

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4652568号

(P4652568)

(45) 発行日 平成23年3月16日(2011.3.16)

(24) 登録日 平成22年12月24日(2010.12.24)

(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 17 (全 16 頁)

(21) 出願番号	特願2000-535117 (P2000-535117)	(73) 特許権者	598036300
(86) (22) 出願日	平成11年2月9日(1999.2.9)		テレフオンアクチーボラゲット エル エ
(65) 公表番号	特表2002-506243 (P2002-506243A)		ム エリクソン (パブル)
(43) 公表日	平成14年2月26日(2002.2.26)		スウェーデン国 スtockホルム エスー
(86) 国際出願番号	PCT/SE1999/000172		1 6 4 8 3
(87) 国際公開番号	W01999/045673	(74) 代理人	100076428
(87) 国際公開日	平成11年9月10日(1999.9.10)		弁理士 大塚 康德
審査請求日	平成18年2月6日(2006.2.6)	(74) 代理人	100112508
(31) 優先権主張番号	09/036,390		弁理士 高柳 司郎
(32) 優先日	平成10年3月6日(1998.3.6)	(74) 代理人	100115071
(33) 優先権主張国	米国 (US)		弁理士 大塚 康弘
		(74) 代理人	100116894
			弁理士 木村 秀二
		(74) 代理人	100130409
			弁理士 下山 治

最終頁に続く

(54) 【発明の名称】 擬似ランダムシーケンス生成器及び生成方法

(57) 【特許請求の範囲】

【請求項 1】

ワードメモリと、イニシャライザと、出力シーケンスセクタと、新規メモリーワードセクタとを備える擬似ランダムノイズ生成器が擬似ランダムノイズシーケンスを生成する方法であって、

前記ワードメモリが、メモリーエレメントのセットを形成する形成工程であって、各メモリーエレメントが任意のワード長を有するメモリーワードを格納する、形成工程と、

前記イニシャライザが、前記形成工程で形成された各メモリーエレメントを初期状態で初期化する初期化工程であって、各メモリーエレメントの初期化に用いられる前記初期状態値が前記メモリーエレメントに格納されるメモリーワードを形成する、初期化工程と

10

前記出力シーケンスセクタが、出力シーケンスを形成するために、少なくとも一つの前記メモリーエレメントに格納された少なくとも一つの前記メモリーワードを選択する選択工程であって、前記出力シーケンスは、擬似ランダムノイズシーケンスの一部を形成する、選択工程と、

前記新規メモリーワードセクタが、前記メモリーエレメントのセットの少なくとも一つの前記メモリーエレメントに格納される少なくとも一つの新規のメモリーワードを選択する工程であって、前記新規メモリーワードは、前記メモリーエレメントセット内の前記メモリーエレメントに格納された前記メモリーワードの任意の結合で構成され、前記少なくとも一つの新規メモリーワードのワード長は、前記出力シーケンスを形成するために選

20

択されたメモリーワードのワード長と一致する、工程とを備え、

前記擬似ランダムノイズシーケンスが所定の次数のウィンドミル多項式によって生成された値と一致する値を有し、前記所定の次数は、少なくとも部分的に、前記形成工程において形成された前記メモリーエレメントセットの前記メモリーエレメントの数に限定される

ことを特徴とする方法。

【請求項 2】

前記メモリーエレメントセットのメモリーエレメントの数が、さらに前記各メモリーワードを形成するワード長に反比例することを特徴とする、請求項 1 に記載の方法。

10

【請求項 3】

前記メモリーエレメントセットを形成するメモリーエレメントの数が、選択された次数に正比例することを特徴とする請求項 2 に記載の方法。

【請求項 4】

前記形成工程において形成された前記メモリーエレメントセットが、出力メモリーエレメントを形成するために選択された複数メモリーエレメントのスタックのうちの少なくとも一つのメモリーエレメントである、メモリーワードのスタックを形成する、前記メモリーエレメントの論理的に連続したグループを備え、少なくとも一つの前記メモリーワードを選択する前記工程において選択されたメモリーワードの少なくとも一つが、出力メモリーエレメントに格納された少なくとも一つのメモリーワードを備えることを特徴とする請求項 1 に記載の方法。

20

【請求項 5】

前記メモリーエレメントの論理的に連続するグループの連続が列を定義し、かつ、メモリーワードを列方向に、メモリーエレメントのスタックを通してシフトされることを特徴とする請求項 4 に記載の方法。

【請求項 6】

前記少なくとも一つの新規メモリーワードを選択する工程において選択された前記少なくとも一つの新規メモリーワードが、前記任意の次数のウィンドミル多項式によって生成された帰還値に一致する値のメモリーワードを備えることを特徴とする請求項 5 に記載の方法。

30

【請求項 7】

前記メモリーエレメントの任意の少なくとも一つに、少なくとも一つの巡回更新ポイントが割り当てられることを特徴とする請求項 1 に記載の方法。

【請求項 8】

割り当てられた前記少なくとも一つの巡回更新ポイントが、前記選択工程において選択されたメモリーワードが格納されている少なくとも一つの前記メモリーエレメントを識別することを特徴とする請求項 7 に記載の方法。

【請求項 9】

割り当てられた前記少なくとも一つの巡回更新ポイントが、少なくとも一つの新規メモリーワードを選択する前記工程において選択され、前記少なくとも一つの新規メモリーワードが格納される、少なくとも一つのメモリーエレメントを識別することを特徴とする請求項 8 に記載の方法。

40

【請求項 10】

前記形成工程において形成されたメモリーエレメントのそれぞれに格納されている前記メモリーワードのそれぞれの任意のワード長が、互換性のあるワード長を形成する任意のワード長の少なくとも一つの倍数となるように選択され、前記選択工程において選択された少なくとも一つのメモリーワードが、少なくとも一つの単一メモリーワードの倍数を備えることを特徴とする請求項 1 に記載の方法。

