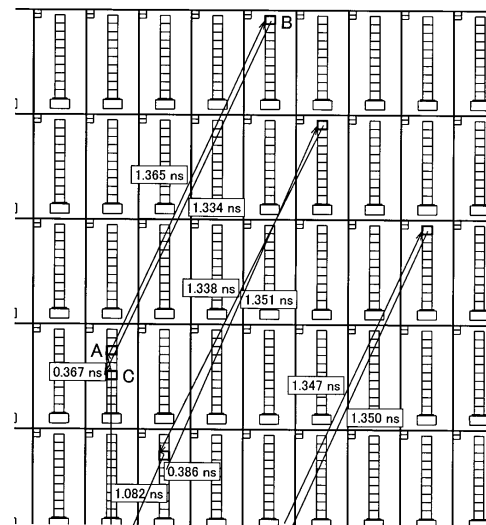
【 図 1 0 】



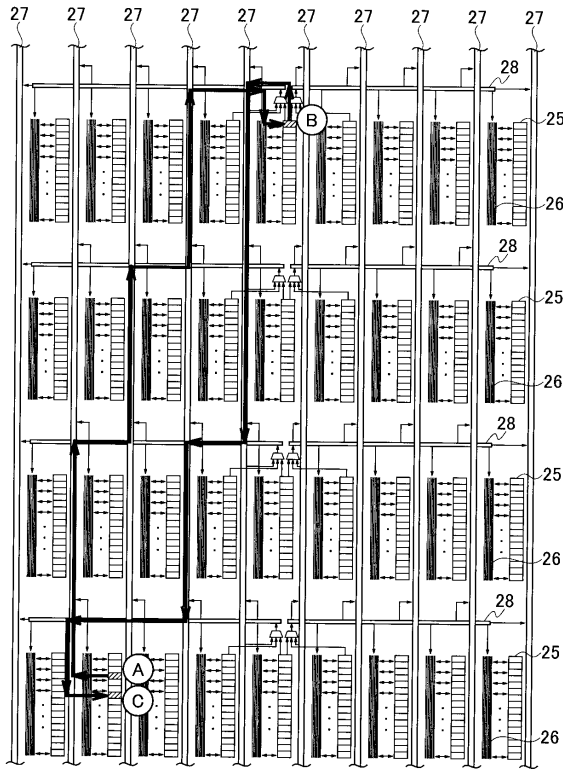
【 図 1 1 】



【 図 1 2 】



【 図 1 3 】



【 図 1 4 】

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 1 5 】

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	0.2 X:146	0.6 X:142	0.22 X:126	0.31 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 1 6 】

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

Fターム(参考) 5J049 AA01 CA09
5J104 FA10 GA01 NA22