(19)日本国特許庁(JP)

# 再 公 表 特 許(A1)

(11)国際公開番号
WO2017/150672

発行日　平成30年12月27日(2018.12.27)

(43)国際公開日　平成29年9月8日(2017.9.8)

| (51)Int.Cl. | | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|---|
| G06F | 7/58 | (2006.01) | G06F | 7/58 | 620 | 5J104 |
| G09C | 1/00 | (2006.01) | G09C | 1/00 | 650B | |

審査請求 未請求　予備審査請求 未請求　（全 19 頁）

| | |
|---|---|
| 出願番号 | 特願2018-503400 (P2018-503400) |
| (21)国際出願番号 | PCT/JP2017/008294 |
| (22)国際出願日 | 平成29年3月2日(2017.3.2) |
| (31)優先権主張番号 | 特願2016-41564 (P2016-41564) |
| (32)優先日 | 平成28年3月3日(2016.3.3) |
| (33)優先権主張国 | 日本国(JP) |

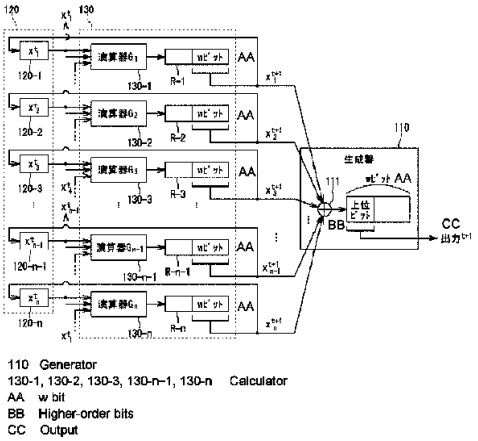
(71)出願人　504132272
国立大学法人京都大学
京都府京都市左京区吉田本町３６番地１
(74)代理人　110000280
特許業務法人サンクレスト国際特許事務所
(72)発明者　岩▲崎▼　淳
京都府京都市左京区吉田本町３６番地１
国立大学法人京都大学内
(72)発明者　梅野　健
京都府京都市左京区吉田本町３６番地１
国立大学法人京都大学内

Ｆターム(参考)　5J104 FA04

最終頁に続く

(54)【発明の名称】乱数発生装置、乱数発生方法及びコンピュータプログラム

(57)【要約】
乱数発生装置１００は、複数の変数を記憶する記憶部１２０と、複数の変数それぞれを更新する複数の更新式の演算を実行し、複数の変数の更新値を記憶部１２０へ出力する演算部１３０と、複数の変数の少なくともいずれか一つの変数に基づいて、乱数を生成する生成器１１０と、を備える。更新式は、更新式によって更新される対象変数の置換多項式と、複数の変数に含まれる対象変数以外の他の変数と、を含み、更新式によって対象変数を繰り返し更新したときの周期性が、一筆書き周期性である。



【特許請求の範囲】
【請求項１】
複数の変数を記憶する記憶部と、
複数の前記変数それぞれを更新する複数の更新式の演算を実行し、複数の前記変数の更新値を前記記憶部へ出力する演算部と、
複数の前記変数の少なくともいずれか一つの変数に基づいて、乱数を生成する生成器と、
を備え、
前記更新式は、
前記更新式によって更新される対象変数の置換多項式と、複数の前記変数に含まれる前記対象変数以外の他の変数と、を含み、
前記更新式によって前記対象変数を繰り返し更新したときの周期性が、一筆書き周期性である
乱数発生装置。
【請求項２】
前記更新式は、前記対象変数の前記置換多項式と、前記他の変数と、の和を含む
請求項１記載の乱数発生装置。
【請求項３】
前記対象変数の前記置換多項式は、前記対象変数に乗じられる係数部分であって、多項式で表される前記係数部分を含み、前記他の変数は、前記係数部分に含まれる
請求項１又は２に記載の乱数発生装置。
【請求項４】
前記置換多項式は、一筆書き多項式である
請求項１～３のいずれか１項に記載の乱数発生装置。
【請求項５】
演算部が、記憶部に記憶された複数の変数それぞれを更新する複数の更新式の演算を実行すること、
前記演算部が、複数の前記変数の更新値を記憶部へ出力すること、
生成器が、複数の前記変数の少なくともいずれか一つの変数に基づいて、乱数を生成すること、
を含み、
前記更新式は、
前記更新式によって更新される対象変数の置換多項式と、複数の前記変数に含まれる前記対象変数以外の他の変数と、を含み、
前記更新式によって前記対象変数を繰り返し更新したときの周期性が、一筆書き周期性である
乱数発生方法。
【請求項６】
コンピュータを、
複数の変数を記憶する記憶部、
複数の前記変数それぞれを更新する複数の更新式の演算を実行し、複数の前記変数の更新値を前記記憶部へ出力する演算部、及び
複数の前記変数の少なくともいずれか一つの変数に基づいて、乱数を生成する生成器
として機能させるためのコンピュータプログラムであって、
前記更新式は、
前記更新式によって更新される対象変数の置換多項式と、複数の前記変数に含まれる前記対象変数以外の他の変数と、を含み、
前記更新式によって前記対象変数を繰り返し更新したときの周期性が、一筆書き周期性である
コンピュータプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、乱数発生装置等に関するものである。
【背景技術】
【０００２】
特許文献１は、置換多項式を用いた乱数発生装置を開示している。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特許第３８０６７６２号公報
【発明の概要】
【０００４】
一般に、乱数には、高い乱数性が望まれる。置換多項式の値を用いて生成される乱数の乱数性を高くするための一つのアプローチは、置換多項式の次数を大きくすることである。しかし、置換多項式の次数が大きくなると、演算器による演算時間の増大を招き易い。
【０００５】
このため、次数を大きくするのとは別のアプローチで、高い乱数性を容易に得ることが望まれる。
【０００６】
一の観点からみた本発明は、乱数発生装置である。乱数発生装置は、複数の変数それぞれを更新する複数の更新式の演算を実行する。更新式は、更新式によって更新される対象変数の置換多項式と、複数の変数に含まれる対象変数以外の他の変数と、を含む。更新式は、更対象変数を繰り返し更新したときの周期性が、一筆書き周期性である。本発明によれば、一筆書き多項式と同様の長周期が得られ、高い乱数性が容易に得られる。
【０００７】
他の観点からみた本発明は、乱数を生成する方法である。他の観点からみた本発明は、コンピュータを乱数発生装置として機能させるためのコンピュータプログラムである。コンピュータプログラムは、コンピュータ読み取り可能な記録媒体に記憶される。
【図面の簡単な説明】
【０００８】
【図１】置換多項式の軌道を示す図である。
【図２】一筆書き多項式の軌道を示す図である。
【図３】乱数発生装置のブロック図である。
【発明を実施するための形態】
【０００９】
［１．用語］
【００１０】
［１．１　置換多項式］
置換多項式Ｆ（Ｘ）は、有限集合上でＸの置換を与える多項式である。置換多項式は、有限集合において全単射を与える。置換多項式による変数Ｘの値の変化を示す軌道は、必ず、周期軌道になる。すなわち、置換多項式による変数Ｘの値の変化は、周期性を持つ。
【００１１】
［１．２　２冪剰余環］
２冪剰余環は、以下のように表される有限集合である。本明細書では、以下のように表される２冪剰余環を、「冪指数ｗの２冪剰余環」というものとする。ｗは、任意の非負整数である。