【請求項 11】

前記出力シーケンスを構成するために前記メモリーワードの少なくとも一つを選択し、

50

かつ、前記新規メモリーワードの少なくとも一つを選択する前記工程が、反復的に実施されることを特徴とする請求項 1 に記載の方法。

【請求項 1 2】

任意のウィンドミル多項式のために、共通の擬似ランダムシーケンスを生成するためのウィンドミル多項式生成器の代替構成の互換性を決定する、特徴付け手段と、決定手段と、識別手段とを備える装置における、該互換性の決定方法であって、前記任意のウィンドミル多項式がウィンドミル多項式次元及び、ウィンドミル多項式重みによって識別される方法が、

前記特徴付け手段が、第一の多項式部分と、第二の多項式部分とによって前記ウィンドミル多項式を特徴付ける工程であって、前記第一の多項式部分の次数が前記ウィンドミル多項式の次数と一致している、工程と、

10

前記決定手段が、前記第二の多項式部分の特性を決定する工程であって、前記第二の多項式部分は前記第一の多項式部分と結合して前記ウィンドミル多項式を形成し、前記第二の多項式部分の各特性がウィンドミル多項式生成器の分離構成を識別し、前記第二の多項式部分の特性のそれぞれが所定の基準を満たすかどうかを決定する、工程と、

前記識別手段が、前記特性が前記所定の基準を満たしている場合に、ウィンドミル多項式生成器が互換性のある代替構成を有すると識別する工程とを備えることを特徴とする方法。

【請求項 1 3】

前記第二の多項式部分の各特性が、ワードサイズを識別する設計べき指数と関連することを特徴とする、請求項 1 2 に記載の方法。

20

【請求項 1 4】

前記第二の多項式部分が前記所定の基準を満たすかどうかを決定するための前記所定の基準が、等式 $1 = L \bmod v$ を備え、ここで、 L が前記ウィンドミル多項式の次数であり、 v が前記第二の多項式部分に関連する設計べき指数であることを特徴とする請求項 1 2 に記載の方法。

【請求項 1 5】

前記所定の基準を前記特性のそれぞれが満たすかどうかを決定するための前記所定の基準が、等式 $v - 1 = L \bmod v$ を備え、ここで、 L が前記ウィンドミル多項式の次数であり、 v が前記第二の多項式部分に関連する設計べき指数であることを特徴とする請求項 1 2 に記載の方法。

30

【請求項 1 6】

擬似ランダムノイズシーケンスを生成するための擬似ランダムノイズ生成器であって、任意のワード長を有するメモリーワードをそれぞれのメモリーエレメントに格納するためのメモリーエレメントセットと、

前記セットの各メモリーエレメントを初期状態値で初期化するためのイニシャライザと、

前記セットのメモリーエレメントの少なくとも一つに格納されている、少なくとも一つのメモリーワードを選択するための出力シーケンスセクタであって、前期出力シーケンスが擬似ランダムノイズシーケンスの一部を構成する出力シーケンスセクタと、

40

前記セットのメモリーエレメントの少なくとも一つに格納される、少なくとも一つの新規メモリーワードを選択するための新規メモリーワードセクタであって、前記新規メモリーワードが、前記メモリーエレメントのセットのメモリーエレメントに格納されたメモリーワードの任意の結合から構成されており、少なくとも一つの新規メモリーワードのワード長が出力シーケンスを構成するために選択されたメモリーワードのワード長と一致する、新規メモリーワードセクタとを備え、

前記擬似ランダムノイズシーケンスが所定の次数のウィンドミル多項式によって生成された値と一致する値を有し、前記所定の次数は、少なくとも部分的に、前記形成工程において形成された前記メモリーエレメントセットの前記メモリーエレメントの数に限定され

50

る
ことを特徴とする擬似ランダムノイズ生成器。

【請求項 17】

任意のウィンドミル多項式のために、共通擬似ランダムシーケンスを生成するための、ウィンドミル多項式生成器の代替構成の互換性を決定する装置であって、前記任意のウィンドミル多項式が、ウィンドミル多項式次数及びウィンドミル多項式重みシーケンスによって識別される装置が、

前記ウィンドミル多項式を第一の多項式部分と第二の多項式部分とにより特徴づける特徴付け手段であって、前記第一の多項式部分の次数は、前記ウィンドミル多項式の次数と一致している、特徴付け手段と、

前記第二の多項式部分の特性を決定する決定手段であって、前記第二の多項式部分の各特性によりウィンドミル多項式生成器の分離構成を識別し、所定の基準を前記第二の多項式部分の各特性が満たすかどうかを決定する決定手段と、

前記所定の基準を前記特性が満たす場合には、ウィンドミル多項式生成器が互換性のある代替構成を有すると識別するための識別手段と
を備えることを特徴とする決定装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は一般には、例えば暗号化処理において利用されるような擬似乱数シーケンスの生成に関連する。より詳細には、本発明は、任意のウィンドミル多項式により生成されたシーケンスに一致する擬似乱数シーケンスを生成するための擬似乱数シーケンス生成器及び、生成方法に関連する。本発明は、さらには、ウィンドミル多項式ベースの擬似乱数シーケンス生成器の異なる構成間の互換性を決定する方法と関連する。

【0002】

ワード志向のメモリーエレメントは擬似乱数シーケンスを形成するワードを格納するために利用される。メモリーワードのサイズは、ウィンドミル生成器の代替的な互換性のある構成に一致する、同一の擬似乱数シーケンスの生成を増加促進するために、継続的な反復動作の間にウィンドミルによって生成されるシーケンス部が直ちに増加するように選択される。

【0003】

本発明の実施形態により生成される擬似乱数シーケンスは、セルラー通信システムの移動局と無線基地局の間で形成されるような、無線リンクを介して通信されるデータを暗号化するためにシステムの一部として有益に利用される。本発明の実施形態の作用により生成される擬似乱数シーケンスはまた、スペクトル拡散通信（CDMA）、自動レンジングシステム、音声信号圧縮方法、及びレーダーシステムにおいて有益に利用される。

