

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-202017
(P2001-202017A)

(43) 公開日 平成13年7月27日 (2001.7.27)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 0 9 C 1/00	6 5 0	G 0 9 C 1/00	6 5 0 Z 5 J 1 0 4
G 0 6 G 7/26		G 0 6 G 7/26	A 9 A 0 0 1

審査請求 有 請求項の数 7 O L (全 13 頁)

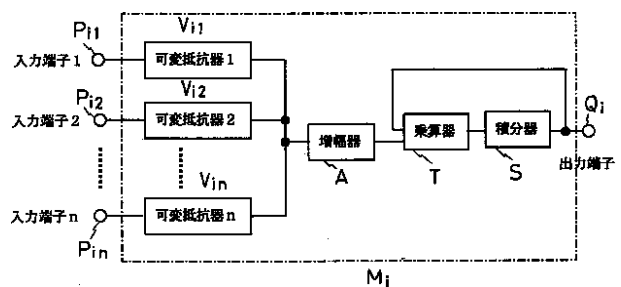
(21) 出願番号	特願2000-9224(P2000-9224)	(71) 出願人	500026887 農林水産省農業研究センター 茨城県つくば市観音台3-1-1
(22) 出願日	平成12年1月18日(2000.1.18)	(71) 出願人	399128415 平藤 雅之 茨城県つくば市吾妻4-13-23
		(72) 発明者	平藤 雅之 茨城県つくば市観音台3-1-1 農林水産省農業研究センター内
		(74) 代理人	100093399 弁理士 瀬谷 徹 (外2名)
		Fターム(参考)	5J104 AA18 NA08 NA21 9A001 BB05 EE02 EE03 KK12

(54) 【発明の名称】 単純な演算要素による任意関数発生回路並びにそれを用いた暗号化方法

(57) 【要約】

【課題】 簡便な装置による複雑な関数及び波形の生成する演算回路を提供する。

【解決手段】 アナログ乗算器、増幅器、周波数通倍器を用いて一般化ロトカ-ポルテラ方程式に相当する非線形アナログ回路を構成し、高速に演算させる。



【特許請求の範囲】

【請求項1】 単純な演算要素の回路素子を用いて、下記の一般化トロカ - ボルテラ方程式(1)式を演算する

$$\frac{dx_i}{dt} = x_i \left(r_i + \sum_{j=1}^n \mu_{ij} x_j \right) \quad (i = 1, 2, \dots, n) \quad (1)$$

(x_i はシステムの構成する要素を代表する個体群 i の個体数、 μ_{ij} は前記要素間の相互作用定数、 r_i は前記個体群 i の成長率で前記各要素に固有の定数値。) 複数 n 個の入力端子及び 1 個の出力端子を有する n 個のモジュール群と、第 1 のモジュールの出力端子と前記 n 個のモジュールのそれぞれの第 1 の入力端子を接続する第 1 の接続線と、第 2 のモジュールの出力端子と前記 n 個のモジュールのそれぞれの第 2 の入力端子を接続する第 2 の接続線と、以下同様に順次接続し、最後に第 n のモジュールの出力端子と前記 n 個のモジュールのそれぞれの第 n の入力端子を接続する第 n の接続線とを備え、前記各モジュールはそれぞれ、その n 個の入力端子とそれぞれ接続する n 個の可変抵抗器群と、それらの出力を

$$\frac{dx_i}{dt} = x_i \sum_{j=1}^n \mu_{ij} x_j \quad (i = 1, \dots, n) \quad (7)$$

前記演算回路は、前記 n 個のモジュール群の各出力端子では、任意関数が発生するシステムを構成する要素を代表する個体群 i の個体数 x_i ($i = 1, 2, \dots, n$) が前記各モジュールの出力信号として出力すると共にそれらの出力を前記 n 個の入力接続線を経由して前記モジュール群の入力端子群へ送り、各モジュールの入力端子群では相互作用定数 μ_{ij} が設定された前記可変抵抗器を介して、前記出力合算接続線で合算し、その合算値と当該モジュールの出力値とを前記乗算器で乗算し、その値を前記積分回路で積分し、それぞれの出力端子へ出力し、以上の過程を繰り返すことにより前記変形した一般化トロカ - ボルテラ方程式の演算を実行することを特徴とする単純な演算要素による任意関数発生回路。

【請求項2】 前記可変抵抗器へのそれぞれの相互作用定数 μ_{ij} の設定は、各モジュール内でプログラマブルに前記可変抵抗器群のそれぞれの値を変更する相互作用定数設定手段を備えて行うか、もしくは、各モジュール内のそれぞれの可変抵抗器群に可変抵抗器として FET 半導体素子回路を備え、それを外部からの制御信号で抵抗値を変更して行うかのいずれかであることを特徴とする請求項1記載の単純な演算要素による任意関数発生回路。

【請求項3】 請求項1又は2記載の(7)式に変形した一般化トロカ - ボルテラ方程式を解く演算回路であつ

$$e = x_1 \sin \omega_1 t + x_2 \sin \omega_2 t + \dots + x_n \sin \omega_n t \quad (8)$$