【数１】

$$\mathbb{Z}/2^{w}\mathbb{Z}=\{0,\ 1,\ 2,\ \cdots,\ 2^{w}-1\}$$

なお、計算途中で値が集合の範囲外に出たら、”ｍｏｄ　２$^{w}$”をとる。ｍｏｄは、剰余演算子である。

【００１２】

［１．３　２冪剰余環上置換多項式］

２冪剰余環上置換多項式は、２冪剰余環上で置換を与える置換多項式である。２冪剰余環上置換多項式は、整数係数多項式である。すなわち、２冪剰余環上置換多項式Ｆ（Ｘ）は、Ｆ（Ｘ）　ｍｏｄ　２$^{w}$が、冪指数ｗの２冪剰余環上で全単射を与える整数係数多項式であり、以下のようにも定義される。

【数２】

$$F(X)=a_nX^{n}+a_{n-1}X^{n-1}+\cdots+a_0$$

$$\{F(\bar{X})\mod 2^{w}|\bar{X}\in\mathbb{Z}/2^{w}\mathbb{Z}\}=\mathbb{Z}/2^{w}\mathbb{Z}$$

【００１３】

例えば、冪指数３の２冪剰余環上における、置換多項式Ｆ$_{a}$（Ｘ）＝２Ｘ$^{2}$＋Ｘ＋１の軌道は、図１（ａ）に示すように、周期軌道になる。すなわち、Ｆ$_{a}$（０）　ｍｏｄ　２$^{3}$＝１であり、Ｆ$_{a}$（１）　ｍｏｄ　２$^{3}$＝４であり、Ｆ$_{a}$（４）　ｍｏｄ　２$^{3}$＝５であり、Ｆ$_{a}$（５）　ｍｏｄ　２$^{3}$＝０である。

【００１４】

また、置換多項式Ｆ$_{a}$（Ｘ）＝２Ｘ$^{2}$＋Ｘ＋１は、図１（ｂ）に示す別の周期軌道も持つ。すなわち、Ｆ$_{a}$（２）　ｍｏｄ　２$^{3}$＝３であり、Ｆ$_{a}$（３）　ｍｏｄ　２$^{3}$＝６であり、Ｆ$_{a}$（６）　ｍｏｄ　２$^{3}$＝７であり、Ｆ$_{a}$（７）　ｍｏｄ　２$^{3}$＝２である。

【００１５】

［１．４　一筆書き周期性と一筆書き多項式］

一筆書き周期性とは、多項式Ｆ（Ｘ）が成す１本の軌道（１周期の軌道）が、２冪剰余環のすべての要素をめぐることをいう。軌道が一筆書き周期性を持つ多項式を、一筆書き多項式という。一筆書き多項式は、以下のように定義される。

【数３】

$$\forall w\in\mathbb{N}\cup\{0\},\forall\bar{X}\in\mathbb{Z}/2^{w}\mathbb{Z},\ \{F^{i}(\bar{X})\mod 2^{w}|i\in\mathbb{Z}/2^{w}\mathbb{Z}\}=\mathbb{Z}/2^{w}\mathbb{Z}$$

【００１６】

図２は、冪指数３の２冪剰余環＝｛０，１，２，３，４，５，６，７｝上における、一筆書き多項式Ｆ$_{b}$（Ｘ）＝４Ｘ$^{2}$＋Ｘ＋１の軌道を示している。図２に示す軌道は、周期軌道であり、１周期の軌道が、｛０，１，２，３，４，５，６，７｝のすべての要素を１回ずつ通過している。したがって、Ｆ$_{b}$（Ｘ）による２冪剰余環上の軌道は、一筆書き周期性を持ち、Ｆ$_{b}$（Ｘ）は一筆書き多項式である。図１と図２との対比からも明らかなように、一筆書き周期性がある場合、軌道の周期は最大となり、周期長は２$^{w}$となる。長い周期は、乱数発生において有利である。

【００１７】

置換多項式Ｆ（Ｘ）が、一筆書き多項式である必要十分条件は、

【数４】

$$a_0 \equiv 1 \mod 2,$$
$$a_1 \equiv 1 \mod 2,$$
$$(a_1 + a_2 + a_3 + \cdots) \equiv 1 \mod 4,$$
$$(a_3 + a_5 + a_7 + \cdots) \equiv 2a_2 \mod 4$$

