(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4629876号
(P4629876)
(45)発行日　平成23年2月9日(2011.2.9)　(24)登録日　平成22年11月19日(2010.11.19)

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

請求項の数 3　(全 18 頁)

(21)出願番号　特願2000-608542 (P2000-608542)
(86)(22)出願日　平成12年3月16日 (2000.3.16)
(65)公表番号　特表2002-540482 (P2002-540482A)
(43)公表日　平成14年11月26日 (2002.11.26)
(86)国際出願番号　PCT/US2000/006916
(87)国際公開番号　WO2000/059153
(87)国際公開日　平成12年10月5日 (2000.10.5)
審査請求日　平成19年2月15日 (2007.2.15)
(31)優先権主張番号　09/283,096
(32)優先日　平成11年3月31日 (1999.3.31)
(33)優先権主張国　米国(US)

(73)特許権者　591003943
インテル・コーポレーション
アメリカ合衆国　９５０５２　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００
(74)代理人　100064621
弁理士　山川　政樹
(72)発明者　ウエルズ・スティーブン・イー
アメリカ合衆国・９５７６２・カリフォルニア州・エル　ドラド　ヒルズ・ウェザーベイン　コート・４２３６
(72)発明者　ワード，デイビッド・エイ
アメリカ合衆国・９５８２６・カリフォルニア州・サクラメント・ハニーサックル　ウェイ・２８０８

最終頁に続く

(54)【発明の名称】乱数発生器用デューティ・サイクル修正器

(57)【特許請求の範囲】
【請求項１】
ランダム・ビット・ソースのランダム・ビット・ストリーム出力から修正されたビット・ストリームを生成する方法であって、
前記ランダム・ビット・ストリーム内のペアとなるビットを比較回路で互いに比較するステップと、
前記ペアとなるビットが等しい場合には確認論理回路で前記ペアとなるビットを破棄するステップと、
前記ペアとなるビットが異なる場合には前記確認論理回路で前記ペアとなるビットを受け入れるステップと、
前記異なるビットの順序に基づいて前記確認論理回路で異なるビットの前記ペアのそれぞれ一方を、即ち、前記ペア内の最初のビットまたは２番目のビットの一方を破棄するステップと、
前記ペアとなるビットが異なる時は出力回路で前記ペアとなるビットの破棄されないビットを、即ち、前記ペア内の最初のビットまたは２番目のビットの他方を出力するステップと、
ビット間の自己相関を低減するためにモジュロＸカウンタにより決定されたＸビットごとに破棄するステップとを含む方法。
【請求項２】
ランダム・ビット・ソースのランダム・ビット・ストリーム出力から修正されたビット・

ストリームを生成するためのデューティ・サイクル修正回路であって、
前記ランダム・ビット・ストリームのペアとなるビットの第１のビットを受信及び記憶する第１のストレージ回路と、
前記ペアとなるビットの第２のビットを受信及び記憶する、前記第１のストレージ回路に直列に結合された第２のストレージ回路と、
前記ペアとなるビットを比較して前記ペアとなるビットが異なるかどうかを決定する前記第１のストレージ回路と前記第２のストレージ回路に結合された比較回路と、
前記第１と第２のストレージ回路と前記比較回路に結合された確認論理回路であって、前記ビットが同じ場合には前記ペアとなるビットを破棄し、前記ビットが異なる場合には前記ビットの順序に基づいて前記ペアとなるビットのそれぞれ一方を、即ち、前記ペア内の最初のビットまたは２番目のビットの一方を選択する確認論理回路と、
ビット間の自己相関を低減するためにモジュロＸカウンタにより決定された前記ランダム・ビット・ストリームからＸビットごとに破棄する、前記確認論理回路に結合されたタイミング回路とを備えるデューティ・サイクル修正回路。
【請求項３】
ネットワーク・メディアによりメッセージを送信及び受信を行うべく動作し得るネットワーク・インターフェース・デバイスと、
前記ネットワーク・メディアにより転送されたメッセージの符号化及び復号化を行うべく動作し得る暗号化／解読回路であって、ランダム・ビット・ストリームを生成するように動作し得る乱数発生器を有する暗号化／解読回路とを備えるコンピュータであって、
前記乱数発生器が、
（ａ）前記ランダム・ビット・ストリームのペアとなるビットの第１のビットを受信及び記憶する第１のストレージ回路と、
（ｂ）前記ペアとなるビットの第２のビットを受信及び記憶する、前記第１のストレージ回路に直列に結合された第２のストレージ回路と、
（ｃ）前記ペアとなるビットを比較して前記ペアとなるビットが異なるかどうかを決定する前記第１のストレージ回路と前記第２のストレージ回路に結合された比較回路と、
（ｄ）前記第１と第２のストレージ回路と前記比較回路に結合された確認論理回路であって、前記ビットが同じ場合には前記ペアとなるビットを破棄し、前記ビットが異なる場合には前記ビットの順序に基づいて前記ペアとなるビットのそれぞれ一方を、即ち、前記ペア内の最初のビットまたは２番目のビットの一方を選択する確認論理回路と、
（ｅ）ビット間の自己相関を低減するためにモジュロＸカウンタにより決定された前記ランダム・ビット・ストリームからＸビットごとに破棄する、前記確認論理回路に結合されたタイミング回路とを備えることを特徴とするコンピュータ。
【発明の詳細な説明】
【０００１】
（技術分野）
本発明は、全体的にコンピュータ・セキュリティに関し、より詳細に述べれば、乱数発生器におけるほぼ一様なデューティ・サイクルの発生に関する。
【０００２】
（発明の背景）
乱数発生回路は、各種の電子応用において使用されている。乱数発生器に関する重要な応用の１つに、メッセージ・データの暗号化と解読が行なわれるコンピュータ・セキュリティの分野におけるものがある。暗号システムは、データを、符号化したメッセージに変える変換を含み、それが送信されたとき、意図された受取人だけがそれを復号することができる。もっとも一般的な暗号テクニックにおいては、暗号（キー）が使用され、送り側はそれを用いてメッセージを符号化し、受け側はそれを用いて当該符号化されたメッセージを復号する。広く知られた暗号システムには、メッセージの符号化および復号化に単一のキーを使用する方法と、メッセージの符号化とその復号化にそれぞれ別のキーを使用する方法がある。

【０００３】
メッセージの符号化および復号化に使用されるキーは、基本的にバイナリ・データ・パターンであり、それに照らしてメッセージの処理、すなわちフィルタリングが行なわれる。効果的な暗号システムは、充分に大きなビット数を有し、再生がほとんど不可能なキーの使用を必要とする。さらに、キーを構成するデータ・パターンは、そのキーによって符号化が行なわれたメッセージ内において、それらのパターンないしはパターン群を予測不能にできる充分なランダム性を有していなければならない。したがって効果的な暗号システムには、メッセージ内のバイナリ・データが完全に予測不能な態様で変換されることを保証するように、質の高い乱数発生器を使用する必要がある。一般に、暗号スキームにおけるランダム性の欠如は、符号化済みデータと未符号化データの間に、ある種の相関をもたらす。その後、この相関を使用し、符号化済みメッセージに基づいて試行錯誤を繰り返し、可能性のある出力パターンの予測といったテクニックを通じて、コードの盗み出しが可能になる。

【０００４】
バイナリ乱数に望ましい特徴は、純粋にランダムな順序において「０」と「１」のビットが出力されることである。すなわち、あらゆる時点において出力ビットの値が完全に予測不能となることである。乱数発生器の出力のデューティ・サイクルは、無限の標本サイズにわたって約５０パーセントとなり、出力が論理ロー（「０」）になる確率と、出力が論理ハイ（「１」）になる確率が等しくなることが望ましい。また、乱数発生器によって示される任意ビットと他のビットの間の相関が低く（たとえば、約ゼロの相関）、出力ビットの間のフーリエ分布が平坦になることが望ましい。