【0004】

【従来の技術】

[発明の背景]

通信システムは、送信局と受信局の間で通信チャネル方法により情報通信を行うことができる。有線通信システムでは、通信チャネルが送受信局の間で固定的な接続により形成されている。そして、無線通信システムでは、通信チャネルは電磁波周波数スペクトラムの一部を形成する。無線通信システムの送受信局間で通信チャネルを形成するのに固定的な接続は必要とされないので、送受信局間での固定的な接続が実用的でない場合にも通信が可能となる。

【0005】

ディジタル通信システムは、送信局から受信局に通信される情報がディジタル化される通信システムである。ディジタル通信システムは、有線通信システム及び無線通信システムの両方で実現できる。ディジタル通信システムは、送受信局間に及ぶ通信チャネルのより効果的な利用を可能とし、これにより通信システムの通信容量は従来のアナログ通信シス

10

20

30

40

50

テムよりも増加することになる。

【0006】

送受信局間の通信は時には必然的に秘密であることが要求される。即ち、通信信号を送受信する当事者が、送受信当事者のみが通信信号の情報の内容にアクセスできることを意図することがある。特に、通信チャネルが無線通信システムの無線通信チャネルである場合は、送受信局間の通信プライバシーには問題が多い。無線チャネルは元来全く公のものであるので、通信チャネルにより転送される通信信号は、通信信号の範囲内の、無線チャネルに同調されたいかなる受信局によっても検出できる。不許可のパーティーは、例えば、無線受信機を通信信号が伝送される無線チャネルの周波数に同調させることができ、これにより通信信号を受信できる。同様のセキュリティ問題は、不許可のパーティーによる有線通信チャネルへのアクセスが増加する状況では、有線通信システムにおける考慮事項でもある。

10

【0007】

通信システムにおける通信の安全性を改善する一つの手法は、通信信号を形成する情報を暗号化することである。許可されたパーティーのみが暗号化された通信信号を復号化できるとすると、不許可のパーティーは通信チャネルで伝送される通信信号の情報内容を理解できない。これにより、通信の秘密がより保証されることになる。

【0008】

ディジタル情報信号は特に暗号化処理と相性がよい。ディジタル情報信号は、ビットシーケンスで形成され、要求があれば、情報信号の各ビットは送信局において通信チャネルでの伝送前に暗号化される。情報信号の暗号化方法を知らない不許可のパーティーは、受信信号を復号化して伝送信号の情報内容を復元することができない。暗号化された信号を復号化できる受信局のみが、受信信号の情報内容を復元できる。

20

【0009】

さまざまな手法がディジタル情報信号を暗号化するために利用されている。セルラー通信において用いられるような典型的な暗号化手法は、情報信号のディジタルビットが擬似乱数シーケンス生成器により生成される擬似乱数シーケンスのビットと結合される暗号化手法を利用している。擬似乱数シーケンス生成器は、対称暗号化方式において、送信局及び許可された受信局に既知な秘密鍵と結合して実現される。秘密鍵は許可された受信局で受信した暗号化信号を復号化するのに利用され、それにより伝送信号の情報内容が復元される。

30

【0010】

擬似乱数シーケンスは場合によっては、ウィンドミル多項式の計算から導出される。ハードウェアやソフトウェアで実装されようと、擬似乱数シーケンスをこの手法で生成する構成は、ウィンドミル生成器として引用されることがある。ウィンドミル生成器により生成される出力ビットは、とりわけ情報信号を暗号化するために利用される擬似乱数シーケンスを形成する。ウィンドミル生成器は、ある有限体 $GF(q)$ 上の選択された原始多項式に直接関連する。 $q=2$ の場合、有限体 $GF(2)$ は、バイナリケースとして引用され、ディジタル通信において特に重要である。ウィンドミル生成器を導く原始多項式の数、多項式の多くの制約により制限される。特にバイナリケースにおいて、出力に必要な処理を最小にするために、多項式のノンゼロ係数がわずかでなければならぬ場合は、ウィンドミル多項式を形成するために利用される適切な多項式の数、多項式のノンゼロ係数の数は、多項式の重みとして引用される。

40

【0011】

$GF(2)$ のバイナリケースならば、3つまたは5つのノンゼロ係数及び5000次までの次数を有する多項式のような、原始多項式をリストするテーブルが存在する。

【0012】

重み3のバイナリウィンドミル多項式で生成される、ここでしばしば n タプルとして引用される出力のランダム性は一般に乏しく、出力のランダム性を増加させるために高い重みの多項式が必要となる。しかし、そのような改善されたランダム性は、処理要求の増大によ

50

る出費の原因となる。既存のテーブルは、擬似乱数シーケンスを導くためのウィンドミル多項式を選択するのに必ずしも利用することができない。というのも、そのような既存のテーブルが3つまたは5つのノンゼロ係数を伴う全ての原始多項式を必ずしも示す訳ではないからである。特に、擬似乱数シーケンスが暗号化処理に利用される場合には、有限体GF(2)での任意の次数の全てのウィンドミル多項式が分かっていることは価値がある。しかし、そのような知識を導くための方法はない。代わりに、従来、Knuth Allanenテストのような原始的であるかどうかのテストを含む検証プロセスが実施される。

【0013】

従来のウィンドミル生成器から得られるヴェインは、生成器で形成された出力のビットサイズ、即ち、 n タプルを決定する。処理速度のより高い処理装置の連続的な発生と共に処理性能が改善されるので、膨大なヴェインを有する従来ウィンドミル生成器はいよいよ実用的なものとなる。多数のヴェインを有するウィンドミル生成器からは、より大きなビットサイズの出力を得ることができる。ゆえに、擬似乱数シーケンスをより早く生成することができる。