がすべて成り立つことである。上記の必要十分条件は、

係数ａ$_0$と１とは法２に関して合同であり、

係数ａ$_1$と１とは法２に関して合同であり、

添え字が１以上であるすべての係数ａ$_1$，ａ$_2$，ａ$_3$，・・・の和と１とは、法４に関して合同であり、

添え字が３以上の奇数であるすべての係数ａ$_3$，ａ$_5$，ａ$_7$，・・・の和と２ａ$_2$とは、法４に関して合同であることを示す。

【００１８】

一筆書き多項式は、長周期であるという観点では乱数の生成に有利であるが、時間発展（変数Ｘの時間的変化）が単純となり、十分な乱数性を得るのが困難な場合がある。したがって、単なる一筆書き多項式単体は、乱数の生成に不利な面も有する。

【００１９】

［２．実施形態の概要］

【００２０】

［第１項］

実施形態に係る乱数発生装置は、

複数の変数を記憶する記憶部と、

複数の前記変数それぞれを更新する複数の更新式の演算を実行し、複数の前記変数の更新値を前記記憶部へ出力する演算部と、

複数の前記変数の少なくともいずれか一つの変数に基づいて、乱数を生成する生成器と、

を備える。

前記更新式は、

前記更新式によって更新される対象変数の置換多項式と、複数の前記変数に含まれる前記対象変数以外の他の変数と、を含み、

前記更新式によって前記対象変数を繰り返し更新したときの周期性が、一筆書き周期性である。

【００２１】

第１項の乱数発生装置によれば、乱数の生成に用いられる変数を更新する更新式は、更新式によって更新される対象変数以外の他の変数も含むので、対象変数の置換多項式の次数を大きくしなくても、乱数性を高くすることができる。しかも、更新式は一筆書き周期性を持つので、長い周期を得ることができる。

【００２２】

［第２項］

前記更新式は、前記対象変数の前記置換多項式と、前記他の変数と、の和を含むことができる。

【００２３】

［第３項］

前記対象変数の前記置換多項式は、前記対象変数に乗じられる係数部分であって、多項式で表される前記係数部分を含み、前記他の変数は、前記係数部分に含まれていてもよい。

【００２４】
［第４項］
前記置換多項式は、一筆書き多項式であるのが好ましい。
【００２５】
［第５項］
実施形態に係る方法は、
演算部が、記憶部に記憶された複数の変数それぞれを更新する複数の更新式の演算を実行すること、
前記演算部が、複数の前記変数の更新値を記憶部へ出力すること、
生成器が、複数の前記変数の少なくともいずれか一つの変数に基づいて、乱数を生成すること、
を含む。
前記更新式は、
前記更新式によって更新される対象変数の置換多項式と、複数の前記変数に含まれる前記対象変数以外の他の変数と、を含み、
前記更新式によって前記対象変数を繰り返し更新したときの周期性が、一筆書き周期性である。
【００２６】
［第６項］
実施形態に係るコンピュータプログラムは、
コンピュータを、
複数の変数を記憶する記憶部、
複数の前記変数それぞれを更新する複数の更新式の演算を実行し、複数の前記変数の更新値を前記記憶部へ出力する演算部、及び
複数の前記変数の少なくともいずれか一つの変数に基づいて、乱数を生成する生成器
として機能させるためのコンピュータプログラムである。
前記更新式は、
前記更新式によって更新される対象変数の置換多項式と、複数の前記変数に含まれる前記対象変数以外の他の変数と、を含み、
前記更新式によって前記対象変数を繰り返し更新したときの周期性が、一筆書き周期性である。
【００２７】
［３．実施形態の詳細］
【００２８】
［３．１　乱数発生装置の構成］
図３は、実施形態に係る乱数発生装置１００を示している。乱数発生装置１００は、例えば、乱数を発生させるための演算を実行する演算回路を備えたハードウェアによって構成されている。乱数発生装置１００は、乱数発生コンピュータプログラムがインストールされたコンピュータであってもよい。コンピュータは、乱数発生コンピュータプログラムを実行することによって、乱数発生装置１００として機能する。
【００２９】
乱数発生装置１００は、乱数を生成する生成器１１０を備えている。生成器１１０は、変数ｘから乱数を生成する。実施形態に係る生成器１１０は、ｎ個（ｎは２以上の整数）の変数$x_1$，・・・，$x_n$に基づいて、乱数を生成する。ここで、変数$x_1$，・・・，$x_n$は、それぞれ、ｗビットの符号なし変数である。ｗは、任意の非負整数であり、例えば６４である。以下では、変数ｘの時間発展を表す$x^t$の表記を用いることもある。$x^t$は、時刻ｔにおける変数ｘの値を示す。
【００３０】
乱数発生装置１００は、ｎ個の変数を記憶する記憶部１２０と、ｎ個の変数を更新する演算を実行する演算部１３０と、を備える。記憶部１２０は、ｎ個の変数を記憶するため

のｎ個の記憶領域１２０－１，・・・，１２０－ｎを有する。各記憶領域１２０－１，・・・，１２０－ｎの大きさは、ｗビットである。

【００３１】

演算部１３０は、ｎ個の記憶領域１２０－１，・・・，１２０－ｎに対応する、ｎ個の演算器１３０－１，・・・，１３０－ｎを有している。各演算器１３０－１，・・・，１３０－ｎは、対応する記憶領域１２０－１，・・・，１２０－ｎに記憶された変数$x_1$，・・・，$x_n$を更新するため更新式本体$G_1$，・・・，$G_n$の演算を実行する。更新式本体$G_1$，・・・，$G_n$は、後述する更新式から”ｍｏｄ　$2^w$”を除いた部分をいう。

【００３２】

各演算器１３０－１，・・・，１３０－ｎが演算の対象とする変数ｘを、対象変数とよぶ。例えば、演算器１３０－１にとっての対象変数は、変数$x_1$であり、演算器１３０－ｎにとっての対象変数は、変数$x_n$である。

【００３３】

各演算器１３０－１，・・・，１３０－ｎは、対象変数の更新のため、記憶部１２０から対象変数を取得する。例えば、演算器１３０－１は、記憶領域１２０－１から変数$x_1$を対象変数として取得し、演算器１３０－ｎは、記憶領域１２０－ｎから変数$x_n$を対象変数として取得する。