【０００５】
しかしながら、現在知られている乱数発生器は、統計的に有意な標本サイズにわたって「０」の数と「１」の数が等しくならない傾向にある。従来技術の乱数発生器が一様でないデューティ・サイクルとなる共通の理由としては、禁止されたセットアップ／ホールドタイムの間にデータがラッチされたとき、一般に、乱数発生器を構成するラッチが２つの状態のうちの一方に偏ることが挙げられる。乱数発生器におけるデューティ・サイクルの変動を抑える現在の一般的な方法は、ランダム・ビット・ソースの出力段におけるリニア・フィードバック・シフト・レジスタ（ＬＦＳＲ）の使用が関連する。

【０００６】
図１は、従来技術における乱数発生器の一例を示しており、ランダム・ビット・ソース１０２の出力と結合されるリニア・フィードバック・シフト・レジスタ１０４を使用する。ＬＦＳＲ　１０４は、多数のラッチ１０５とゲート１０６を含み、それを通じてランダム・ビット・ソース１０２からの出力ビットが伝播される。出力ビットの状態は、ゲート１０６によってランダムに反転され、ビットの順序がさらに、ラッチ１０５を通るビットのフィードバックを介して撹乱される。

【０００７】
概して、図１に示したようなリニア・フィードバック・シフト・レジスタは、特定の不利益を有し、しかも典型的なランダム・ビット・ソースによってもたらされる一様でないデューティ・サイクル特性の完全な修正が得られない。ＬＦＳＲ　１０４によって示されるように、通常、ＬＦＳＲ自体が複数のラッチとゲートを包含している。これらのラッチとゲートは、ランダム・ビット・ソース１０２内のラッチの場合に同じく、特定の状況下において「０」または「１」のラッチへ偏る傾向にある。つまり、通常のＬＦＳＲ自体が「１」と「０」の一様なデューティ・サイクルを生成せず、そのためランダム・ビット・ソースにおけるデューティ・サイクルの変動を完全には修正し得ない。

【０００８】
それ以外にもリニア・フィードバック・シフト・レジスタは、多数のラッチとゲートを必要とするという不利益がある。たとえば、図１に示したような３２ビットのＬＦＳＲであれば、３２個のＤタイプのラッチが必要になるだけでなく、多数の組み合わせゲートが必要になる。このことは、この種のＬＦＳＲを使用する乱数発生器のために必要となるシリ

コン面積を格段に増加させることになる。
【０００９】
（発明の要約）
ここでは、ランダム・ビット・ソースによって出力されたランダム・ビット・ストリームから、修正後のビット・ストリームを生成する方法および装置を開示する。それにおいては、ランダム・ビット・ストリーム内のビットの連続するペアが比較される。ビットのペアを構成する２つのビットがまったく等しい場合には、出力されたビットが破棄される。ビットのペアを構成する２つのビットが互いに異なる場合には、そのビットのペアの一方のビットを出力ビットとして採用する。
【００１０】
このほかの本発明の特徴ならびに利点は、添付の図面および以下の詳細な説明から逐次明らかなものとなろう。
【００１１】
なお、添付図面には、限定の意味ではなく、例示のための手段として本発明が示されており、それらにおいては、類似の要素に類似の参照番号が用いられている。
【００１２】
（詳細な説明）
乱数発生器内で使用するデューティ・サイクル修正器を説明する。一実施形態においては、このデューティ・サイクル修正器によって、ランダム・ビット・ソースから出力されたビットの連続するペアが処理される。ビットのペアを構成する２つのビットがまったく等しい場合には、デューティ・サイクル修正器によってそのビットのペアが破棄されるか、あるいは出力されない。ビットのペアを構成する２つのビットが互いに異なる場合には、デューティ・サイクル修正器によってビット・ペア内のビットの一方が出力される。
【００１３】
本発明の実施形態の利点として意図されていることは、ランダム・ビット・ソースの出力に関してほぼ一様なデューティ・サイクルを生成する回路を提供することである。さらに、集積回路デバイス内に実装された場合に、必要とするシリコン面積が小さい乱数発生器を提供することも本発明の実施形態の利点として意図されている。
【００１４】
ここで、ランダム・ビット・ソースは、ランダムと推定される順序でバイナリ・ディジット系列を出力するディジタル回路であることを思い出されたい。理想的なランダム・ビット・ソースにおいては、所定の出力ビットが「０」となる確率が、それが「１」となる確率に等しい。つまり、ランダム・ビット・ソースの出力波形のデューティ・サイクルは、統計的に有意な標本サイズにわたって一様に５０パーセントとなる。しかしながら、ほとんどのランダム・ビット・ソースは、禁止されたホールドタイムまたはセットアップタイムの間にデータがラッチされると、ランダム・ビット・ソース内のラッチならびにゲートが特定の論理・レベルをラッチするという傾向に起因したデューティ・サイクルの変動を呈する。
【００１５】
ランダム・ビット・ソースによって特定時に所定のビットが出力される確率は、一定の数学的関係によって表すことができる。たとえば、出力が「０」になる確率（Ｐ（０））をｐとすれば、出力が「１」となる確率（Ｐ（１））は１－ｐで表される。すなわち、
「０」を生成する確率：Ｐ（０）＝ｐ
「１」を生成する確率：Ｐ（１）＝１－ｐ
である。理想的なランダム・ビット・ソースにおいては、ｐが５０パーセントになる。逆に、理想的でないランダム・ビット・ソースの場合は、ｐが５０パーセントより実質的に大きくなるか、あるいはそれより小さくなる。
【００１６】
ランダム・ビット・ソースの連続する出力をペアとして考えると、この確率は次のようになる。

「０」「０」を生成する確率：Ｐ（００）＝Ｐ（０）Ｐ（０）＝ｐ^2
「０」「１」を生成する確率：Ｐ（０１）＝Ｐ（０）Ｐ（１）＝ｐ（１－ｐ）
「１」「０」を生成する確率：Ｐ（１０）＝Ｐ（１）Ｐ（０）＝（１－ｐ）ｐ
「１」「１」を生成する確率：Ｐ（１１）＝Ｐ（１）Ｐ（１）＝（１－ｐ）^{2}

【００１７】

数学的に、「０」「１」の出力ペアと「１」「０」の出力ペアが生成される確率は、上記の確率の式からもわかるように、互いに等しい。つまり、ｐ（１－ｐ）＝（１－ｐ）ｐであり、したがってＰ（０１）＝Ｐ（１０）である。

【００１８】

この性質は、ランダム・ビット・ソースが「１」を生成する確率、または「０」を生成する確率とは無関係に、与えられた任意の出力に関して真となる。したがって、特定のランダム・ビット・ソースについて、ｐが５０パーセントとならない場合であっても、そのランダム・ビット・ソースが「０－１」の出力ペアを生成する確率は、それが「１－０」の出力ペアを生成する確率に等しい。本発明の一実施形態においては、この原理を用いて、一様でないデューティ・サイクルを呈し、かつ所定の出力ビット・ストリーム内の「０」と「１」の分布が一様でないランダム・ビット・ソースの出力を訂正する。

【００１９】

本発明の１つの方法においては、デューティ・サイクル修正器がランダム・ビット・ソースから出力されたペアとなるビットを処理して、修正した、実質的にデューティ・サイクルが一様なビット・ストリームを決定する。一実施形態においては、ビットのペアを構成するビットがともに等しいときには、デューティ・サイクル修正器によってそのペアが破棄され、修正後のビット・ストリームの一部として出力されない。つまり、出力ビットのペアを構成するビットがともに「０」であれば、そのペアが破棄される。それと同様に、出力ビットのペアを構成するビットがともに「１」であれば、そのペアが破棄される。しかしながら、出力ビットのペアを構成するビットが互いに異なれば、デューティ・サイクル修正器により、そのペアの一方のビットが修正後のビット・ストリームの１つのビットとして出力される。一実施形態においては、デューティ・サイクル修正器が異なるビットからなるペア内の最初のビットを修正後のビットとして出力する。したがって、この実施形態においては、出力ペアが「０－１」であれば修正後のビットが「０」にセットされ；出力ペアが「１－０」であれば修正後のビットが「１」にセットされる。各種のペアの場合に対応する修正後のビット値は、次の関係を用いて表すことができる。