10

【0014】

ウィンドミル生成器が他のウィンドミル生成器と互換性のある構成の場合、同一擬似乱数シーケンスは各構成の生成器で生成される。そのような互換性は、異なる構成のウィンドミル生成器を利用する装置及び方法から同一結果を得るために一般に必要とされる。

【0015】

しかしながら、ウィンドミル生成器の異なる構成の互換性を簡単に決定する方法は存在しない。従来、分離構成間の互換性は、ある構成のある初期状態を別の構成のそれに写像することによってのみ実現された。しかし、そのような写像は、膨大な操作を必要とした。しかしながら、特別のウィンドミル多項式は、構成間の実に単純な変換を可能とする。

20

【0016】

従って、共通の擬似乱数シーケンスを生成するためのウィンドミル生成器の代替構成の互換性を決定する方法を提供することは有効である。

【0017】

さらに、単純化された構成であって、任意のウィンドミル多項式に一致する擬似乱数シーケンスを生成するだけでなく、要求があれば代替構成に簡単に変換することができるウィンドミル生成器を提供することは有効である。

30

【0018】

擬似乱数シーケンスの生成に関連するこの発明の背景を考慮して、本発明の重要な改良点を以下に説明する。

【0019】

[発明の要約]

本発明は、共通の擬似乱数シーケンスを生成するウィンドミル生成器の代替構成の互換性を決定する方法を提供するものである。

【0020】

本発明は、さらに、単純化された構成であって、選択されたウィンドミル多項式に一致する擬似乱数シーケンスを生成するだけでなく、要求があれば代替構成に変換することができるウィンドミル生成器を提供することができる。

40

【0021】

ウィンドミル生成器の構成は、任意の初期状態で初期化された場合、同一の擬似乱数シーケンスを形成する n タプルを生成するものと同一視される。同一視された構成は、単純な関係をお互いに有する。即ち、同一擬似乱数シーケンスを生成する異なる構成操作において、任意の関係の結果の初期状態値を単にコピーすることによって同一視される。そのようなコピーは、状態空間内の次元、即ち生成する多項式の次数で線形複雑度を有し、従来ある初期状態を等価な状態に写像することを必要とするに二次元複雑度を有しない。

【0022】

一の実施態様では、本発明の実施形態であるウィンドミル生成器により生成される擬似乱

50

数シーケンスは、受信局へ送信局から伝送される情報の暗号化のための補助構成部分として利用される。典型的な実施形態において、通信システムは、セルラー通信システムを構成し、移動局とセルラー通信システムのネットワークインフラとの間で通信される情報は、ウィンドミル生成器によって生成された擬似乱数を利用して暗号化される。受信信号の復号化は、同様にまたウィンドミル生成器によって生成された擬似乱数シーケンスを利用して行われる。

【0023】

本発明の別の側面では、特定の最長シーケンス及びフルレンジシーケンスにおける擬似ランダムノイズシーケンスの有効な一貫性のあるブロックを生成することにより能率的な方法を提供する。擬似乱数シーケンスを生成するためにワード志向のメモリーを利用して

10

【0024】

これらの側面において、方法及び関連する装置は、擬似ランダムノイズシーケンスを生成する。メモリーエレメントのセットは、セットのメモリーエレメントのそれぞれが、その任意のワードプレーンのメモリーワードを格納する。メモリーエレメントのそれぞれは、初期状態値によって初期化される。メモリーエレメントそれぞれの初期化に用いられる初期状態値は、そこに格納されるメモリーワードを構成する。少なくとも一つのメモリーエレメントに格納される少なくとも一つのメモリーワードが、出力シーケンスを生成するために選択される。出力シーケンスは、擬似ランダムノイズシーケンスの一部を構成する。少なくとも一つの新規メモリーワードが、メモリーエレメントセットの少なくとも一つのメモリーエレメントに格納されるために選択される。新規メモリーワードは、メモリーエレメントセットのメモリーエレメントに格納されたメモリーワードの任意の結合から構成される。新規メモリーワードの少なくとも一つの数値は、出力シーケンスを形成するために選択されたメモリーワードの数と一致する。

20

【0025】

本発明のより完全な理解及び範囲は、以下に簡単な概要を示した添付図面、発明の好適な実施形態に係る以下の詳細な説明、及び、請求の範囲の記載より得ることができる。

【0026】

[発明の実施形態]

30

最初に図1を参照すると、10で示される典型的なウィンドミル生成器は、複数の遅延要素12で形成され、かつ、ヴェイン v のセットに分割されている。ここで、各ヴェインは長さ L_i を有し、各ヴェイン v は加算器16の入力端と接続される帰還ループ14を含む。右端のヴェイン v は左端のヴェインの入力端と帰還ループ18によって更に接続される。

【0027】

タップ22は、ヴェイン v の各々からとられ、かつ、タップ22から提供されるシーケンスについて順列を行う順列器へ提供される。順列器24で形成された出力シーケンスは、ライン26上に生成される出力エンドタプルを形成し、図中 S_{3j} 、 S_{3j+1} 、 S_{3j+2} で表される。

40

【0028】

各ヴェイン v の長さ L は、 L_i ($i=0,1,\dots,v-1$) で定義される。 L_0 から L_{v-1} の長さのセットは、既知の手法によって決定される。 $L = L_0 + L_1 + \dots + L_{v-1}$ の場合は、以下の式を満たす。

【0029】

$L = 1 \pmod v$ (L を v で割った余りが1) 又は

$L = (v-1) \pmod v$

上記第一の式に従えば、順列器24によって行われる順列を、同一順列、即ち $0,1,\dots,v-1$ を $0,1,\dots,v-1$ に写像するように選ぶことができる。この場合、長さ L_i は、次式を満たす。