また、前記周波数シンセサイザから出力する設定値は、相互作用係数 μ_{ij} を周波数多重化した下記の(9)式

演算回路であつて、

[数1]

合算するための前記可変抵抗器の出力端子を接続する出力合算接続線と、増幅器で介したその合算値と当該モジュールの出力値とを乗算する乗算器と、その出力を積分する積分器とを備え、前記相互作用定数 μ_{ij} は前記各モジュール内の可変抵抗器の値に相当させ、前記モジュール群の任意の1個である第1のモジュールを常に1を出力するモジュールとし、第1の接続線を介した各モジュールの第1の入力端子から入力する可変抵抗器の値 μ_{ij} に固定値 r_i を担わせると、前記一般化トロカ - ボルテラ方程式は下記の(7)式に変形できる関係を用いて、

[数7]

て、

それぞれ1個の信号入出力端子を有する複数 n 個のモジュール群と、それらの入出力端子を接続する1本の信号バス結線とを備え、

前記各モジュールは、周波数シンセサイザの出力値と前記入出力端子における前記信号バス結線からの入力値とを乗算する第1の乗算器と、その出力値から交流成分を取り除くローパスフィルタと、その出力値を入力する第2の乗算器と、その出力を積分する積分器と、その積分器の出力値を、前記第2の乗算器に入力し、前記ローパスフィルタの出力値と乗算させるための接続回路と、オシレータと、前記積分器の出力値と前記オシレータの出力値を乗算し、入出力端子に接続する第3の乗算器とを少なくとも備え、

各モジュールの前記積分器の出力値 x_i ($i = 1, 2, \dots, n$) を任意波形の関数が発生するシステムを構成する要素の値として、その出力値 x_i と角周波数 ω_i の前記オシレータの生成する搬送波信号を第3乗算器で乗算し、その乗算値 $x_i \sin \omega_i t$ を各モジュールから前記1本の信号バス結線上に出力し、一方、その信号バス結線上から下記の式(8)に示す各モジュールの出力の周波数多重化された加算値 e を入力し、

[数8]

に示す電圧値 W_i とし、

[数9]

$$W_i = \mu_{1i} \sin \omega_1 t + \mu_{2i} \sin \omega_2 t + \dots + \mu_{ni} \sin \omega_n t \quad (9)$$

前記加算値 e とを前記第 1 乗算器に入力してその乗算値を前記ローパスフィルタを通して下記の式 (10) 直流

$$eW_i = \mu_{1i} x_1 + \mu_{2i} x_2 + \dots + \mu_{ni} x_n \quad (10)$$

前記第 2 の乗算器で、前記 eW_i の値と前記積分器の出力 x_i を乗算し、次段の前記積分器で、その乗算値を積分して x_i の信号を出力し、次段の第 3 の乗算器で、その x_i の信号と前記オシレータで生成する搬送波信号を乗算し $x_i \sin \omega_i t$ の信号を出力し、前記入出力端子を介して外部の信号バス結線へ出力し、以上の過程を繰り返すことにより一般化トロカ - ポルテラ方程式の演算を実行することを特徴とする単純な演算要素による任意関数発生回路。

【請求項 4】 前記周波数シンセサイザによる電圧値 W_i の設定手段は各モジュール内部にある前記オシレータからの信号を引き出して重み付け加算する増幅回路として外部に備えるか、もしくは、独立した回路としてそれぞれのモジュール内部に備えるかのいずれかであることを特徴とする請求項 3 記載の単純な演算要素による任意関数発生回路。

【請求項 5】 請求項 1 又は 2 記載の (7) 式に変形した一般化トロカ - ポルテラ方程式を解く演算回路であって、周波数シンセサイザの出力値 W を入力値の 1 つとして入

$$e_1 = x_1 \sin(\omega_0 t) + x_2 \sin(2\omega_0 t) + \dots + x_n \sin(n\omega_0 t) \quad (11)$$

この周波数多重化信号 e_1 は基本周波数 ω_0 の周期より十分長い時間だけ前記遅延回路で遅延される閉ループ中に常時保存させ、一方、前記第 1 の周波数通倍器は信号 e_1 の周波数を n 倍 (n) して信号 e_2 を出力させ、前記第 2 の周波数通倍器は信号 e_1 の周波数を n 倍 (n) して信号 e_3 を出力させ、前記周波数シンセサイザは相互作用係数 μ_{ij} ($i = 1, 2, \dots, n; j = 1, 2, \dots, n$) をそれぞれ周波数多重化した信号 W

$$e_5 = x_1 \left(\sum_{j=1}^n \mu_{1j} x_j \right) \sin(\omega_0 t) + x_2 \left(\sum_{j=1}^n \mu_{2j} x_j \right) \sin(2\omega_0 t) + \dots + x_n \left(\sum_{j=1}^n \mu_{nj} x_j \right) \sin(n\omega_0 t) \quad (18)$$