Ｐ（００）＝Ｐ（０）Ｐ（０）＝ｐ^2　　破棄される
Ｐ（０１）＝Ｐ（０）Ｐ（１）＝ｐ（１－ｐ）　論理「０」が出力される
Ｐ（１０）＝Ｐ（１）Ｐ（０）＝（１－ｐ）ｐ　論理「１」が出力される
Ｐ（１１）＝Ｐ（１）Ｐ（１）＝（１－ｐ）^{2}　　破棄される

【００２０】

変形実施形態においては、デューティ・サイクル修正器が異なるビットからなるペア内の２番目のビットを修正後のビットとして出力する。つまり、この実施形態においては、出力ペアが「０－１」であれば修正後のビットが「１」にセットされ；出力ペアが「１－０」であれば修正後のビットが「０」にセットされる。したがって、この変形実施形態における各種のペアの場合に対応する修正後のビット値は、次の関係を用いて表すことができる。

Ｐ（００）＝Ｐ（０）Ｐ（０）＝ｐ^2　　破棄される
Ｐ（０１）＝Ｐ（０）Ｐ（１）＝ｐ（１－ｐ）　論理「１」が出力される
Ｐ（１０）＝Ｐ（１）Ｐ（０）＝（１－ｐ）ｐ　論理「０」が出力される
Ｐ（１１）＝Ｐ（１）Ｐ（１）＝（１－ｐ）^{2}　　破棄される

【００２１】

図２は、上記の実施形態を具体化したデューティ・サイクル修正器２００の一実施形態を示しており、それにおいては、ランダム・ビット・ソース２０２の出力から実質的に一様なビット・ストリームが生成され、しかも従来のＬＦＳＲ回路より使用されているゲート

数が少ない。ランダム・ビット・ソース２０２は、信号ライン２２２上にランダムなビットのストリームを出力するものであれば、任意のランダム・ビット・ソースとすることができる。本発明の一実施形態においては、ランダム・ビット・ソース２０２が、高速発振信号を周期的にラッチするランダムに変化させた低速クロック信号を使用するラッチ回路として実装される。ランダム・ビット・ソースのラッチから出力されるビットの値は、低速信号によってラッチされたときの高速信号の電圧レベルに依存する。またランダム・ビット・ソース２０２は、この分野において一般に知られているように、クロック信号またはストローブ信号ＣＬＫを生成して信号ライン２１６上に供給する。

【００２２】

デューティ・サイクル修正器２００は、ストレージ・エレメント２０４と２０６、比較回路２０８、確認論理２１０、および出力回路２１２を含んでいる。ストレージ回路２０４と２０６は、ランダム・ビット・ソース２０２から出力されたランダム・ビット・ストリーム内の連続するビットをペアとして、比較回路２０８による比較のためにストアする。ＣＬＫの第１のクロック・サイクルにおいて、ペアとなるビットの最初のビットがストレージ回路２０４にストアされる。この最初のビットは、続くクロック・サイクルにおいてストレージ回路２０６にストアされ、ストレージ回路２０４には、そのときランダム・ビット・ソース２０２から出力された次のビットがストアされる。ストレージ回路２０４と２０６は、ラッチ、レジスタ、揮発性もしくは不揮発性メモリ・セル、およびその他の等価物を含めた任意のタイプのストレージ・エレメントとすることができる。

【００２３】

ストレージ回路２０４と２０６にストアされたビットは、比較回路２０８によって比較される。この比較回路２０８は、エクスクルーシブ－オア・ゲートもしくはコンパレータといった任意のタイプの比較回路とすることができる。２つのビットが等しいときには、比較回路２０８が、信号ライン２２０上の信号を論理ハイの状態にセットしてＡＣＣＥＰＴ（アクセプト）をアサートする。２つのビットが等しくないときには、比較回路２０８が、その信号を論理ローの状態にセットしてＡＣＣＥＰＴ（アクセプト）のアサートを解く。つまり、ＡＣＣＥＰＴ（アクセプト）信号は、ランダム・ビット・ソースから出力されるペアとなるビットが、デューティ・サイクル修正器２００によって出力されるビット・ストリーム内の修正後のビットとなり得るか否かを示すことになる。

【００２４】

ＡＣＣＥＰＴ（アクセプト）信号は、ＣＬＫとともに確認論理２１０に渡される。比較回路２０８は、ストレージ回路２０４と２０６内の連続する２つのビットが互いに異なるとき、ＡＣＣＥＰＴ（アクセプト）をアサートする。しかしながら、デューティ・サイクル修正器２００が一様なデューティ・サイクルの出力ストリームを生成するためには、ランダム・ビット・ソース２０２から出力されるビットをオーバーラップさせることなく比較する方が好ましい。その機能を具体化している部分が確認論理２１０である。確認論理２１０は、ＡＣＣＥＰＴ（アクセプト）がアサートされ、かつ望ましいビットのペアがストレージ回路２０４と２０６にストアされているとき、信号ライン２１８上の信号を論理ハイの状態にセットしてストローブ信号ＳＴＢをアサートする。ＳＴＢがアサートされると、出力回路２１２がストレージ回路２０６内のビットをストアする。出力回路２１２は、レジスタ、ラッチ、１ないしは複数の揮発性もしくは不揮発性メモリ・エレメント、アンド・ゲート、あるいはその他の論理を含めて任意のストレージ・エレメントとすることができる。出力回路２１２によってストアされたビットは、ストレージ回路２０４と２０６内にストアされたビットに対応する修正後のビットとして信号ライン２１４に出力される。

【００２５】

変形実施形態に関しては、ストレージ回路２０６の出力に代えてストレージ回路２０４の出力を出力回路２１２に渡すことができる。その実施形態の場合、ＳＴＢがアサートされると出力回路２１２がストレージ回路２０４内のビットをストアし、このビットをストレージ回路２０４と２０６内にストアされたビットに対応する修正後のビットとして出力す