50

$$L_0 = \dots = L_{v-2} = (L-1)/v, L_{v-1} = 1 + (L-1)/v$$

出力タップ 22 は各 $(L-1)/v$ 番目の遅延要素 12 の後得られる。

【0030】

上記第二の式を考慮すれば、順列の選択を、 $0, 1, \dots, v-1$ を $v-1, \dots, 1, 0$ に写像する、“逆順”にすることができる。長さ L は、この場合、次式によって定義される。

$$L_0 = \dots = L_{v-2} = (L+1)/v, L_{v-1} = -1 + (L+1)/v$$

各ヴェイン v から得られた出力タップ 22 は、 p 番目の遅延要素 12 の後ろに配置される。ここで p は、最大許容互換 v 値に依存する数である。ウィンドミル生成器 10 の初期状態 v とウィンドミル生成器 10 の初期状態 v' との間に、両ウィンドミル生成器 10 が同一の出力シーケンスを生成するための単純な写像関係があれば、 v 及び v' の二つの値は互換性を有する。即ち、ウィンドミル生成器 10 の出力は、次式を満たす。

10

【0031】

$S_j = f_1 S_{(j-1)} + f_2 S_{(j-2)} + \dots + f_L S_{(j-L)}$ ここで、 $j=n, n+1, \dots$ また、 $+$ は有限体 $GF(2)$ における加算を意味し、 $f(x) = 1 - f_1 x^{L-1} - \dots - f_{L-1} x^{L-1} - f_L x^L$

図 2 は、ウィンドミル生成器 10 の 9 時限 $j=0-8$ の連続的な反復操作を行った場合の、遅延要素 12 における値をリストしたテーブルを示す。テーブル 28 の右側は、ウィンドミル生成器 10 によってライン 22 上に生成された出力をリストしたものであり、順列器 24 による同一順列によってライン 26 上でも同順である。

【0032】

図 3 は、ヴェイン v のグループ、遅延要素 12、帰還ループ 14、加算器 16 からなるウィンドミル生成器を示す図である。帰還ループ 18 はまた、右端ヴェイン v と左端ヴェイン v との間でも形成される。タップ 22 は、再度ヴェイン v から取られている。ここで、ウィンドミル生成器 10 が 6 つのヴェインを包含するように、生成器 10 は 6 つのタップ 22 を包含する。同一順列で順列を行う順列器 24 及び、そこからの出力 26 が再度図示されている。

20

【0033】

図 4 は、テーブル 28 と類似するリストを含むテーブル 34 を図示するが、ここでは、図 3 の 6 ヴェインウィンドミル生成器の遅延要素 12 の状態値も示している。右端列は、タップ 22 によってタップされ、ライン 26 上に生成された値を示す。図 1 と図 3 及びテーブル 28 及び 34 に示されたウィンドミル生成器 10 のシーケンス出力を比較するとその共通性が分かる。

30

【0034】

図 1 のウィンドミル生成器 10 のそれぞれのヴェイン v は、同一の帰還接続を持っている。同様に、図 3 のウィンドミル生成器 10 の各ヴェイン v も同一の帰還接続を含んでおり、これは、ウィンドミル多項式 $f(x)$ から導かれる。ウィンドミル多項式 $f(x)$ は、第一の多項式部分と第二の多項式部分に書き換えることができる。それは以下になる。

【0035】

$$f(x) = 1 - f_1 x^{L-1} - \dots - f_{L-1} x^{L-1} - x^L \quad (f_i \text{ は } GF(q) \text{ の要素である。})$$

$$= b(x^v) - x^L$$

多項式 $f(x)$ がこれにより再度特徴付けられる時、ヴェイン v におけるフィードバックは、多項式 $b(x)$ によって特定される。

40

【0036】

バイナリの場合、即ち、有限体が $GF(2)$ で、 $f(x)$ が以下で表される場合は、

$$f(x) = 1 + f_1 x^{L-1} + \dots + f_{L-1} x^{L-1} + x^L \quad 7 \text{ 次のウィンドミル多項式は、}$$

$$f(x) = x^7 + x^6 + 1 \quad \text{となる。}$$

【0037】

これにより図 1 及び図 3 に示されたウィンドミル生成器を実現し、ウィンドミル多項式は以下のように書き換えることができる。

$$f(x) = b(x^3) + x^7$$

ここで、 $b(x) = 1 + x^2$ 。 $F(x)$ はまた、他の方法によっても書き換えることができ、二つの独

50

立多項式部により形成され、例えば、

$$f(x)=b(x^6)+x^7$$

ここで、 $b(x)=1+x$ and $v=6$

図1及び図3に示されたウィンドミル生成器の遅延要素12のそれぞれの初期状態値の適切な選択を通じて、ウィンドミル生成器の独立構成により、生成器10のそれぞれの構成のライン26上の連続的なエンドタプルから形成される同一擬似乱数シーケンスの生成が可能となり得る。L次のウィンドミル多項式は、ウィンドミル生成器10を許容し、 $v1$ ヴェインまたは $v2$ ヴェインを有し、上記等式 ($1=L \bmod v1=L \bmod v2$, $v-1=L \bmod v1=L \bmod v2$) を満たす場合、初期状態値の簡単な写像は、同一の擬似乱数シーケンスを生成する異なる構成を許容する。

10

【0038】

図5は、典型的な7次のウィンドミル多項式における写像を示す。上段は、初期状態値を図示するもので、図1のウィンドミル生成器10のヴェイン2、ヴェイン1、ヴェイン0における文字a,b,c,d,e,f及びxで示されている。下段は、図3に示されたウィンドミル生成器10のヴェイン5、ヴェイン4、ヴェイン3、ヴェイン2、ヴェイン1、ヴェイン0の6 ヴェインvに写像された初期状態値を図示するものである。図示された初期値の写像は、同一擬似ランダム出力シーケンスを生成するための図1及び図3それぞれのウィンドミル生成器10の独立の構成を許容する。

【0039】

$v1-1=L \bmod v1, v2-1=L \bmod v2$ の時、互換値vの簡単な写像、異なる構成のウィンドミル生成器の形成は、以下の等式で決定される。ここでpは、例えば、p番目の遅延要素のように使用されるが、最大許容互換v値に依存する数である。