この生成された信号 e_5 は (7) 式の右辺の周波数多重化微分値信号 (de_1/dt) に相当し、この信号 e_5 は前記加算器において信号 e_1 と加算されて、その結果 (7) 式の積分が実行される演算回路となり、1 個の前記モジュールにより任意の n に対して (7) 式の演算を行い一般化トロカ - ポルテラ方程式を解く演算回路となることを特徴とする単純な演算要素による任意関数発生回路。

【請求項 6】 請求項 5 記載の単純な演算要素による任

成分のみとし、
[数 10]

力する第 1 の乗算器と、その出力値から第 1 の周波数成分をカットする第 1 のローパスフィルタと、その出力値 e_4 を入力値の 1 つとして入力する第 2 の乗算器と、その出力値から第 1 の周波数より低い第 2 の周波数成分をカットする第 2 のローパスフィルタと、その出力値 e_5 を入力値の 1 つとして入力する加算器と、その出力値 e_1 を遅延させると共にその出力値を前記加算器の第 2 の入力値とする遅延回路と、また、その出力値 e_1 の周波数を通倍すると共にその出力値 e_2 を第 2 の乗算器の第 2 の入力値とする第 1 の周波数通倍器と、さらに、前記出力値 e_1 の周波数を通倍すると共にその出力値 e_3 を第 1 の乗算器の第 2 の入力値とする第 2 の周波数通倍器とを 1 個のモジュールに備え、

前記 (7) 式の信号 x_i ($i = 1, 2, \dots, n$) を振幅の大きさが x_i の交流信号 $x_i \sin(\omega_0 t)$ 、($i = 1, 2, \dots, n$, ω_0 は基本角周波数) とし、前記演算回路の加算器の出力値 e_1 を x_i の全信号を加算した下記の (11) 式に示す周波数多重化信号となるようにし、

[数 11]

を一度に生成させて出力させ、前記第 1 の乗算器は、信号 e_3 と W の乗算を行わせ、第 1 のローパスフィルタで ω_0 近傍周波数以上の成分をカットし、信号 e_4 を出力させ、前記第 2 の乗算器は信号 e_2 と e_4 の乗算を行わせ、第 2 のローパスフィルタで ω_0 近傍周波数以上の成分をカットし、下記の (18) 式に示す信号 e_5 を出力させ、

[数 18]

意関数発生回路を用いる暗号化変調方法であって、その演算回路の前記周波数シンセサイザの出力信号 W 及び前記周波数多重化信号 e_1 の初期値 $e_1|_{t=0}$ のそれぞれの値の違いにより、出力される信号 e_1 の時間変化パターンがそれぞれ異なることを利用して、初期値 $e_1|_{t=0}$ を暗号化変調したいコードとし、信号 W を暗号化変調のための鍵コードとし、信号 e_1 の時間変化パターン或は時刻 T における信号 $e_1|_{t=T}$ を暗号化変調された信号とすることを特徴とする暗号化方法。

【請求項 7】 請求項 5 記載の単純な演算要素による任意関数発生回路を用いる暗号化変調方法であって、その演算回路の前記周波数シンセサイザの出力信号 W 及び前記周波数多重化信号 e₁ の初期値 e₁ | t = 0 のそれぞれの値の違いにより、出力される信号 e₁ の時間変化パターンがそれぞれ異なることを利用して、信号 W を暗号化変調したいコードとし、信号 e₁ | t = 0 を暗号化変調のための鍵コードとし、信号 e₁ の時間変化パターン或は時刻 T における信号 e₁ | t = T を暗号化変調された信号とすることを特徴とする暗号化方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、複雑なシステムのシミュレーションの高速化技術、信号の変調及び暗号化秘匿化の技術に関する。

【0002】

【従来の技術】定量的な変化を記述する数理モデルはパラメータの値によって特定の関数を生成する一種の任意関数発生器である。これをアナログ演算回路でシミュレートすると高速なシミュレーションができる。そのため、かつては実際にアナログコンピュータでこの関数を

$$\frac{dx_i}{dt} = x_i \left(r_i + \sum_{j=1}^m \mu_{ij} x_j \right) \quad (i = 1, 2, \dots, n) \quad (1)$$

ここで、x_i はシステムを構成する要素を代表するパラメータ（個体群 i の個体数）、μ_{ij} は要素間の相互作用定数、r_i は個体群 i の成長率で、前記各要素に固有の定数値、すなわち要素固有のパラメータである。この方程式は n が十分に大きいと任意の正の連続関数を任意の精度で近似できる。n や μ_{ij} を変えることで、様々な変化する x_i のパターンを生成することができる。そのため、現象のモデリングだけでなく、任意波形発生器としても広い用途が考えられる。本発明は、この式の対称性に着目して、この演算をハードウェア化または多数のデジタルコンピュータによる並列処理によるエミュレーションで行うことで高速化する技術である。

【0005】すなわち、本発明は前述した点に鑑みてな

$$\frac{dx_i}{dt} = x_i \left(r_i + \sum_{j=1}^m \mu_{ij} x_j \right) \quad (i = 1, 2, \dots, n) \quad (1)$$