る。
【００２６】
図３は、デューティ・サイクル修正器２００の一実施形態であるデューティ・サイクル修正器３００を示している。デューティ・サイクル修正器３００は、ストレージ回路２０４と２０６のそれぞれ一実施形態であるラッチ３０４および３０６；比較回路２１０の一実施形態であるエクスクルーシブ－オア・ゲート３１０；確認論理２１０の一実施形態であるトランスペアレント・ラッチ３０８およびアンド・ゲート３０９の組み合わせ；および出力回路２１２の一実施形態であるラッチ３１２を含んでいる。
【００２７】
ラッチ３０４および３０６は、ランダム・ビット・ソース２０２から出力された連続するビットをペアとして、エクスクルーシブ－オア・ゲート３１０による比較のためにストアする。ペアとなるビットの最初のビットが、ＣＬＫによってラッチ３０４内にラッチされる。ＣＬＫの次のクロック・パルスでは、この最初のビットがラッチ３０６にラッチされ、ランダム・ビット・ソース２０２から出力された次のビットがラッチ３０４内にラッチされる。ビットのペアを構成する２つのビットが等しければ、エクスクルーシブ－オア・ゲート３１０がＡＣＣＥＰＴ（アクセプト）のアサートを行わずに「０」を出力し；ビットのペアを構成する２つのビットが互いに異なれば、エクスクルーシブ－オア・ゲート３１０が「１」を出力してＡＣＣＥＰＴ（アクセプト）をアサートする。
【００２８】
トランスペアレント・ラッチ３０８は、ランダム・ビット・ソース３０２からのＣＬＫをラッチし、ＡＣＣＥＰＴ（アクセプト）がアサートされ、かつラッチ３０４および３０６にオーバーラップのないビットのペアがストアされているときにＳＴＢがアサートされるようにアンド・ゲート３０９をクロックする。ＳＴＢがアサートされると、ラッチ３１２がラッチ３０６から出力されたビットを、信号ライン２１４上に出力する修正後のビットとしてラッチする。別の実施形態においては、ラッチ３０４の出力をラッチ３１２に供給することができる。このビットを、ラッチ３１２によりＳＴＢに応答してラッチすればよい。
【００２９】
図４は、デューティ・サイクル修正器３００の動作を示したフローチャートである。ステップ４００において、ラッチ３０４および３０６がランダム・ビット・ソース２０２から最初のペアとなるビットをラッチするが、そのうちの最初のビットはラッチ３０６にストアされ、２番目のビットはラッチ３０４にストアされる。ステップ４０２においては、エクスクルーシブ－オア・ゲート３１０が、ペアを構成する２つのビットが等しいか否かを決定する。ペアを構成する２つのビットが等しいときには、ステップ２０４において、ＡＣＣＥＰＴ（アクセプト）のアサートおよびＳＴＢのアサートが行なわれることなく、このビットのペアが拒絶または破棄される。ステップ２０４においては、いずれのビットもラッチ３１２によってラッチされることがなく、また信号ライン２１４に出力されることもない。しかしながら、ステップ４０２において２つのビットが互いに異なると判断されると、ステップ４０６においてペア内の最初のビットが出力として獲得される。
【００３０】
ステップ４０８においては、続くオーバーラップするペアとなるビットがランダム・ビット・ソース２０２から取り込まれ、その後プロセスがステップ４０２から繰り返される。このプロセスは、ランダム・ビット・ソースからの出力ビットのペアがすべて処理されるまで繰り返される。ペアを構成しない乱数源からの出力ビットは、処理不可能であり、したがって破棄される。ここでは、ペアを構成する最初のビットがラッチ３０６から修正後のビットとして供給されているが、別の方法においては、修正後のビットとして、ペアを構成する２番目のビットをラッチ３０４から供給できることに注意する必要がある。
【００３１】
図５は、デューティ・サイクル修正器３００の動作をさらに別の形で説明している。図５を参照すると、２番目のペアとなるビット（ビット２および３）および３番目のペアとな

るビット（ビット４および５）は修正後のビットを生成するが、最初のペアとなるビット（ビット０および１）および４番目のペアとなるビット（ビット６および７）からは生成されないことがわかる。

【００３２】

ランダム・ビット・ソース２０２は、ラッチ、論理ゲート、およびその他の回路エレメントの特性に起因して、連続的に生成されたビットの間に１次の自己相関を有するビットを出力することがある。つまり、図２および３に示したような上記のデューティ・サイクル修正器が実質的に一様なデューティ・サイクルを有するランダム・ビット・パターンを実質的に出力できる場合であっても、ランダム・ビット・ソースによって出力されるビット間の自己相関が低くないとデューティ・サイクル修正器の出力が一様なデューティ・サイクルに近づく可能性が高くならない。言い換えれば、ランダム・ビット・ストリーム内のビットが互いに相関を有していない場合においては、デューティ・サイクル修正器の出力が一様なデューティ・サイクルに近づく可能性が高くなる。

【００３３】

図５に示されるように、図３に示したデューティ・サイクル修正器３００は、ビットの連続するペアに対してデューティ・サイクル修正器３００が作用することから、ランダム・ビット・ソース２０２によって出力されたランダム・ビット・ストリーム内のビット間における１次の自己相関による影響を受けることがあり得る。図６は、別の実施形態、すなわちランダム・ビット・ソース２０２によって出力されるビットのペアの間における１次の自己相関の影響を軽減するデューティ・サイクル修正器６００を示している。このデューティ・サイクル修正器６００は、修正後のビットを生成したビットのペアが検出されるごとに、ランダム・ビット・ソース２０２から出力されるビットを１つ破棄することによって１次の自己相関の影響を軽減する。

【００３４】

デューティ・サイクル修正器６００は、デューティ・サイクル修正器３００に類似であるが、確認論理のトランスペアレント・ラッチ３０８がモジュロ２カウンタ６０２に置き換えられている点が異なる。デューティ・サイクル修正器６００の動作を図７に示す。ステップ７００においては、モジュロ２カウンタ６０２のカウント「０」と「１」に応答して、ラッチ３０４および３０６がランダム・ビット・ソース２０２からの最初のペアとなるビットをラッチする。ステップ７０２においては、エクスクルーシブ－オア・ゲート３１０が、ペアを構成する２つのビットが等しいか否かを決定する。ペアを構成する２つのビットが等しいときには、ステップ７０４において、ＡＣＣＥＰＴ（アクセプト）のアサートおよびＳＴＢのアサートが行なわれることなく、このビットのペアが拒絶または破棄される。ステップ７０４においては、いずれのビットもラッチ３１２によってラッチされることがなく、また信号ライン２１４に出力されることもない。しかし、ステップ７０２において２つのビットが互いに異なると判断されると、ステップ７０４において、カウント「１」に応答してＡＣＣＥＰＴ（アクセプト）がアサートされ、ＳＴＢがアサートされて、ラッチ３１２により最初のビット（または、それに代えて２番目のビット）が出力される。このＳＴＢは、モジュロ２カウンタ６０２にもフィードバックされ、その結果、ＳＴＢがアサートされるとモジュロ２カウンタ６０２が１カウントをスキップし、次の２クロック・サイクルをローに（つまり両方をカウント「０」に）保持する。これによりステップ８０７において、デューティ・サイクル修正器６００は、ランダム・ビット・ソース２０２からのランダム・ビット・ストリーム内の次のビットを破棄する。この「次のビット」はラッチ３０４内にロードされているが、モジュロ２カウンタ６０２が次にアンド・ゲート３０９に対してカウント「１」を出力する前に、クロックされてラッチ３０６を通り抜けることからこれが可能になる。ステップ７０８においては、続くオーバーラップするペアとなるビットがランダム・ビット・ソース２０２から取り込まれ、その後プロセスがステップ７０２から繰り返される。このプロセスは、ランダム・ビット・ソースからの出力ビットのペアがすべて処理されるまで繰り返される。

【００３５】

デューティ・サイクル修正器６００の動作を別の形で図８に示す。最初のペアとなるビット（ビット０および１）の処理時においては、ペア内のビットが等しいことから破棄され、このビットのペアに関しては修正後のビットが生成されない。それに加えて、ＳＴＢのアサートがないことからモジュロ２カウンタ６０２によるカウントのスキップも行なわれない。２番目のペアとなるビット（ビット２および３）はビット値が異なることから、デューティ・サイクル修正器６００が「０」を出力し、続いてモジュロ２カウンタ６０２がカウントをスキップすることから、その次のビット、つまりビット４が破棄される。３番目のペアとなるビット（ビット５および６）もビット値が等しくない。その結果、デューティ・サイクル修正器６００が「１」を出力し、モジュロ２カウンタ６０２がカウントをスキップすることから、その次のビット、つまりビット７が破棄される。最後のペアとなるビット（ビット８および９）は、ビット値が等しいことから破棄される。

【００３６】

ビット４および７を破棄することによって２番目のビットのペア（ビット２および３）と３番目のビットのペア（ビット５および６）の間の１次の自己相関、および３番目のビットのペアと４番目のビットのペア（ビット８および９）の間の１次の自己相関が低減される。修正後のビット・ストリームは、ランダム・ビット・ソース２０２によって出力された２番目のビットのペアと３番目のビットのペアの間、および３番目のビットのペアと４番目のビットのペアの間における２次の自己相関の影響を受けるが、その有意性はあまり高くない。

【００３７】

デューティ・サイクル修正器６００は、ランダム・ビット・ソースによって生成されたビットの間における１次の自己相関を低減する。しかしながら、それぞれの破棄されるビット（たとえば図８のビット４および７）がランダム・ビット・ストリーム内に一様に分布していないことから、修正後のビット・ストリームのデューティ・サイクルに非一様性が招かれる傾向を否定できない。