【００３４】

各演算器１３０－１，・・・，１３０－ｎは、対象変数だけでなく、記憶部１２０から他の変数も取得する。他の変数は、複数の変数$x_1$，・・・，$x_n$に含まれる変数であって、対象変数以外の変数である。他の変数は、１つであってもよいし、複数であってもよい。各演算器１３０は、複数の変数$x_1$，・・・，$x_n$すべてを取得してもよい。例えば、演算器１３０－１は、記憶領域１２０－２から変数$x_2$などを他の変数として取得し、演算器１３０－ｎは、記憶領域１２０－１から変数$x_1$などを他の変数として取得する。

【００３５】

各演算器１３０－１，・・・，１３０－ｎが取得した他の変数は、対象変数とともに、対象変数の更新に用いられる。すなわち、更新式は、対象変数と他の変数とを含む式である。更新式の例については後述する。

【００３６】

各演算器１３０－１，・・・，１３０－ｎは、更新式本体$G_1$，・・・，$G_n$の演算結果Ｒ－１，・・・，Ｒ－ｎを出力する。演算結果Ｒ－１，・・・，Ｒ－ｎのビット数は、ｗビットを超えることがある。各演算結果Ｒ－１，・・・，Ｒ－ｎの下位ｗビットが、変数$x_1^t$，・・・，$x_n^t$の更新値$x_1^{t+1}$，・・・，$x_n^{t+1}$となる。各演算結果Ｒ－１，・・・，Ｒ－ｎから、それらの下位ｗビットを取り出すことは、数学的には、各演算結果Ｒ－１，・・・，Ｒ－ｎに対して、”ｍｏｄ　$2^w$”の演算を行うことと等価である。本実施形態では、剰余演算を行う必要がないため、演算を高速化できる。

【００３７】

更新値$x_1^{t+1}$，・・・，$x_n^{t+1}$は、演算部１３０から記憶部１２０へ出力される。更新値$x_1^{t+1}$，・・・，$x_n^{t+1}$は、記憶領域１２０－１，・・・，１２０－ｎに上書きされる。

【００３８】

本実施形態では、生成器１１０は、時刻ｔ＋１において演算部１３０から出力された１又は複数の変数$x^{t+1}$から、乱数発生に用いられる出力系列$^{t+1}$を生成し、その出力系列$^{t+1}$から時刻ｔ＋１における乱数$^{t+1}$を生成する。生成器１１０の構成は、１又は複数の変数ｘから乱数を生成する所定の演算を行うものであれば、特に限定されない。生成器１１０が変数から乱数を生成する演算は、複数の変数ｘ全部又は一部を如何様に組み合わせた演算であってもよいし、複数の変数ｘのうちの１つの変数だけを用いた演算であってもよい。なお、生成器１１０は、変数ｘの更新値が記憶部１２０に上書きされてから、変数ｘを記憶部１２０から読み出して乱数を生成してもよい。

【００３９】

実施形態に係る生成器１１０は、排他的論理和演算部１１１を備える。排他的論理和演算部１１１は、ｎ個の変数$x_1$，・・・，$x_n$の排他的論理演算を行う。排他的論理和演算部１１１の出力の所定上位ビット（例えば、上位１６ビット）が、出力系列$^{t+1}$となる。生成器１１０は、出力系列$^{t+1}$を用いて乱数$^{t+1}$を生成し、生成された乱数数$^{t+1}$を出力する。なお、排他的論理和演算部１１１は、Ｎ個の変数$x_1$，・・・，$x_n$それぞれの上位ビットに対する排他的論理和演算を行っても良い。また、生成器１１０は、出力系列を乱数として出力してもよい。

【００４０】

［３．２　更新式の第１例］

ｎ個の変数$x_1$，・・・，$x_n$それぞれ更新するｎ個の更新式の第１例は、以下のとおりである。

【数５】

$$
\begin{aligned}
x_1^{(i+1)} &= F_1(x_1^{(i)}) + c_{1,1}x_1^{(i)} + c_{1,2}x_2^{(i)} + c_{1,3}x_3^{(i)} + \cdots + c_{1,n}x_n^{(i)} \mod 2^w \\
x_2^{(i+1)} &= F_2(x_2^{(i)}) + c_{2,1}x_1^{(i)} + c_{2,2}x_2^{(i)} + c_{2,3}x_3^{(i)} + \cdots + c_{2,n}x_n^{(i)} \mod 2^w \\
x_3^{(i+1)} &= F_3(x_3^{(i)}) + c_{3,1}x_1^{(i)} + c_{3,2}x_2^{(i)} + c_{3,3}x3^{(i)} + \cdots + c_{3,n}x_n^{(i)} \mod 2^w \\
&\vdots \\
x_n^{(i+1)} &= F_n(x_n^{(i)}) + c_{n,1}x_1^{(i)} + c_{n,2}x_2^{(i)} + c_{n,3}x_3^{(i)} + \cdots + c_{n,n}x_n^{(i)} \mod 2^w
\end{aligned}
$$

ここで,

- $F_1(X),\ F_2(X),\ \cdots,\ F_n(X)$：一筆書き多項式
- $x_1,\ x_2,\cdots,\ x_n$：$w$ビットの符号なし変数

また，任意の変数$a$に対して，$a^{(i)}$で時刻$i$での変数$a$の値を表すものとする

【００４１】

各更新式の右辺は、”ｍｏｄ　２$^{w}$”の部分と、”ｍｏｄ　２$^{w}$”以外の部分である更新式本体と、を有する。例えば、変数$x_1$の更新式の更新式本体$G_1$は、変数$x_1$の更新式のうち、”ｍｏｄ　２$^{w}$”以外の部分である”$F_1(x_1^{(i)})+c_{1,1}x_1^{(i)}+c_{1,2}x_2^{(i)}+c_{1,3}x_3^{(i)}+\cdots+c_{1,n}x_n^{(i)}$”の部分である。他の変数$x_2$，・・・，$x_n$についても同様である。