(x_i はシステムの構成する要素を代表する個体群 i の個体数、μ_{ij} は前記要素間の相互作用定数、r_i は前記個体群 i の成長率で前記各要素に固有の定数値。) 複数 n 個の入力端子及び 1 個の出力端子を有する n 個のモジュール群と、第 1 のモジュールの出力端子と前記 n 個のモジュールのそれぞれの第 1 の入力端子を接続する第 1 の接続線と、第 2 のモジュールの出力端子と前記 n 個のモジュールのそれぞれの第 2 の入力端子を接続する第 2 の接続線と、以下同様に順次接続し、最後に第 n のモジュールの出力端子と前記 n 個のモジュールのそれぞ

シミュレートしていた。しかし、問題ごとに回路の結線を組み替えるのが煩雑であることと問題が大規模になると回路が巨大になるため、実際にはほとんど使われていない。その後、アナログ演算回路の結線をプログラムによって電氣的に変更できるようになったが、複雑な回路の高集積化は困難であるためアナログ演算方式は使われていない。

【0003】

【発明が解決しようとする課題】多数の変数を持つ現象を高速にシミュレートするためにはアナログ演算回路による任意関数の発生を行うことが有利であるが、実用化のためにはアナログ演算回路の結線を物理的に変更することなく種々の異なる関数をプログラブルに発生させることが必要である。また高集積化のためには、RAM のように単純なマスクパターンの繰り返しで実現できる単純な回路構成でなければならない。また、回路を構成する部品数もできる限り少なくしなければならない。

【0004】一方、一般化ロトカ - ボルテラ方程式は以下のような微分方程式で表され、生物群集の動態や植物生長モデルなどに利用されている。

[数 1]

されたものであり、その目的とするところは、単純な演算要素、つまり、比較的単純な回路素子を用いた演算回路により、一般化ロトカ - ボルテラ方程式が解ける任意波形発生回路或は任意関数発生回路を提供するものであり、また、その任意関数発生回路を用いた暗号化変調方法を提供するものである。

【0006】

【課題を解決するための手段】前記課題を解決するため、本発明の単純な演算要素による任意関数発生回路は、単純な演算要素の回路素子を用いて、下記の一般化ロトカ - ボルテラ方程式 (1) 式を演算する演算回路であって、

[数 1]

れの第 n の入力端子を接続する第 n の接続線とを備え、前記各モジュールはそれぞれ、その n 個の入力端子とそれぞれ接続する n 個の可変抵抗器群と、それらの出力を合算するための前記可変抵抗器の出力端子を接続する出力合算接続線と、増幅器で介したその合算値と当該モジュールの出力値とを乗算する乗算器と、その出力を積分する積分器とを備え、前記相互作用定数 μ_{ij} は前記各モジュール内の可変抵抗器の値に相当させ、前記モジュール群の任意の 1 個である第 1 のモジュールを常に 1 を出力するモジュールとし、第 1 の接続線を介した各モジ

ジュールの第 1 の入力端子から入力する可変抵抗器の値 μ_{ij} に固定値 r_i を担わせると、前記一般化トロカ - ボ

$$\frac{dx_i}{dt} = x_i \sum_{j=1}^n \mu_{ij} x_j \quad (i = 1, \dots, n)$$

前記演算回路は、前記 n 個のモジュール群の各出力端子では、任意関数が発生するシステムを構成する要素を代表する個体群 i の個体数 x_i ($i = 1, 2, \dots, n$) が前記各モジュールの出力信号として出力すると共にそれらの出力を前記 n 個の入力接続線を経由して前記モジュール群の入力端子群へ送り、各モジュールの入力端子群では相互作用定数 μ_{ij} が設定された前記可変抵抗器を介して、前記出力合算接続線で合算し、その合算値と当該モジュールの出力値とを前記乗算器で乗算し、その値を前記積分回路で積分し、それぞれの出力端子へ出力し、以上の過程を繰り返すことにより前記変形した一般化トロカ - ボルテラ方程式の演算を実行することを特徴とする。

【0007】また、前記可変抵抗器へのそれぞれの相互作用定数 μ_{ij} の設定は、各モジュール内でプログラム的に前記可変抵抗器群のそれぞれの値を変更する相互作用定数設定手段を備えて行うか、もしくは、各モジュール内のそれぞれの可変抵抗器群に可変抵抗器として FET 半導体素子回路を備え、それを外部からの制御信号で抵抗値を変更して行うかのいずれかであることを特徴とする。

【0008】また、請求項 1 又は 2 記載の (7) 式に変

$$e = x_1 \sin \omega_1 t + x_2 \sin \omega_2 t + \dots + x_n \sin \omega_n t \quad (8)$$

また、前記周波数シンセサイザから出力する設定値は、相互作用係数 μ_{ij} を周波数多重化した下記の (9) 式

$$W_i = \mu_{i1} \sin \omega_1 t + \mu_{i2} \sin \omega_2 t + \dots + \mu_{in} \sin \omega_n t \quad (9)$$