【００３８】

図９は、さらに別の実施形態、すなわちランダム・ビット・ソース２０２によって出力されるビットのペアの間における１次の自己相関の影響を軽減するデューティ・サイクル修正器９００を示している。デューティ・サイクル修正器９００は、ランダム・ビット・ソース２０２の、モジュロ５カウンタの特定のカウントに応じてシフト－インされたビットを破棄することによって、１次の自己相関を低減する。

【００３９】

デューティ・サイクル修正器９００は、デューティ・サイクル修正器３００に類似であるが、確認論理のトランスペアレント・ラッチ３０８が、モジュロ５カウンタ９０２、インバータ９０４、９０６、９０８、アンド・ゲート９１０、９１２、およびノア・ゲート９１４に置き換えられている点が異なる。モジュロ５カウンタ９０２は、３つのバイナリ出力ビットＣ０、Ｃ１、Ｃ２を有している。アンド・ゲート９１０は、３入力アンド・ゲートであり、第１の入力がインバータ９０４を介してＣ２に結合され、第２の入力がＣ１に結合され、第３の入力がインバータ９０８を介してＣ０に結合されている。アンド・ゲート９１２は、３入力アンド・ゲートであり、第１の入力がＣ２に結合され、第２の入力がインバータ９０６を介してＣ１に結合され、第３の入力がインバータ９０８を介してＣ０に結合されている。ノア・ゲート９１４は、アンド・ゲート９１０および９１２の出力を受け取り、アンド・ゲート３０９の一方の入力をドライブする。

【００４０】

デューティ・サイクル修正器９００の動作を図１０に示す。ステップ１０００およびモジュロ５カウンタ９０２のカウント「０」において、最初のビットがラッチ３０４にロードされる。カウント「０」と「１」については、信号ライン９１５上に信号がアサートされないことから、このビットは破棄される。ステップ１００２においては、カウント「１」と「２」に応答して、最初のペアとなるビットがランダム・ビット・ソース２０２からラッチ３０４および３０６にラッチされる。このラッチが、修正器１０００に最初のビット

を破棄させる。ステップ１００４およびカウント「２」においては、エクスクルーシブ－オア・ゲート３１０が、ペアを構成する２つのビットが等しいか否かを判断する。ペアとなるビットが等しいときには、ステップ１００６において、ＡＣＣＥＰＴ（アクセプト）のアサートおよびＳＴＢのアサートが行なわれることなく、このビットのペアが拒絶または破棄される。ステップ１００６においては、いずれのビットもラッチ３１２によってラッチされることがなく、また信号ライン２１４に出力されることもない。ステップ１００４およびカウント「２」において、２つのビットが互いに異なると判断されると、ステップ１００８においてＡＣＣＥＰＴ（アクセプト）がアサートされ、ＳＴＢがアサートされて、ラッチ３１２によりペア内の最初のビット（または、それに代えて２番目のビット）が出力される。

【００４１】

ステップ１０１０においては、カウント「３」および「４」に応答して、２番目のペアとなるビットがランダム・ビット・ソース２０２からラッチ３０４および３０６にラッチされる。ステップ１０１２およびカウント「４」においては、エクスクルーシブ－オア・ゲート３１０が、ペアを構成する２つのビットが等しいか否かを判断する。ペアとなるビットが等しいときには、ステップ１０１４において、ＡＣＣＥＰＴ（アクセプト）のアサートおよびＳＴＢのアサートが行なわれることなく、このビットのペアが拒絶または破棄される。ステップ１０１２およびカウント「４」において、２つのビットが互いに異なると判断されると、ステップ１０１６においてＡＣＣＥＰＴ（アクセプト）がアサートされ、ＳＴＢがアサートされて、ラッチ３１２によりペア内の最初のビット（または、それに代えて２番目のビット）が出力される。このプロセスが、ランダム・ビット・ソースから出力されるすべてのビットのペアに対する処理を完了するまで繰り返される。

【００４２】

図１１は、デューティ・サイクル修正器９００の動作をさらに別の形で示している。最初のビット、すなわちビット０は、修正器９００にロードされるが、最初のペアとなるビットがロードされるときに破棄される。最初のペアとなるビット（ビット１と２）は、ビット値が等しいことから破棄され、このビットのペアに関しては修正後のビットが生成されない。２番目のペアとなるビット（ビット３と４）はビット値が異なることから、デューティ・サイクル修正器９００が「０」を出力する。その後、モジュロ５カウンタ９０２のカウントが「０」に戻り、その結果、ビット５が破棄される。３番目のペアとなるビット（ビット６と７）もビット値が異なり、デューティ・サイクル修正器９００は「１」を出力する。最後のペアとなるビット（ビット８および９）はビット値が互いに等しく、したがって破棄される。

【００４３】

ビット０と５を破棄することによって２番目のビットのペア（ビット３と４）と３番目のビットのペア（ビット６と７）の間の１次の自己相関が低減される。修正後のビット・ストリームは、２番目のビットのペアと３番目のビットのペアの間における２次の自己相関の影響を受けるが、その有意性はあまり高くない。カウント「０」（カウント「５」、カウント「１０」等）で破棄されるビットは、ランダム・ビット・ストリーム内に一様に分布し、それらを除外しても、結果的に修正後のビット・ストリームに関するデューティ・サイクルは概略で一様になる。

【００４４】

図１２は、さらに別の実施形態、すなわちランダム・ビット・ソース２０２によって出力されるビットのペアの間における１次の自己相関の影響を軽減するデューティ・サイクル修正器１２００を示している。デューティ・サイクル修正器１２００は、ランダム・ビット・ソース２０２が出力したビットから、比較されるビットのペアの間に挟まれるビットを破棄することによって１次の自己相関を抑える。

【００４５】

デューティ・サイクル修正器１２００は、デューティ・サイクル修正器３００に類似であるが、確認論理のトランスペアレント・ラッチ３０８が、カウント「２」のときにのみ信

号ライン１２０４上に論理ハイの信号を出力するモジュロ３カウンタ１２０２に置き換えられている点が異なる。

【００４６】

デューティ・サイクル修正器１２００の動作を図１３に示す。ステップ１３００およびモジュロ３カウンタ９０２のカウント「０」において、最初のビットがラッチ３０４にロードされる。カウント「０」と「１」については、信号ライン１２０４上に信号がアサートされないことから、このビットは破棄されることになる。ステップ１３０２においては、カウント「１」と「２」に応答して、最初のペアとなるビットがランダム・ビット・ソース２０２からラッチ３０４および３０６にラッチされる。このラッチによって、修正器１２００が最初のビットを破棄する。ステップ１３０４およびカウント「２」においては、エクスクルーシブ－オア・ゲート３１０が、ペアを構成する２つのビットが等しいか否かを判断する。ペアとなるビットが等しいときには、ステップ１３０６において、ＡＣＣＥＰＴ（アクセプト）のアサートおよびＳＴＢのアサートが行なわれることなく、このビットのペアが拒絶または破棄される。ステップ１３０６においては、いずれのビットもラッチ３１２によってラッチされることがなく、また信号ライン２１４に出力されることもない。ステップ１３０４およびカウント「２」において、２つのビットが互いに異なると判断されると、ステップ１３０８においてＡＣＣＥＰＴ（アクセプト）がアサートされ、ＳＴＢがアサートされて、ラッチ３１２によりペア内の最初のビット（または、それに代えて２番目のビット）が出力される。このプロセスが、ランダム・ビット・ソースからの出力ビットのペアがすべて処理されるまで繰り返される。