20

【0040】

$$p=(L+1-v_{\max})/v$$

ここで、 $v_{\max}$ は、あるウィンドミル多項式についてのvの最大互換値である。

【0041】

例えば、17 次のウィンドミル多項式ならば、 $f(x)=x^{17}+x^{12}+1$ 、 $v_{\max}=6$ かつ $p=4$ となる。

【0042】

図6は、上記二つの場合における出力エンドタプルを示す。図の左部において、各ヴェインにおける出力タップを形成するビットは、pで示される列から取られる。その一方で、図の右部は、 $v_{\max}$ の値により異なる列から取られた出力ビットを示す。

30

【0043】

図7は、バイナリ3タプルのブロックを生成するために利用される127次までのウィンドミル多項式のテーブルを示す。各3タプルは63nタプルまでの同一ウィンドミル多項式を導くことができるウィンドミル生成器によって生成されるような8値の整数番号を表す。図7のテーブルはさらに、同一擬似乱数シーケンスを生成できるウィンドミル生成器の異なる構成をもたらすヴェインvの許容値を示す。

【0044】

図8は、各ウィンドミル多項式についての許容v値を生成する、一般に52において示される方法を図示する。方法52は、選択されたウィンドミル多項式について、共通の擬似乱数シーケンスを生成するウィンドミル多項式生成器の代替構成の互換性を決定することができる。第一に、ブロック54に示されているように、選択されたウィンドミル多項式は、第一の多項式部分及び第二の多項式部分によって特徴付けられる。即ち、ウィンドミル多項式 $f(x)$ は、 $b(x^v)-x^L$ によって上述のように特徴付けられ、 $f(x)$ は原始的かどうかをチェックされる。そして、ブロック56に示されるように、第二の多項式部分の特性は、第一の多項式部分と足し合わされると、任意のウィンドミル多項式を構成する。第二の多項式部分のそれぞれの特性は、ウィンドミル生成器の独立した構成と結びつく。すなわち、 $b(x^v)$ の異なる値が選択される。

40

【0045】

50

そして、ブロック 58 に示されているように、 $b(x^v)$ の特性のそれぞれが任意の基準を満たすかどうか決定される。即ち、選択された基準は $l=L \bmod v$ 又は $v-l=L \bmod v$ のいずれかを満たすことを要求する。

【0046】

最後に、ブロック 62 に示されているように、ウィンドミル生成器の特徴は、もし任意の基準をその特徴が満足するならば、互換性のある代替構成として識別される。

【0047】

図 9 は、本発明の実施形態に基づくウィンドミル生成器 (100) を示す。ウィンドミル生成器 100 は、図 1 及び図 3 に示されたウィンドミル生成器 10 と機能的に等価であるが、ここではワード用メモリを使って実現されている。ここで、メモリーエレメント 104 のスタック 102 が形成されている。メモリーエレメント 104 のそれぞれは、任意のワード長を有し、スタック 102 はメモリーエレメント 104 の任意の数 M から構成される。

10

【0048】

M の値は、以下の式の一に従って決定される。

$$M=2+(l-1)/v$$

$$M=1+(L+1)/v$$

【0049】

メモリーエレメント 104 のコンテンツは、イニシャライザ 108、出力シーケンスセクタ 102、及び新規メモリーワードセクタ 114 によって表されるアプリケーションを実行することができる処理部 106 の操作を通じて選択的に作用する。イニシャライザ 108 は、メモリーエレメントを初期状態値のメモリーワードに初期化することができる。出力シーケンスセクタ 102 は、 n タプル出力シーケンスを構成するための、任意のメモリーワードの読出しを行うことができる。新規メモリーワードセクタは、生成器 100 の動作中に任意の 1 以上のメモリーエレメント 104 に書込まれる新規メモリーワードの選択を行うことができる。

20

【0050】

図 10 は、本発明の実施形態の動作中におけるメモリーワードの写像を示すものである。メモリーエレメントがイニシャライザ 108 の動作により初期状態値で 1 度初期化されると、メモリーワードは図の 118 で示される矢印に従って反復的にシフトされる。出力シーケンス生成器 112 の動作を介して、メモリーワードの一つがメモリーエレメントから読出されエンドタプル出力を形成する。そして、メモリーエレメント 104 中の任意部分に格納されたメモリーワード部分の任意のコンビネーションで形成される、新規入力ワードは、新規メモリーワードセクタ 114 の動作を介して利用可能なメモリーエレメント 104 へ挿入される。図に示されるように、メモリーエレメント 104 に格納されているメモリーワードの要素の内容は列方向に写像される。そして、新規入力ワードセクタ 114 の動作を介して、新規メモリーワードが利用可能なメモリーエレメント 104 へ挿入される。メモリーワードの連続的なシフト、任意の n タプルの出力及び新規入力ワードの形成は、擬似乱数シーケンスの生成を可能とする。ウィンドミル生成器 100 のワード志向により、もしより多くの n タプル出力が必要であれば、複数のメモリーエレメント 104 に格納された複数のメモリーワードの出力 n タプルを生成器 100 の動作の反復の間に出力することができる。

30

40

【0051】

図 11 は、図 9、図 10 に示されたメモリーエレメント 104 のスタック 102 を図示する。ここでは、新規メモリーワードセクタが利用可能なメモリーエレメントに挿入される新規メモリーワードの値を形成する手法を示す。メモリーワードが 1 度出力され出力 n タプルが形成されると、矢印 128 と 132 で示されるように、各ヴェインの最後の d エレメントの値が利用される。その後、矢印 134 でしめすように、行成分が巡回的に同一の場所で回転する。その後、矢印 136 で示すように、加算的フィードバックが行われる。そして、矢印 138 で示すように、形成されたワードがコラム方向に上へシフトされる。