前記加算値 e とを前記第 1 乗算器に入力してその乗算値を前記ローパスフィルタを通して下記の式 (10) 直流

$$eW_i = \mu_{i1} x_1 + \mu_{i2} x_2 + \dots + \mu_{in} x_n \quad (10)$$

前記第 2 の乗算器で、前記 eW_i の値と前記積分器の出力 x_i を乗算し、次段の前記積分器で、その乗算値を積分して x_i の信号を出力し、次段の第 3 の乗算器で、その x_i の信号と前記オシレータで生成する搬送波信号を乗算し $x_i \sin \omega_i t$ の信号を出力し、前記入出力端子を介して外部の信号バス結線へ出力し、以上の過程を繰り返すことにより一般化トロカ - ボルテラ方程式の演算を実行することを特徴とする。

【0009】また、前記周波数シンセサイザによる電圧値 W_i の設定手段は各モジュール内部にある前記オシレータからの信号を引き出して重み付け加算する増幅回路として外部に備えるか、もしくは、独立した回路としてそれぞれのモジュール内部に備えるかのいずれかである

ルテラ方程式は下記の (7) 式に変形できる関係を用いて、[数 7]

(7)

形した一般化トロカ - ボルテラ方程式を解く演算回路であって、それぞれ 1 個の信号入出力端子を有する複数 n 個のモジュール群と、それらの入出力端子を接続する 1 本の信号バス結線とを備え、前記各モジュールは、周波数シンセサイザの出力値と前記入出力端子における前記信号バス結線からの入力値とを乗算する第 1 の乗算器と、その出力値から交流成分を取り除くローパスフィルタと、その出力値を入力する第 2 の乗算器と、その出力を積分する積分器と、その積分器の出力値を、前記第 2 の乗算器に入力し、前記ローパスフィルタの出力値と乗算させるための接続回路と、オシレータと、前記積分器の出力値と前記オシレータの出力値を乗算し、入出力端子に接続する第 3 の乗算器とを少なくとも備え、各モジュールの前記積分器の出力値 x_i ($i = 1, 2, \dots, n$) を任意波形の関数が発生するシステムを構成する要素の値として、その出力値 x_i と角周波数 ω_i の前記オシレータの生成する搬送波信号を第 3 乗算器で乗算し、その乗算値 $x_i \sin \omega_i t$ を各モジュールから前記 1 本の信号バス結線上に出力し、一方、その信号バス結線上から下記の式 (8) に示す各モジュールの出力の周波数多重化された加算値 e を入力し、

[数 8]

に示す電圧値 W_i とし、

[数 9]

成分のみとし、

[数 10]

(10)

ことを特徴とする。

【0010】また、請求項 1 又は 2 記載の (7) 式に変形した一般化トロカ - ボルテラ方程式を解く演算回路であって、周波数シンセサイザの出力値 W を入力値の 1 つとして入力する第 1 の乗算器と、その出力値から第 1 の周波数成分をカットする第 1 のローパスフィルタと、その出力値 e_4 を入力値の 1 つとして入力する第 2 の乗算器と、その出力値から第 1 の周波数より低い第 2 の周波数成分をカットする第 2 のローパスフィルタと、その出力値 e_5 を入力値の 1 つとして入力する加算器と、その出力値 e_1 を遅延させると共にその出力値を前記加算器の第 2 の入力値とする遅延回路と、また、その出力値 e_1 の周波数を逡倍すると共にその出力値 e_2 を第 2 の乗

算器の第2の入力値とする第1の周波数通倍器と、さらに、前記出力値 e_1 の周波数を通倍すると共にその出力値 e_3 を第1の乗算器の第2の入力値とする第2の周波数通倍器とを1個のモジュールに備え、前記(7)式の信号 x_i ($i = 1, 2, \dots, n$)を振幅の大きさが x_i

$$e_1 = x_1 \sin(\omega_0 t) + x_2 \sin(2\omega_0 t) + \dots + x_n \sin(n\omega_0 t) \quad (11)$$

この周波数多重化信号 e_1 は基本周波数 ω_0 の周期より十分長い時間だけ前記遅延回路で遅延される閉ループ中に常時保存させ、一方、前記第1の周波数通倍器は信号 e_1 の周波数を n 倍して信号 e_2 を出力させ、前記第2の周波数通倍器は信号 e_1 の周波数を n 倍して信号 e_3 を出力させ、前記周波数シンセサイザは相互作用係数 μ_{ij} ($i = 1, 2, \dots, n; j = 1, 2, \dots, n$)をそれぞれ周波数多重化した信号 W

$$e_5 = x_1 \left(\sum_{j=1}^n \mu_{1j} x_j \right) \sin(\omega_0 t) + x_2 \left(\sum_{j=1}^n \mu_{2j} x_j \right) \sin(2\omega_0 t) + \dots + x_n \left(\sum_{j=1}^n \mu_{nj} x_j \right) \sin(n\omega_0 t)$$

(18)

この生成された信号 e_5 は(7)式の右辺の周波数多重化微分値信号(de_1/dt)に相当し、この信号 e_5 は前記加算器において信号 e_1 と加算されて、その結果(7)式の積分が実行される演算回路となり、1個の前記モジュールにより任意の n に対して(7)式の演算を行い一般化トロカ-ボルテラ方程式を解く演算回路となることを特徴とする。