【００４７】

図１４は、デューティ・サイクル修正器１２００の動作をさらに別の形で示している。最初のビット、すなわちビット０は、修正器１２００にロードされるが、最初のビットのペアがロードされるとき破棄される。最初のペアとなるビット（ビット１と２）の処理時においては、ペア内のビットが等しいことから破棄され、このビットのペアに関しては修正後のビットが生成されない。４番目のビット、すなわちビット３は、修正器１２００にロードされるが、２番目のペアとなるビットがロードされるとき破棄される。２番目のペアとなるビット（ビット４と５）はビット値が異なることから、修正器１２００が「０」を出力する。７番目のビット、すなわちビット６は、修正器１２００にロードされるが、３番目のペアとなるビットがロードされるとき破棄される。３番目のペアとなるビット（ビット７と８）はビット値が異なり、デューティ・サイクル修正器１２００は「１」を出力する。１０番目のビット、すなわちビット９は、修正器１２００にロードされるが、４番目のペアとなるビットがロードされるとき破棄される。４番目のペアとなるビット（ビット１０と１１）は、ビット値が等しいことから破棄される。

【００４８】

ビット０、３、６、９等を破棄することによって、比較を行うビットのペアの間における１次の自己相関が低減される。修正後のビット・ストリームは、比較を行うビットのペアの間における２次の自己相関の影響を受けるが、その有意性はあまり高くない。モジュロ３カウンタ１２０２のカウント０、３、６、９等において破棄されるビットは、ランダム・ビット・ストリーム内に一様に分布し、それらを除外しても、結果的に修正後のビット・ストリームに関するデューティ・サイクルは概略で一様になる。

【００４９】

以上、ランダム・ビット・ソースのランダム・ビット・ストリーム内の連続する２つのビットを比較するものとしてデューティ・サイクル修正器の説明を行ってきたが、変形実施形態として、連続しないビットを比較することもできる。たとえば、ストレージ回路２０４と２０６の間に追加のストレージ回路を挿入し、あるいはそれぞれのストレージ回路を異なるクロックもしくは異なるクロック・エッジを用いてクロックすることが考えられる。

【００５０】

また、ここで説明した出力回路２１２は、ストレージ回路２０４と２０６のうちのいずれ

か一方の出力を受け取る。変形実施形態においては、比較論理２０８に、ストレージ回路２０４と２０６にストアされているデータに応答して出力回路２１２に提供されるデータを決定する論理を含めることができる。

【００５１】

ランダム・ビット・ソースから実質的に一様な「１」と「０」の分布を生成するための、ここで説明したデューティ・サイクル修正器は、コンピュータ・ネットワークを介して送られるメッセージの符号化および復号化を行うための乱数発生器と組み合わせて使用することができる。図１５は、上記のいずれかの実施形態を使用して暗号化されたメッセージを送信するためのコンピュータ・ネットワークを示したブロック図である。ネットワーク１５００は、送信ホスト・コンピュータ１５０２およびネットワークを介してそれに結合された受信ホスト・コンピュータ１５０４を含んでいる。送信ホスト・コンピュータおよび受信ホスト・コンピュータは、ともにネットワーク・インターフェース・デバイスを備え、それによってホスト・コンピュータ・システムとネットワーク・メディアの間の物理的かつ論理的な接続が提供される。さらにいずれのホスト・コンピュータにも暗号化回路／解読回路が備わり、それが、データ通信のセキュリティに関する各種の暗号機能を実行する。送信ホスト１５０２は、暗号化回路／解読回路１５０６を備えており、受信ホスト１５０４は、暗号化回路／解読回路１５０７を備えている。暗号化回路／解読回路１５０６および１５０７には、それぞれ乱数発生器１５０８および１５０９が備わり、そこには、図２、３、６、９、または１２に示した実施形態のいずれかが採用されている。これらの乱数発生器は、公開キー／秘密キーシステムにおける公開キー／秘密キーの生成に使用される。

【００５２】

ネットワーク１５００においては、送信ホスト１５０２と受信ホスト１５０４の間の安全な通信を保証するために、各種のデータ暗号化方法を使用することができる。一実施形態においては、ネットワーク１５００が公開キー（非対称）暗号システムを使用する。公開キーシステムにおいては、２つの異なるキーが使用される。一方のキーは、送信側がメッセージの符号化のために使用し、他方のキーは、受信側が符号化されたメッセージの復号化のために使用する。このシステムにおいては、暗号化（公開）キーは広く公開してもよいが、復号（秘密）キーは、意図された受信側だけがメッセージの復号化を行えるように秘密にする必要がある。公開キーおよび秘密キーは、通常、非常に大きな素数および乱数からともに導かれる。したがって、真にランダムなキーのペアを生成するためには、効果的な乱数発生器が必要になる。

【００５３】

公開キーシステムを使用するデータ送信の例において、送信ホスト１５０２は、受信ホスト１５０４に送信するためのメッセージＭを作成する。この伝送のために使用される２つのキーは、受信側の公開キー（PuK_R）および受信側の秘密キー（PrK_R）からなる。通常、受信側は、公に入手可能な登録キーから公開キーを選択し、受信側のみが知っている変換プロセスを介して、当該公開キーから秘密キーを導く。つまり、一般に公開キーと秘密キーの間の相関は、秘密であり、かつ安全である。送信ホスト１５０２は、公開キーを使用し、暗号化回路／解読回路１５０６を介してメッセージを符号化し、符号化済みのメッセージＭ’を生成する。符号化が行なわれた後は、適切な秘密キーを使用しない限りメッセージを復号化することができない。受信ホスト１５０４は、メッセージを受信すると、秘密キーを用いてメッセージＭ’の復号化を行い、オリジナルのメッセージＭを取り出す。

【００５４】

一実施形態においては、受信ホスト１５０４内の暗号化回路／解読回路１５０７が、図２、３、６、９、または１２の実施形態のいずれかを採用した乱数発生器１５０９を備えている。このテクニックは、乱数発生器１５０９からのビットの分布が充分に一様かつランダムであり、そのため公開キーと、受信ホスト１５０４によって生成される秘密キーの間に一貫性のある相関が存在しない。ネットワーク１５００内に示されるように、送信ホス

ト１５０２内の暗号化回路／解読回路１５０６もまた、図２、３、６、９、または１２の実施形態のいずれかを採用した乱数発生器１５０８を備えている。これにより送信ホスト１５０２は、公開キーによる送信を採用するときの、安全な秘密キーおよび公開キーの生成が可能になる。これらのキーのペアの生成には、秘密キーの網羅的でないサーチが極めて困難になるように高度のランダム性が要求される。

【００５５】

別の実施形態においては、ネットワーク１５００が単一キー（対称）システムを使用して、暗号機能を実行する。単一キーシステムの場合には、送信側と受信側が１つのキーを共有し、それを使用して送信側はメッセージの暗号化を行い、受信側は、符号化されたメッセージの解読をおこなう。このシステムの信頼性は、キーのセキュリティに依存する。したがって、第三者に知られることのない、送信側と受信側の間のみにおけるキーの開示のために安全なプロセスが必要になる。この実施形態においては、通常、メッセージ・トランザクションが異なるごとに異なるキーが使用される。つまり、各種のキーが生成されることから、あるメッセージ・トランザクションに使用されるキーが、別のメッセージ・トランザクションに使用されたキーから決定不可能であることが保証される必要がある。このシステムの場合、ネットワーク１５００の各ホスト・コンピュータ内の暗号化回路／解読回路において、乱数発生器が使用されてホスト・コンピュータ間で送信されるメッセージ・データの符号化および復号化を行うためのランダムなキーパターンが生成される。

【００５６】

なお、ここでは単一キーおよび公開キー／秘密キー暗号システムとの関連から本発明の実施形態を説明したが、本発明の実施形態は、安全なコンピュータ・ネットワーキングのための、これ以外のタイプの暗号システムにも使用できることに注意する必要がある。さらに、図１５に示した暗号化回路／解読回路は、安全なデータ送信システムにおけるメッセージの符号化および復号化、送信されたメッセージの認証、ディジタル署名の検証、およびその他の機能を含めた各種の暗号機能の実行に使用することができる。