50

【0052】

図12は、本発明の別の実施形態のウィンドミル生成器100を示すものである。ここでは、メモリーエレメント104のスタック102が同様に形成され、メモリーエレメントには長さMのメモリーワードが同様に格納されている。そして、同様に、処理部106は、イニシャライザ108、出力シーケンスセクタ112及び新規メモリーワードセクタ114で表されるアプリケーションを実行することができる。ここでは、生成器100のそれぞれの動作の反復の間にメモリーワードの内容をシフトするのではなく、矢印148で表される新規入力ワードポインタが巡回的にスタック102を形成するMワードの間を移動する。即ち、新規入力ワードの位置がメモリーワードの間で巡回的に再識別される。低消費電力が操作における重要な目的であるならば、ポインタ148の再配置で消費する電力は、スタック102全体を各メモリーワードがシフトするよりもより少なくなる。

10

【0053】

図13は、図12に類似するウィンドミル生成器100の実施形態を示すものである。しかし、ここでは唯一の周期的な更新ポインタ148が利用され、セットだけが、データが読出されるか又は格納されるべき、メモリにおけるワードの正確な位置にポイントをオフセットする。

【0054】

本発明の様々な実施形態の動作により、任意のウィンドミル多項式のためのウィンドミル生成器の互換性のある構成が決定される。任意のメモリーワードを連続的な生成器の反復動作の間に単に連続的に読出すことにより擬似乱数シーケンスを簡単に生成するワード志向のウィンドミル生成器が実現される。

20

【0055】

これまでの記載は、発明の実施のための最適な実施形態に関するもので、発明の範囲はこの記載に必ずしも限定されるべきではない。発明の範囲は、請求の範囲に基づき定義されるものである。

【図面の簡単な説明】

【図1】 3タプル出力を生成可能な第一の構成におけるウィンドミル生成器のブロック図を示す。

【図2】 図1に示すウィンドミル生成器の遅延要素における値及び、ウィンドミル生成器の反復生成された3タプルの出力のテーブルリストを示す図である。

30

【図3】 6タプルの出力を生成可能な第二の構成におけるウィンドミル生成器のブロック図を示す。

【図4】 図3に示すウィンドミル生成器の遅延要素における値及び、ウィンドミル生成器の反復生成された6タプルの出力のテーブルリストを示す図である。

【図5】 図1及び図3に示すウィンドミル生成器の構成のための初期状態値及び、両構成が同一の擬似乱数出力シーケンスを生成できるようにするためのその間の写像を示す。

【図6】 二つの手法において決められる出力エンドタップを示す図である。

【図7】 127次までのウィンドミル多項式及び、本発明の実施形態の操作において計算される許容値 v を示すテーブルを表す図である。

【図8】 図7における許容値を決定するためのステップを示す、フローチャートである。

40

【図9】 本発明の実施形態に基づくウィンドミル生成器のブロック図である。

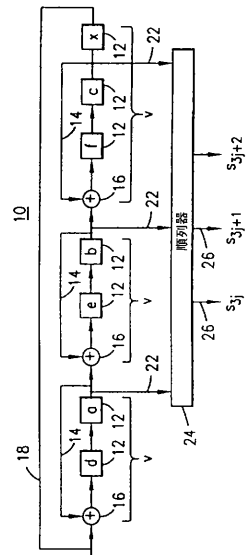
【図10】 図9に示すウィンドミル生成器の操作におけるメモリーワードの写像を示す図である。

【図11】 図9に示すウィンドミル生成器の操作における新規入力ワードの生成手法を示す図である。

【図12】 本発明の別の実施形態に基づくウィンドミル生成器のブロック図である。

【図13】 本発明の別の実施形態に基づくウィンドミル生成器のブロック図である。

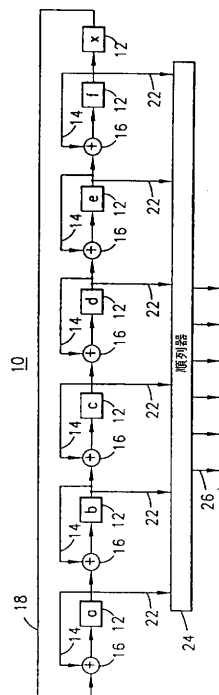
【図 1】



【図 2】

	$g_i \neq 0$	$g_i \neq 1$	$g_i \neq 2$	s_{3j}	s_{3j+1}	s_{3j+2}
$i=0$	1	0	0	0	0	1
$i=1$	0	1	0	1	1	0
$i=2$	0	0	1	0	0	1
$i=3$	0	0	0	1	1	1
$i=4$	1	0	0	0	0	1
$i=5$	1	1	0	1	0	1
$i=6$	0	1	1	1	0	1
$i=7$	1	0	1	0	1	1
$i=8$	1	1	1	1	1	1

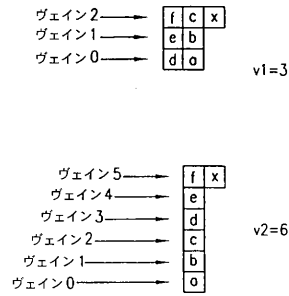
【図 3】



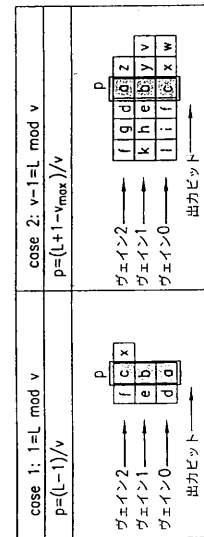
【図 4】

	$L=7$	$v=6$	s_{3j}	s_{3j+1}	s_{3j+2}
$i=0$	0	0	1	1	0
$i=1$	0	0	1	0	0
$i=2$	0	0	1	0	1
$i=3$	1	0	1	0	1