【0011】また、本発明の暗号化変調方法は、請求項5記載の単純な演算要素による任意関数発生回路を用いる暗号化変調方法であって、その演算回路の前記周波数シンセサイザの出力信号 W 及び前記周波数多重化信号 e_1 の初期値 $e_1|_{t=0}$ のそれぞれの値の違いにより、出力される信号 e_1 の時間変化パターンがそれぞれ異なることを利用して、初期値 $e_1|_{t=0}$ を暗号化変調したいコードとし、信号 W を暗号化変調のための鍵コードとし、信号 e_1 の時間変化パターン或は時刻 T における信号 $e_1|_{t=T}$ を暗号化変調された信号とすることを特徴とする。

【0012】また、請求項5記載の単純な演算要素による任意関数発生回路を用いる暗号化変調方法であって、その演算回路の前記周波数シンセサイザの出力信号 W 及び前記周波数多重化信号 e_1 の初期値 $e_1|_{t=0}$ のそれぞれの値の違いにより、出力される信号 e_1 の時間変化パターンがそれぞれ異なることを利用して、信号 W を暗号化変調したいコードとし、信号 $e_1|_{t=0}$ を暗号化変調のための鍵コードとし、信号 e_1 の時間変化パターン或は時刻 T における信号 $e_1|_{t=T}$ を暗号化変調された信号とすることを特徴とする。

の交流信号 $x_i \sin(i\omega_0 t)$ 、($i = 1, 2, \dots, n$, ω_0 は基本角周波数)とし、前記演算回路の加算器の出力値 e_1 を x_i の全信号を加算した下記の(11)式に示す周波数多重化信号となるようにし、

[数11]

を一度に生成させて出力させ、前記第1の乗算器は、信号 e_3 と W の乗算を行わせ、第1のローパスフィルタで ω_0 近傍周波数以上の成分をカットし、信号 e_4 を出力させ、前記第2の乗算器は信号 e_2 と e_4 の乗算を行わせ、第2のローパスフィルタで ω_0 近傍周波数以上の成分をカットし、下記の(18)式に示す信号 e_5 を出力させ、

[数18]

【0013】

【発明の実施の形態】(タイプ1)(第1実施例)

本発明の第1実施例を図1、図2に示す。図2は一般化トロカ-ボルテラ方程式の演算回路全体を示し、その中の回路モジュール部のブロック図を図1に示す。ここで、 M_i は任意のモジュールを表し、演算回路はモジュール n 個で構成される。各モジュールはそれぞれ n 個の入力端子 P_{ij} と1個の出力端子 Q_i を有する。第1のモジュール M_1 の出力端子 Q_1 と各モジュールの第1の入力端子 $P_{11}, P_{21}, \dots, P_{n1}$ に接続する第1の接続線と、第2のモジュール M_2 の出力端子 Q_2 と各モジュールの第2の入力端子 $P_{12}, P_{22}, \dots, P_{n2}$ に接続する第2の接続線と、以下同様に順次接続し、最後に第 n のモジュールの出力端子 Q_n と各モジュールの第 n 番目の入力端子 $P_{1n}, P_{2n}, \dots, P_{nn}$ に接続する第 n の接続線を備えている。一方、各モジュールはそれぞれ n 個の入力端子 P_{ij} とそれぞれ接続する n 個の可変抵抗器群 V_{ij} とそれらの出力を合算する接続線と、増幅器 A を介してその合算値とそのモジュール出力値とを乗算する乗算器 T とその出力を積分する積分器 S を備えている。一般化トロカ-ボルテラ方程式の演算は図1で示すブロックダイアグラムを有する回路モジュール M_i を相互に図2のように結線することで実現できる。ここで、 μ_{ij} は各モジュール内の可変抵抗器 V_{ij} の値に相当し、 r_i は固定値を出力する特殊なモジュールを一つ用意しておき、そのモジュールからの入力値とする。すなわち、(1)式を、

[数2]

$$\frac{dx_i}{dt} = x_i \left(r_i + \mu_{i1} x_1 + \sum_{j=2}^n \mu_{ij} x_j \right) \quad (i = 1, 2, \dots, n) \quad (2)$$

と書き換えておき、ここで第1のモジュールM₁を常に [数3]
x₁ = 1を出力する固定値出力のモジュールとすると、

$$\frac{dx_i}{dt} = x_i \left(r_i + \mu_{i1} x_1 + \sum_{j=2}^n \mu_{ij} x_j \right) \quad (i = 2, 3, \dots, n) \quad (3)$$

ただし、 [数4]

$$x_1 = 1 \quad (4)$$

である。

【0014】ここで、右辺の括弧内で定数値(バイアス値)を与えているr_iの役割を、常時固定値1を出力する第1のモジュールM₁(x₁ = 1)からの重み付き入

力μ_{i1}に担わせて、μ_{i1}がr_iの値であると仮定すると、

[数5]

$$\frac{dx_i}{dt} = x_i \left(\mu_{i1} x_1 + \sum_{j=2}^n \mu_{ij} x_j \right) \quad (i = 2, 3, \dots, n) \quad (5)$$