【００４２】

更新式本体は、対応する演算器によって演算される。例えば、更新式本体$G_1$は、演算器１３０－１によって演算される。更新式本体$G_1$は、対象変数$x_1$の置換多項式としての一筆書き多項式$F_1(x_1^{(i)})$、と、付加多項式$c_{1,1}x_1^{(i)}+c_{1,2}x_2^{(i)}+c_{1,3}x_3^{(i)}+\cdots+c_{1,n}x_n^{(i)}$と、の和として表される。付加多項式は、少なくとも一つの他の変数（対象変数$x_1$以外の変数）$x_2$，・・・$x_n$を含む。付加多項式は、対象変数$x_1$を含んでも良い。第１例において、付加多項式は、付加多項式に含まれる複数の変数ｘに関して、$c_{k,1}$を係数とした線形結合となっている。なお、本明細書において、多項式は、単項式を含む。以上の更新式本体$G_1$についての説明は、他の変数$x_2$，・・・，$x_n$についての更新式本体$G_2$，・・・，$G_n$においても同様である。

【００４３】

更新式の第１例では、各一筆書き多項式に付加多項式が付加されているが、各更新式全

体における一筆書き周期性が維持されている。

【００４４】

更新式の第１例において、一筆書き周期性を持つための条件は、以下のとおりである。

・係数$c_{k,l}$（$k=1,2,\cdots,n$，$l=1,2,\cdots,n$）はすべて偶数（偶数は０を含む、以下同様）である。

・任意のｋに対して、$c_{k,1}$，$c_{k,2}$，・・・，$c_{k,n}$のうち、４で割り切れないものの個数は偶数である。

【００４５】

なお、付加多項式中の”＋”、及び、付加多項式と置換多項式（一筆書き多項式）との和をとるための”＋”は、算術和演算である必要はなく、排他的論理和演算であってもよい。また、複数の”＋”に対応する演算として、算術和演算と排他的論理和演算とが混在してもよい。算術和演算と排他的論理和演算とが混在する場合には、両演算の優先順位を適宜決めればよい。

【００４６】

更新式の第１例は、以下の点で有用である。まず、各更新式は一筆書き周期性を持つため、各変数の周期は、$2^w$という長周期になることが保証される。すなわち、以下が成り立つ。

【数６】

$$\forall m,\ x_m^{(a)} \neq x_m^{(0)}\ (0 < a < 2^w),\ x_m^{(2^w)} = x_m^{(0)}.$$

なお、長周期性は、疑似乱数発生器やストリーム暗号において重要な性質である。

【００４７】

更新式の第１例の時間発展は、単なる一筆書き多項式単体の時間発展より複雑な挙動となるため有利である。更新式の第１例では、各更新式の次数は２に抑えられているが、次数を高くしなくても、時間発展の複雑な挙動が得られる。次数の増加は、演算負荷が大きい乗算の増加を招くが、更新式の第１例では、各更新式の次数を低く抑えられて有利である。

【００４８】

また、更新式の第１例は、一筆多項式に付加多項式が付加されているが、一筆書き多項式と同様に、実質的に除算を行う必要がない。つまり、剰余算はデジタルコンピュータ上では無視できるという一筆書き多項式の優れた点が維持されている。

【００４９】

ｎ個の更新式を並列に演算することで、すなわち、各演算器１３０－１，・・・，１３０－ｎが並列に演算することで、変数の数が増加しても演算時間の増加を抑えることができる。

【００５０】

係数$c_{k,l}$の値として、２の冪乗のものを選択すると、更新式中では乗算として表現されている$c_{k,l}x_{k,l}$を、変数$x_{k,l}$のビットシフト操作で実現できるため、より高速化が可能である。また、係数$c_{k,l}$の値としては、上記の条件を満たす限り、様々な値を採用できる。したがって、乱数発生装置としての設計の自由度が高くなる。

【００５１】

［３．３　更新式の第１例の評価］

更新式の第１例の乱数性を評価するため、以下のｎ個の更新式を用いた。

【数７】

更新式本体

$$
\begin{aligned}
x_1^{(i+1)} &= [2\{x_1^{(i)}\}^2 + a_1 x_1^{(i)} + b_1] + 4x_2^{(i)} \mod 2^{64} \\
x_2^{(i+1)} &= [2\{x_2^{(i)}\}^2 + a_2 x_2^{(i)} + b_2] + 4x_3^{(i)} \mod 2^{64} \\
x_3^{(i+1)} &= [2\{x_3^{(i)}\}^2 + a_3 x_3^{(i)} + b_3] + 4x_4^{(i)} \mod 2^{64} \\
x_4^{(i+1)} &= [2\{x_4^{(i)}\}^2 + a_4 x_4^{(i)} + b_4] + 4x_5^{(i)} \mod 2^{64} \\
x_5^{(i+1)} &= [2\{x_5^{(i)}\}^2 + a_5 x_5^{(i)} + b_5] + 4x_6^{(i)} \mod 2^{64} \\
x_6^{(i+1)} &= [2\{x_6^{(i)}\}^2 + a_6 x_6^{(i)} + b_6] + 4x_1^{(i)} \mod 2^{64}
\end{aligned}
$$

一筆書き多項式　　付加多項式

ただし，$x_1, x_2, x_3, x_4, x_5, x_6, a_1, a_2, a_3, a_4, a_5, a_6, b_1, b_2, b_3, b_4, b_5, b_6$ は64bit符号なし整数で，

$$a_1, a_2, \cdots, a_6 \equiv 3 \mod 4, \quad b_1, b_2, \cdots, b_6 \equiv 1 \mod 2$$

を満たす．

【００５２】

評価は、図１の乱数発生装置における演算部１３０が上記のｎ個の更新式を演算するようにコンピュータを機能させるプログラムを、コンピュータに実行させて行った。乱数発生装置として機能させたコンピュータのプロセッサは、１．３ＧＨｚ　Ｉｎｔｅｌ　Ｃｏｒｅ　ｉ５である。なお、評価は、ｎ個の更新式の演算を並列化せずに行った。