【図 5】



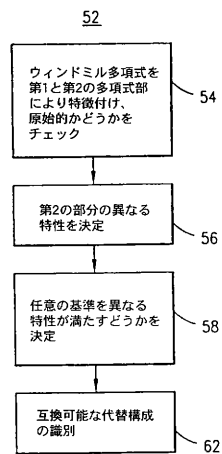
【図 6】



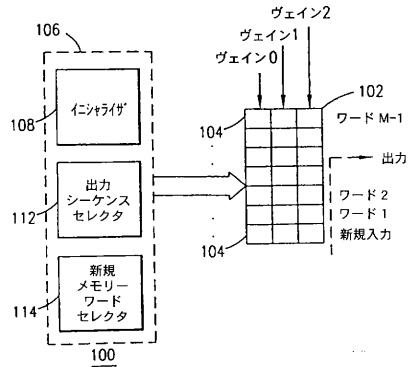
【図 7】

ウィンドミル多項式	許容V値 (3の倍数) +: $1=L \bmod v$, -: $v-1=L \bmod v$
x^7+x^6+1	3+,6+
$x^{17}+x^6+1$	3-,6-
$x^{17}+x^{12}+1$	3-,6-,12
$x^{25}+x^{18}+1$	3-,6-,9,18
$x^{25}+x^{18}+1$	3+,6+,9,18
$x^{31}+x^6+1$	3+,6+
$x^{31}+x^{18}+1$	3+,6+,9,18
$x^{31}+x^{24}+1$	3+,6+,12,24
$x^{47}+x^{42}+1$	3-,6-,21,42
$x^{49}+x^{12}+1$	3+,6+,12+
$x^{55}+x^{24}+1$	3+,6+,12,24
$x^{65}+x^{18}+1$	3-,6-,9,18
$x^{71}+x^6+1$	3-,6-
$x^{71}+x^{18}+1$	3-,6-,9-,18-
$x^{71}+x^{36}+1$	3-,6-,9-,18-,36-
$x^{73}+x^{42}+1$	3+,6+,21,42
$x^{73}+x^{48}+1$	3+,6+,12+,24+,48
$x^{79}+x^{60}+1$	3+,6+,12,15,30,60
$x^{95}+x^{78}+1$	3-,6-,39,78
$x^{95}+x^{84}+1$	3-,6-,21-,42
$x^{97}+x^6+1$	3+,6+
$x^{97}+x^{12}+1$	3+,6+,12+
$x^{103}+x^{30}+1$	3+,6+,15,30
$x^{103}+x^{72}+1$	3+,6+,9,12,18,24,36,72
$x^{103}+x^{90}+1$	3+,6+,9,15,18,30,45,90
$x^{113}+x^{30}+1$	3-,6-,15,30
$x^{121}+x^{18}+1$	3+,6+,9,18
$x^{127}+x^{30}+1$	3+,6+,15,30
$x^{127}+x^{20}+1$	3+,6+,12,15,24,30,60,120
$x^{127}+x^{26}+1$	3+,6+,9+,18+,21+,42+,63+,126+

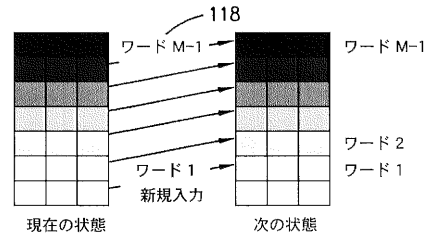
【図 8】



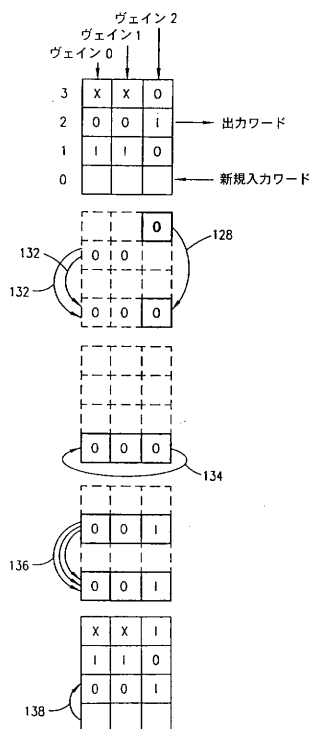
【図 9】



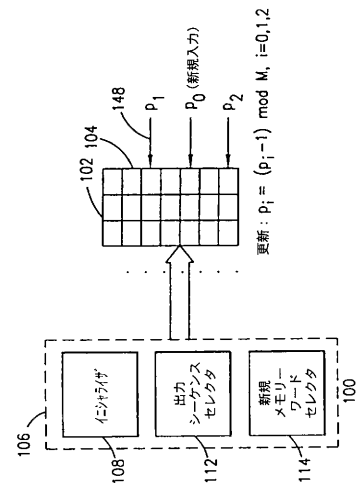
【図 10】



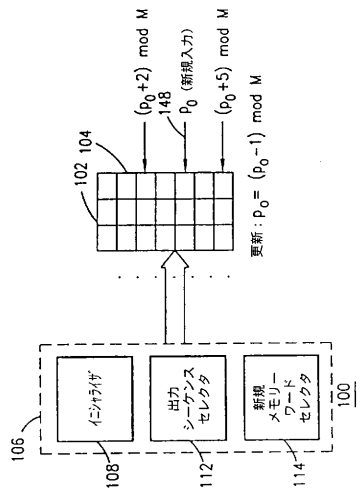
【図 11】



【図 12】



【図 13】



フロントページの続き

(74)代理人 100101306

弁理士 丸山 幸雄

(72)発明者 スミーツ, ベルナルド, ヤン, マリー

スウェーデン国 ダルビュー エス-240 10, ダルバックヴェーゲン 11

審査官 新田 亮

(56)参考文献 特開平02-043594 (JP, A)

B.J.M.Smeets et.al., Windmill pn-sequence generators, IEEE Proc. E.Computers & Digital Techniques, 1989年 9月, Vol.136, p.401-404, URL, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=31392