ただし、仮定により、

[数6]

$$\mu_{i1} = r_i \quad (6)$$

である。括弧内の項μ_{i1}x₁を(6)式右辺の中に戻して、

[数7]

$$\frac{dx_i}{dt} = x_i \sum_{j=1}^n \mu_{ij} x_j \quad (i = 1, \dots, n) \quad (7)$$

となる。すなわち、固定値出力のモジュールを導入することで(1)式は(7)式に単純化され、右辺の演算は積和演算を行う積和演算回路(図1の可変抵抗器V_{ij}(j = 1 ~ n)と増幅器Aで構成される)とその演算結果にx₁の値を乗算する乗算回路(図1の乗算器T)で実現できる。更に、この値を積分回路(図1の積分器S)によって積分するとx_i(i = 2, 3, ..., n)の値が得られる。

【0015】x_i(i = 2, 3, ..., n)の値の時間変化パターンはμ_{ij}の設定値(図1の可変抵抗器V_{ij}(j = 1 ~ n)の設定値)によって任意に変えることができることから、図1のモジュールM_iをn個接続した回路はn - 1チャンネルの任意関数発生器として利用できる。

【0016】可変抵抗器V_{ij}の値μ_{ij}を外部から変更する場合には、FET(電界効果トランジスタ)等の素子を使って可変にする。

【0017】数個から数十個程度のモジュール数であれば、この回路である程度の複雑さを有する関数は生成できる。要素数(7式のn)が多いと、結線数はn²のオーダーで増えるため集積化が困難となる。また、可変抵抗器V_{ij}の値μ_{ij}を外部から制御するためには複雑な回路が別途必要となる。

【0018】(タイプ2)(第2実施例)本発明の第2実施例を図3、図4に示す。図4は一般化ロトカ-ポルテラ方程式の演算回路全体を示し、その中の回路モジ

ール部のブロック部を図3に示す。ここで、N_iは任意のモジュールを表し、演算回路はモジュールn個で構成される。各モジュールはそれぞれ1個の入出力端子R_iを有する。各モジュールの入出力端子R_iは1本の信号バス結線に接続される。一方、各モジュールN_iは周波数シンセサイザF₁の出力値と前記入出力端子R_iにおける前記信号バス結線からの入力値と乗算する第1の乗算器T₁と、その出力値から交流成分を取り除くローパスフィルタLと、その出力値を入力する第2の乗算器T₂と、その出力を積分する積分器S₁と、その積分器S₁の出力値を前記第2乗算器T₂に入力し、前記ローパスフィルタLの出力値と乗算させるための接続回路と、オシレータGと、前記積分器S₁の出力値と前記オシレータGの出力値を乗算する入出力端子R_iに接続する第3の乗算器T₃を備えている。nが大きい場合に対しては、図3のように任意のモジュールN_iの入出力端子R_iの入出力を異なる周波数の正弦波とし(振幅の大きさを出力値とする)、周波数多重化によって信号伝送を行う。このようにすると1本の結線(信号バス)にすべての信号を載せることができ、図4のような単純な結線で相互結合が実現できる。すなわち、モジュールN_iの出力値をx_isin ω_itとすると、各モジュールN_iからの信号が1本の結線に加算されるため、結線上の電圧は、

[数8]

$$e = x_1 \sin \omega_1 t + x_2 \sin \omega_2 t + \dots + x_n \sin \omega_n t \quad (8)$$

である。相互作用係数 μ_{ij} についても、同様に交流信号 [数9] で表現する。すなわち、 x_1 への相互作用定数を、

$$W_i = \mu_{i1} \sin \omega_1 t + \mu_{i2} \sin \omega_2 t + \dots + \mu_{in} \sin \omega_n t \quad (9)$$

の電圧として供給する。これは各モジュール N_i の内部または外部に設けた周波数シンセサイザ F_1 で個別に生成する。なお、このシンセサイザ F_1 は各モジュール内部にあるオシレータ (OSC) G からの信号を重み付け加算する増幅回路とするか、あるいは、位相のずれは全く問題にならないため完全に独立した回路として図3のモジュール内部に設置しても良い。

【0019】図3に示すモジュール N_i 内ではまず第1

$$eW_i = \mu_{i1} x_1 + \mu_{i2} x_2 + \dots + \mu_{in} x_n \quad (10)$$

となり、(10)式右辺の積和演算した値がリアルタイムに得られる。第2の乗算器 T_2 は、この信号と x_i の値を乗算した信号(7)式の右辺の値を出力する。次段の積分器 S_1 によってこの信号を積分し、 x_i の信号が得られる。次の第3の乗算器 T_3 は x_i の信号とオシレータ (OSC) G で生成した搬送波 $\sin \omega_i t$ の信号を乗算し、 $x_i \sin \omega_i t$ の信号を生成する。この信号は、第1の乗算器 T_1 へ入力させると同時に、入出力端子 R_i を通じて外部へ出力される。