【００５３】

評価において、生成部１１０は、演算部１３０が出力した変数$x_1$，$x_2$，$x_3$，$x_4$，$x_5$，$x_6$の排他的論理和をとり、その結果を、４８ビット右シフトさせた１６ビットの値（出力系列）を評価系列として生成する。すなわち、生成部１１０は、以下の演算を行う。

【数８】

$$(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6) >> 48$$

【００５４】

乱数性の評価は、以下を１セットとして４０セット行った。

１．$x_1$，$x_2$，$x_3$，$x_4$，$x_5$，$x_6$，$a_1$，$a_2$，$a_3$，$a_4$，$a_5$，$a_6$，$b_1$，$b_2$，$b_3$，$b_4$，$b_5$，$b_6$の値をランダムに決める。

２．「１．」で決めた値をセットした乱数発生装置を実行させ、生成された評価系列から$10^9$ビットの乱数を生成する。

３．得られた乱数$10^9$ビットの乱数を、$10^6$ビットの乱数１０００本とする。１０００本の乱数を、米国商務省標準技術局（ＮＩＳＴ）　ＳＰ　８００－２２で定義される乱数検定にかける。

【００５５】

表１は、乱数検定結果を示している。

【表１】

| 合格したテスト項目数 | セット数 |
|---|---|
| 188 | 26 |
| 187 | 12 |
| 186 | 1 |
| 185 | 0 |
| 184 | 1 |

【００５６】

ＮＩＳＴ　ＳＰ　８００－２２は、１８８項目のテストで構成されている。１８８項目すべてについて合格したのは、４０セット中２６セットであった。理想的な乱数の場合に、１８８項目すべてをクリアするセット数の理論値は、標準偏差の範囲で、４０セット中２１セットから２７セットである。また、すべての項目に合格しなかった１４セットについても、理想的な乱数が十分にとり得る成績である。よって、乱数性に関し良好な結果が得られていることがわかる。

【００５７】

また、評価では、３Ｇｂｐｓ以上の実行速度が得られており、実行速度の観点からも良好な結果が得られた。

【００５８】

［３．４　更新式の第２例］

Ｎ個の変数$x_1$，・・・，$x_N$それぞれ更新するＮ個の更新式の第２例は、以下のとおりである。

【数９】

$$x_1^{(t+1)} = \sum_j \left[ a_{1,j} + \sum_{k,l} C_{1,j,k,l} \left\{ x_k^{(t)} \right\}^l \right] \left\{ x_1^{(t)} \right\}^j mod 2^w,$$

$$x_2^{(t+1)} = \sum_j \left[ a_{2,j} + \sum_{k,l} C_{2,j,k,l} \left\{ x_k^{(t)} \right\}^l \right] \left\{ x_2^{(t)} \right\}^j mod 2^w,$$

$$\vdots$$

$$x_N^{(t+1)} = \sum_j \left[ a_{N,j} + \sum_{k,l} C_{N,j,k,l} \left\{ x_k^{(t)} \right\}^l \right] \left\{ x_N^{(t)} \right\}^j mod 2^w,$$

ここで

・ $j$は０以上の整数を, $k,l$ は１以上の整数を動く.ただし,有限の範囲.

・各$i$について$F_i(X) = \sum_j a_{i,j} X^j$ :一筆書き多項式

・ $x_1, x_2, \cdots, x_N$: $w$ ビットの符号なし整数型変数

・ $j = 0$の場合を除く、任意の$(i,j,k,l)$について$C_{i,j,k,l}$は４で割り切れる.

・任意の$(i,k,l)$について,$C_{i,0,k,l}$ は２で割り切れる.

・任意の $i$ について,$\sum_{k,l} C_{i,0,k,l}$は４で割り切れる.(言い換えると, $i$を固定したとき $\{C_{i,0,k,l}\}$ のうち４で割り切れないものの個数は偶数)

・任意の変数$b$に対して, $b^{(t)}$で時刻 $t$での変数 $b$ の値を表すものとする

・任意の $i$ について, $\sum_{k=1}^{K} \sum_{l} C_{i,0,k,l} \equiv 0 \, mod \, 4$ （$l$は３以上の奇数）

【００５９】

なお、第２例中の”＋”も、算術和演算である必要はなく、排他的論理和演算であってもよい。また、複数の”＋”に対応する演算として、算術和演算と排他的論理和演算とが混在してもよい。算術和演算と排他的論理和演算とが混在する場合には、両演算の優先順位を適宜決めればよい。

【００６０】

更新式の第２例は、第１例を包含する形式で定義されている。つまり、全係数$c_{i,j,k,l}$のうち、添え字ｊが０かつ添え字ｌが１（他の添え字ｉ，ｋは、０でもよいし０でなくてよい）である係数$c_{i,0,k,1}$以外のものすべてを０にすると、