【００５７】

以上のとおり、一様なデューティ・サイクルの乱数発生器を作るための回路について説明した。ここでは、特定の具体例とする実施形態を参照して本発明についての説明を行ったが、特許請求の範囲に示される本発明の精神ならびに範囲はそれよりも広く、それから逸脱することなくこれらの実施形態に対して各種の修正ないしは変更を加え得ることは明らかである。したがって、明細書ならびに図面は、限定の意味ではなく例示と考える必要がある。

【図面の簡単な説明】

【図１】　リニア・フィードバック・シフト・レジスタを使用する従来の乱数発生器を示した図である。

【図２】　ランダム・ビット・ソースおよびデューティ・サイクル修正器の一実施形態を示したブロック図である。

【図３】　図２に示したデューティ・サイクル修正器の一実施形態を示した論理図である。

【図４】　図２に示したデューティ・サイクル修正器の動作を示したフローチャートである。

【図５】　図３に示したデューティ・サイクル修正器によって生成される修正後のビット・パターンの一例を示している。

【図６】　図２に示したデューティ・サイクル修正器の別の実施形態を示した論理図である。

【図７】　図６に示したデューティ・サイクル修正器の動作を示したフローチャートである。

【図８】　図６に示したデューティ・サイクル修正器によって生成される修正後のビット・パターンの一例を示している。

【図９】　図２に示したデューティ・サイクル修正器の一実施形態を示した論理図である

。

【図１０】　図１０に示したデューティ・サイクル修正器の動作を示したフローチャートである。

【図１１】　図９に示したデューティ・サイクル修正器によって生成される修正後のビット・パターンの一例を示している。

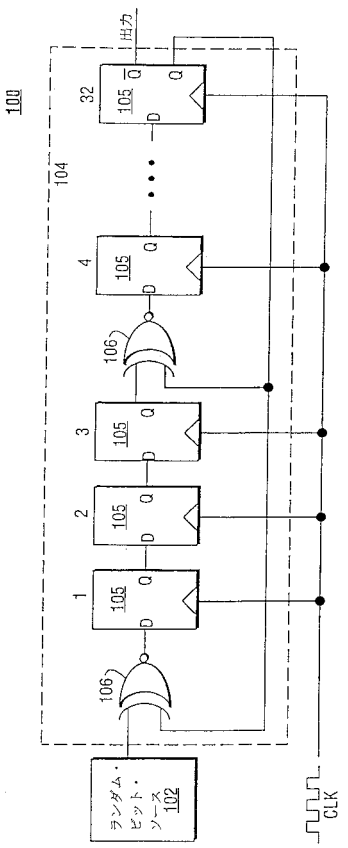
【図１２】　図２に示したデューティ・サイクル修正器の一実施形態を示した論理図である。

【図１３】　図１２に示したデューティ・サイクル修正器の動作を示したフローチャートである。

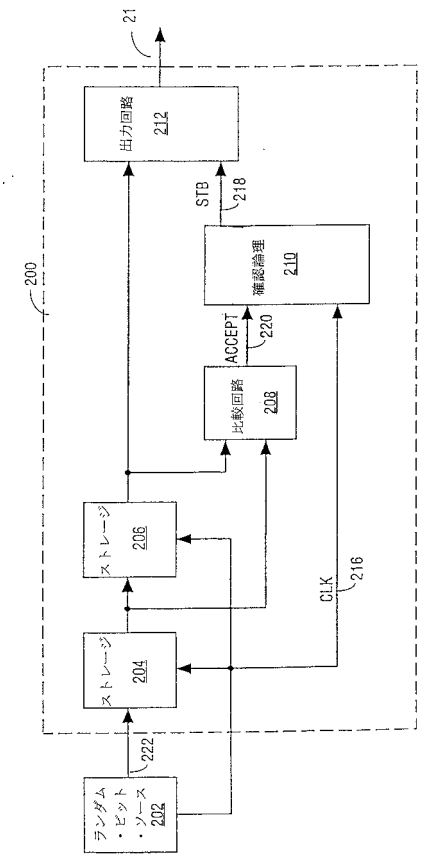
【図１４】　図１２に示したデューティ・サイクル修正器によって生成される修正後のビット・パターンの一例を示している。

【図１５】　本発明の一実施形態に従ったデータ暗号化／解読のためのビット・ペアリング・システムを使用するコンピュータ・ネットワークを示したブロック図である。

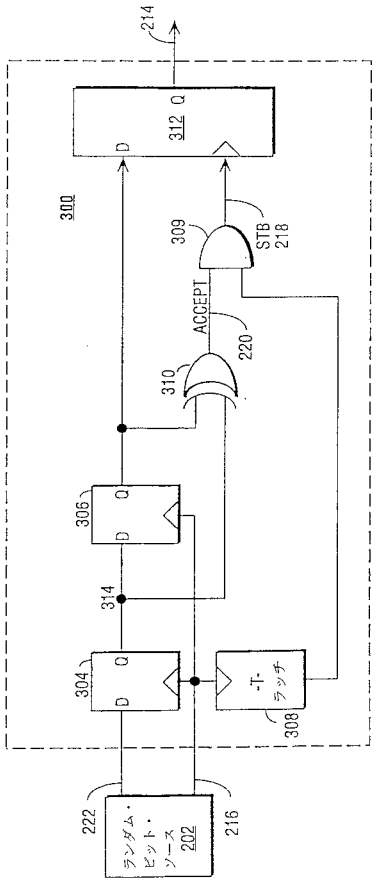
【図１】



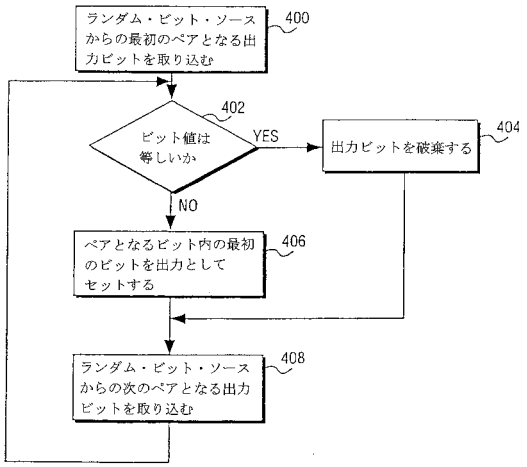
【図２】



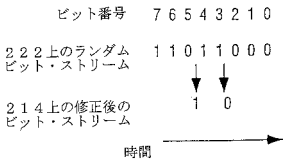
【図３】



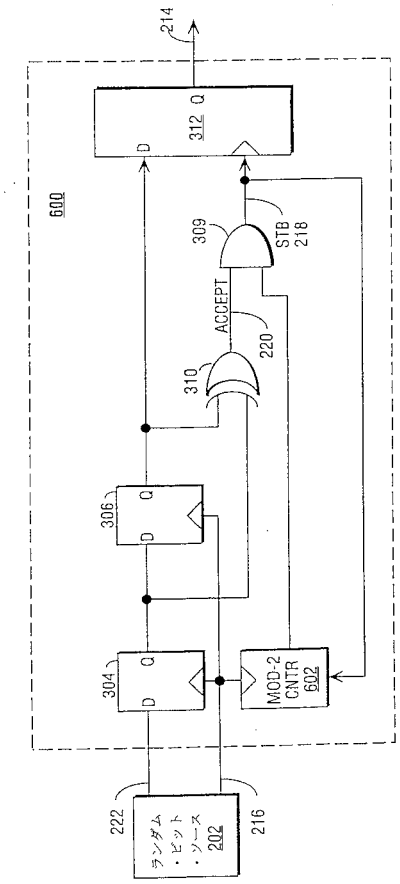
【図４】



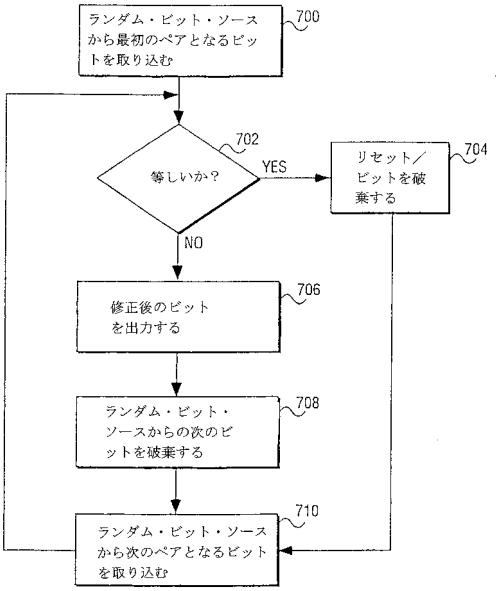
【図５】



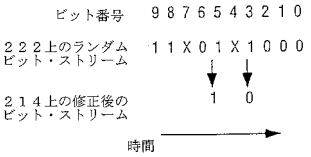
【図６】



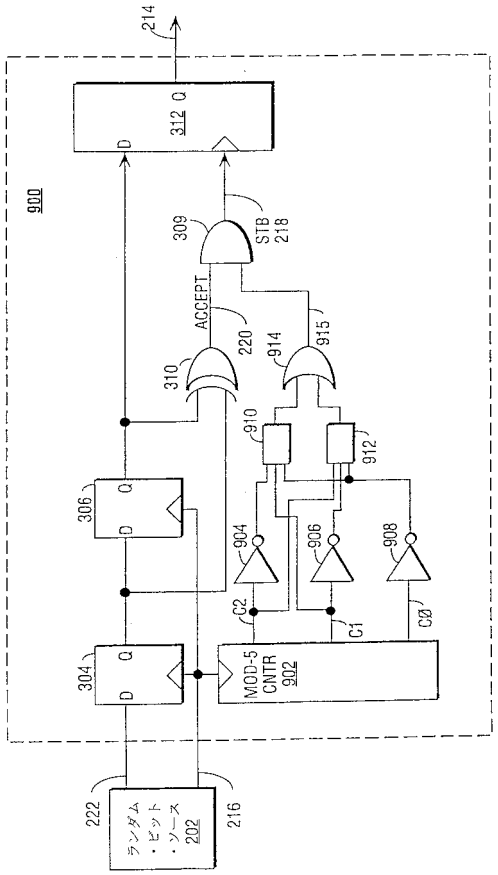
【図７】



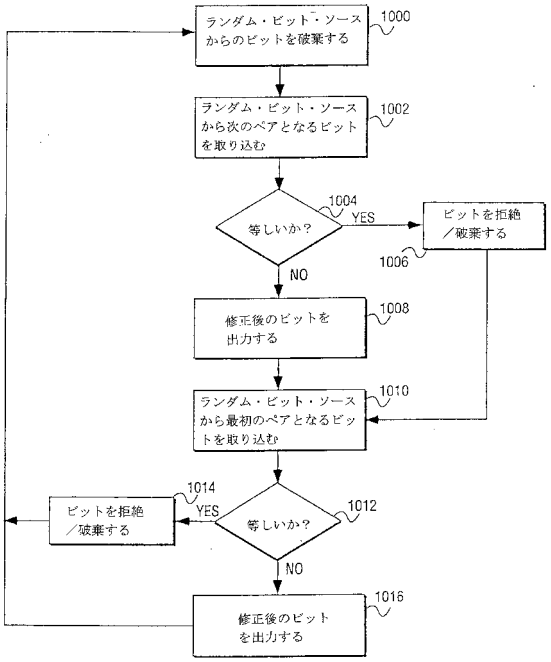
【図８】



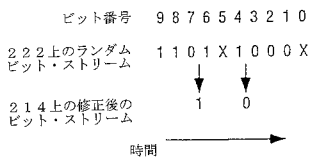
【図９】



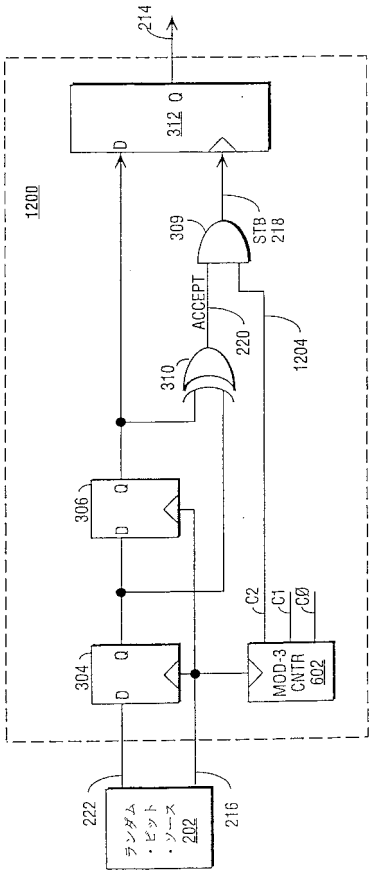
【図１０】



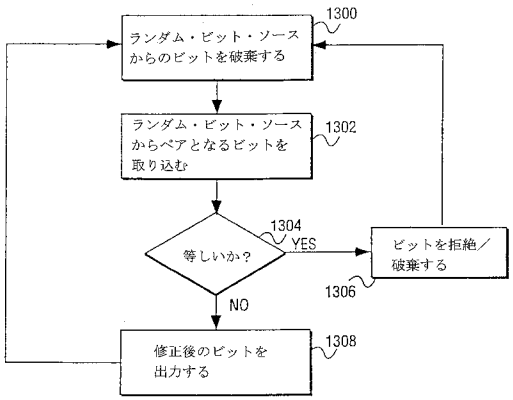
【図１１】



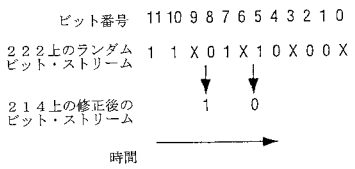
【図１２】



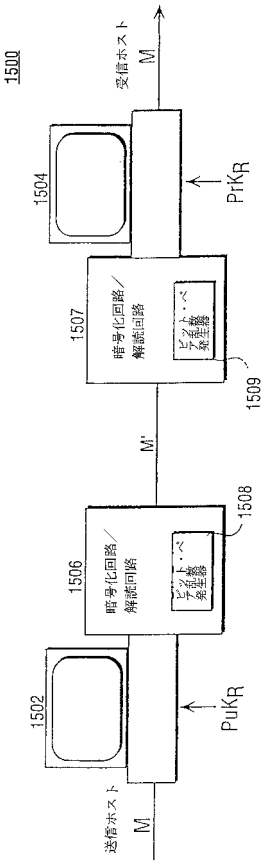
【図１３】


ランダム・ビット・ソースからのビットを破棄する
1300
ランダム・ビット・ソースからペアとなるビットを取り込む
1302
等しいか？
1304
YES
NO
ビットを拒絶／破棄する
1306
修正後のビットを出力する
1308

【図１４】


ビット番号 11 10 9 8 7 6 5 4 3 2 1 0
２２２上のランダムビット・ストリーム 1 1 X 0 1 X 1 0 X 0 0 X
２１４上の修正後のビット・ストリーム 1 0
時間

【図１５】


1500
受信ホスト
M
1504
PrKR
1507
暗号化回路／解読回路
ビット・ペア発生器
1509
M'
1508
1506
1502
PuKR
送信ホスト
M

フロントページの続き

審査官　中里　裕正

(56)参考文献　HANDBOOK of APPLIED CRYPTOGRAPHY, CRC PRESS, １９９６年１０月, p.171-173
Martin Luescher, A Portable High-Quality Random Number Generator for Lattice Field Theory Simulations, The Internet, １９９３年　９月２８日, ＵＲＬ, http://arxiv.org/abs/hep-lat/93020

(58)調査した分野(Int.Cl., ＤＢ名)
G09C　1/00
G06F　7/58
JSTPlus/JMEDPlus/JST7580(JDreamII)