【数１０】

$$x_i^{(t+1)} = F_i\left(x_i^{(t)}\right) + \sum_k C_{i,0,k,1} \, x_k^{(t)}$$

となり、第１例に対応する。

【００６１】

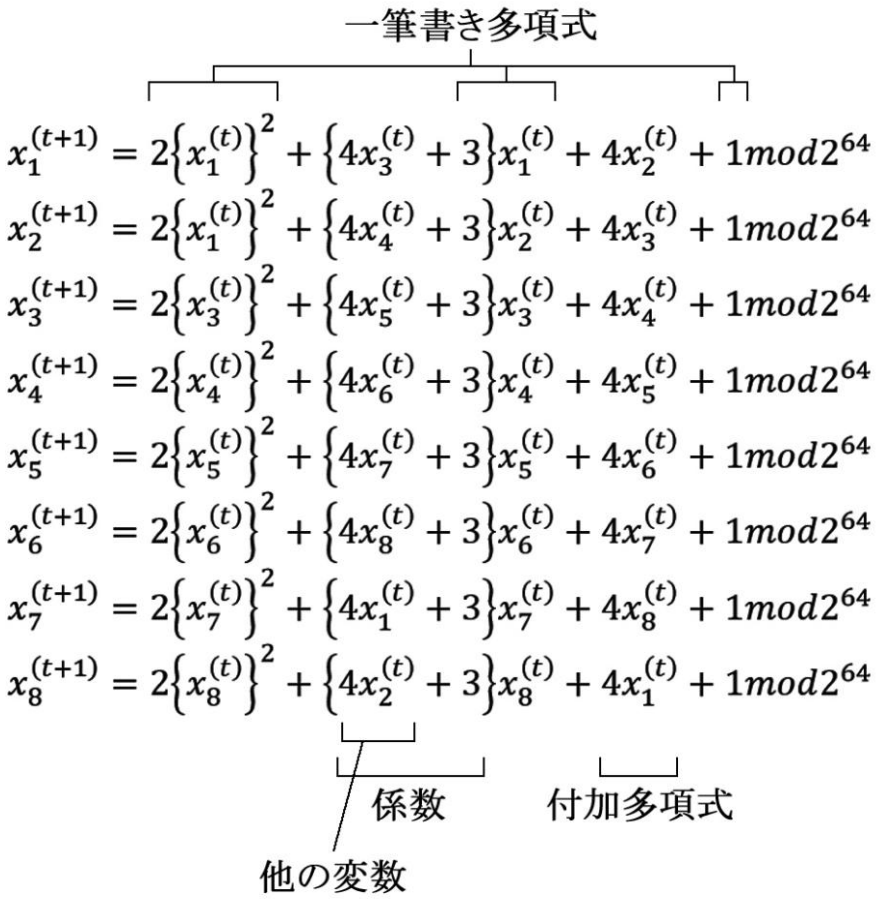
第２例においても、各変数$x_1$，・・・，$x_N$の更新式は、一筆書き周期性を有する。第２例においても、各更新式の右辺は、”ｍｏｄ　$2^w$”の部分と、”ｍｏｄ　$2^w$”以外の部分である更新式本体と、を有する。第２例でも、更新式本体は、対象変数の置換多項式（一筆書き多項式）と、付加多項式としての和として表されるが、第２例では、付加多項式が含まれていなくても良い。第２例では、置換多項式の係数部分（対象変数に乗じ

られる部分）が、対象変数以外の他の変数を含む多項式で表される。

【００６２】

以下は、第２例の具体例を示している。

【数１１】




【００６３】

例えば、変数$x_1$の更新式は、”ｍｏｄ２$^{64}$”以外の更新式本体$G_1$を有している。更新式本体$G_1$において、対象変数$x_1$のための一筆書き多項式に相当するのは、”２｛$x_1^{(t)}$｝$^2$＋｛４$x_3^{(t)}$＋３｝$x_1^{(t)}$＋１”の部分であり、付加多項式に相当するのが、”４$x_2^{(t)}$”の部分である。更新式本体$G_1$の付加多項式は、他の変数として$x_2^{(t)}$を有する。

【００６４】

更新式本体$G_1$の一筆書き多項式においては、$x_1^{(t)}$の係数が、定数ではなく、他の変数$x_3^{(t)}$を含んでいる。したがって、一筆書き多項式の係数が時間的に変化し、更新式の時間発展が、第１例よりも複雑になる。他の変数$x_2$～$x_8$の更新式についても同様である。

【００６５】

また、第２例は、第１例を包含しており、第１例と同様の有用性が得られる。さらに、第２例では、置換多項式（一筆書き多項式）の係数部分を他の変数によって変化させることができるため、係数部分が、時間的に値が変化しない定数を含んでいてもその値は小さくてよい。したがって、値が変化しない定数に大きなメモリを割り当てなくても良くなり、メモリ効率が向上する。

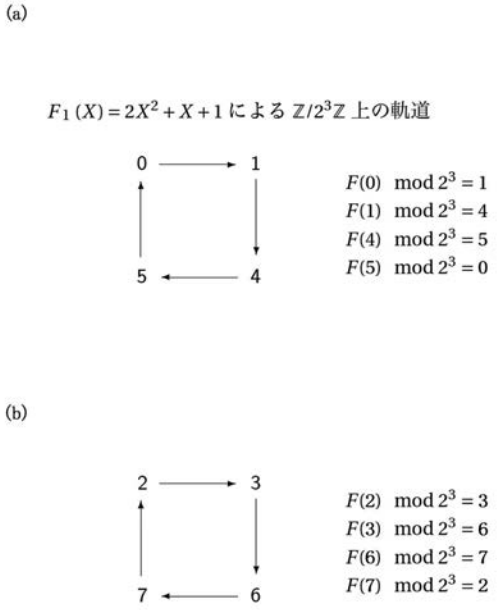
【００６６】

［３．５　更新式の第２例の評価］

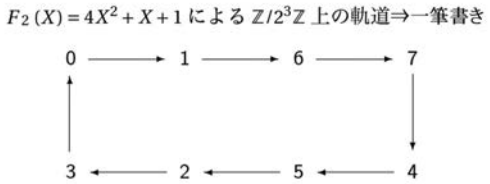
更新式の第２例の乱数性の評価を、上記の具体例として示したｎ個の更新式を用いて行った。

【００６７】
評価の方法は、第１例の評価方法とほぼ同様である。第２例では、５２セットについて評価した。また、第２例では、各変数が６４ビットであり、各変数の上位３２ビットを出力系列生成に用いた。
【００６８】
第２例の場合、実行速度の最高値は、４９３６．８２４７８０Ｍｂｓとなり、暗号化速度に換算すると、２．１６ｃｙｃｌｅ／Ｂｙｔｅとなり、非常に高い速度が得られている。
【００６９】
第２例の場合、ＮＩＳＴ　ＳＰ　８００－２２で定義される乱数検定の結果は、５２セット中、４０セットが、１８８項目すべてについて合格した。第２例においても良好な乱数性が確認された。
【００７０】
本発明は、上記実施形態に限定されるものではなく、様々な変形が可能である。
【符号の説明】
【００７１】
１００　乱数発生装置
１１０　生成器
１２０　記憶部
１３０　演算部

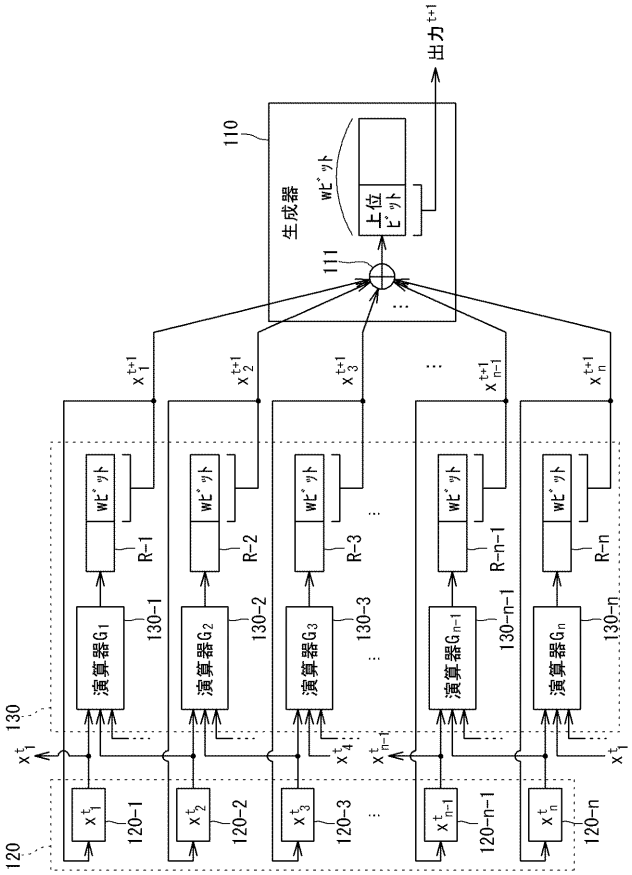
【図１】




【図２】



【図３】


出力$^{t+1}$
110
生成器
wビット
上位ビット
111
$x_1^{t+1}$
$x_2^{t+1}$
$x_3^{t+1}$
$x_{n-1}^{t+1}$
$x_n^{t+1}$
R-1
R-2
R-3
R-n-1
R-n
演算器$G_1$
演算器$G_2$
演算器$G_3$
演算器$G_{n-1}$
演算器$G_n$
130-1
130-2
130-3
130-n-1
130-n
130
120
$x_1^t$
$x_2^t$
$x_3^t$
$x_4^t$
$x_{n-1}^t$
$x_n^t$
120-1
120-2
120-3
120-n-1
120-n

【国際調査報告】

**INTERNATIONAL SEARCH REPORT**

International application No.
PCT/JP2017/008294

A. CLASSIFICATION OF SUBJECT MATTER
*G06F7/58*(2006.01)i, *G09C1/00*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F7/58, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2017
Kokai Jitsuyo Shinan Koho 1971-2017 Toroku Jitsuyo Shinan Koho 1994-2017

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | WO 2005/073842 A1 (Victor Company of Japan, Ltd.), 11 August 2005 (11.08.2005), paragraphs [0014] to [0036] & US 2007/0174374 A1 paragraphs [0022] to [0043] & CN 1914590 A | 1-6 |
| A | JP 2002-99408 A (Hitachi Kokusai Electric Inc.), 05 April 2002 (05.04.2002), paragraphs [0018] to [0048] (Family: none) | 1-6 |

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 05 April 2017 (05.04.17) | 18 April 2017 (18.04.17) |
| Name and mailing address of the ISA/<br>Japan Patent Office<br>3-4-3,Kasumigaseki,Chiyoda-ku,<br>Tokyo 100-8915,Japan | Authorized officer<br><br>Telephone No. |

Form PCT/ISA/210 (second sheet) (January 2015)

**INTERNATIONAL SEARCH REPORT**

International application No.
PCT/JP2017/008294

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | JP 2005-107910 A (National Institute of Information and Communications Technology), 21 April 2005 (21.04.2005), paragraphs [0004] to [0015] (Family: none) | 1-6 |

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２０１７／００８２９４

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl. G06F7/58(2006.01)i, G09C1/00(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl. G06F7/58, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

| | |
|---|---|
| 日本国実用新案公報 | １９２２－１９９６年 |
| 日本国公開実用新案公報 | １９７１－２０１７年 |
| 日本国実用新案登録公報 | １９９６－２０１７年 |
| 日本国登録実用新案公報 | １９９４－２０１７年 |

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

| 引用文献のカテゴリー＊ | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求項の番号 |
|---|---|---|
| A | WO 2005/073842 A1 (日本ビクター株式会社) 2005.08.11, 段落[0014]-[0036] & US 2007/0174374 A1 , 段落[0022]-[0043] & CN 1914590 A | 1-6 |
| A | JP 2002-99408 A (株式会社日立国際電気) 2002.04.05, 段落[0018]-[0048] (ファミリーなし) | 1-6 |
| A | JP 2005-107910 A (独立行政法人情報通信研究機構) 2005.04.21, 段落[0004]-[0015] (ファミリーなし) | 1-6 |

☐ Ｃ欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

| | |
|---|---|
| 国際調査を完了した日<br>０５．０４．２０１７ | 国際調査報告の発送日<br>１８．０４．２０１７ |
| 国際調査機関の名称及びあて先<br>日本国特許庁（ＩＳＡ／ＪＰ）<br>郵便番号１００－８９１５<br>東京都千代田区霞が関三丁目４番３号 | 特許庁審査官（権限のある職員）<br>５Ｕ ４２３６<br>田川 泰宏<br>電話番号 ０３－３５８１－１１０１ 内線 ３５６５ |

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ

（注）この公表は、国際事務局（ＷＩＰＯ）により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願（日本語実用新案登録出願）の国際公開の効果は、特許法第１８４条の１０第１項(実用新案法第４８条の１３第２項）により生ずるものであり、本掲載とは関係ありません。