【0020】このようなモジュール N_i を多数用意し、図4に示すように1本の信号線で結線するだけで、前述の一般化ロトカ - ボルテラ方程式に相当する演算ができる。

【0021】異なる周波数を用いて結線数を減らす方法はアナログ多重通信の基本技術の一つであり、ニューラルネット(学習しきい素子)のハードウェアに関して既に報告があり、公知の事実である。(横井博一、斉藤正男、1986:新しい学習素子 - Foulthreth -, 電子通信学会論文誌, Vol. J69-A, No. 6, 1173-1175)

【0022】本発明のタイプ2では、一般化ロトカ - ボルテラ方程式を計算する演算回路の内部に必要なモジュール間の膨大な結線数(タイプ1では n^2 のオーダーで増える)を信号の周波数多重化によって大幅に減らす(タイプ2では n のオーダーで増える)ことに新規性がある。

【0023】(タイプ3)(第3実施例)図4に示した回路では要素数が n の一般化ロトカ - ボルテラ方程式の演算を行うのに n 個のモジュールが必要で済む。モジュールの総数 n が多いほどより複雑な関数を表現できるようになるため、実装に際してはできるだけ全体の部品点数や配線数を減らすことが望ましい。次に述べる方法によって、1つのモジュールだけで任意の規模(任意の n)の一般化ロトカ - ボルテラ方程式の演算を行うこと

の乗算器 T_1 によって e と W_i の乗算された信号が生成される。乗算された信号には直流成分(搬送波 $\sin \omega_i t$ よりもゆっくりと変化する成分)と交流成分(周波数は各搬送波周波数の和と積)が含まれる。この信号からローパスフィルタ(LPF) L で直流成分だけを得ると、 [数10]

が可能となる。

【0024】そこで、本発明の第3実施例を図5に示す。図5は一般化ロトカ - ボルテラ方程式の演算回路全体を示し、しかも1つのモジュールとしたブロック図である。ここで、周波数シンセサイザ F_2 の出力値 W を入力値の1つとして入力する第1の乗算器 T_4 と、その出力値から第1の周波数成分をカットする第1のローパスフィルタ(LPF1) L_1 と、その出力値 e_4 を入力値の1つとして入力する第2の乗算器 T_5 と、その出力値から第1の周波数より低い第2の周波数成分をカットする第2のローパスフィルタ L_2 と、その出力値 e_5 を入力値の1つとして入力する加算器 B と、その出力値 e_1 を遅延させると共にその出力値を前記加算器 B の第2の入力値とする遅延回路 V と、また、その出力値 e_1 の周波数を逡倍すると共にその出力値 e_2 を第2の乗算器 T_5 の第2の入力値とする第1の周波数逡倍器 H_1 と、さらに、前記出力値 e_1 の周波数を逡倍すると共にその出力値 e_3 を第1の乗算器 T_4 の第2の入力値とする第2の周波数逡倍器 H_2 とを備えている。

【0025】搬送周波数を後述する方法で設定し、図5に示す回路で演算を行うと、更に少ない部品点数で同様の結果を得ることができる。

【0026】まず(7)式の信号 x_i ($i = 1, 2, \dots, n$) を振幅の大きさが x_i の交流信号 $x_i \sin(\omega_i t)$ ($i = 1, 2, \dots, n$) で表現する。ここで、 ω_0 は基本角周波数であり、値は任意である(実際に製作する際には、使用する目的・用途、部品の周波数特性などから決める)。すなわち、 x_i を ω_0 の整数倍の角周波数を有する信号の強度によって表現する。

【0027】この各交流信号は互いに線形独立であるから、全信号を加算して一つの信号線を使って伝送することができる(すなわち、周波数多重化による信号伝送のこと)。全信号を加算した周波数多重化信号は、

[数11]

$$e_1 = x_1 \sin(\omega_0 t) + x_2 \sin(2\omega_0 t) + \dots + x_n \sin(n\omega_0 t) \quad (11)$$

である。図5中では、この周波数多重化信号 e_1 は、遅延回路Vの入力値とする。

【0028】周波数多重化信号 e_1 は遅延回路Vで基本周波数 ω_0 の周期 ($2\pi/\omega_0$) よりも十分長い時間だけ遅延され、加算器Bを経て再び遅延回路Vに入力される。すなわち、周波数多重化信号 e_1 は遅延回路Vから出て再び遅延回路Vに戻るという閉ループの中で常時保存されている。

$$\frac{de_1}{dt} = \frac{dx_1}{dt} \sin(\omega_0 t) + \frac{dx_2}{dt} \sin(2\omega_0 t) + \dots + \frac{dx_n}{dt} \sin(n\omega_0 t) \quad (12)$$

である。加算器Bでは e_1 と de_1/dt が加算され、

$$e_1 + \frac{de_1}{dt} = \left(x_1 + \frac{dx_1}{dt}\right) \sin(\omega_0 t) + \left(x_2 + \frac{dx_2}{dt}\right) \sin(2\omega_0 t) + \dots + \left(x_n + \frac{dx_n}{dt}\right) \sin(n\omega_0 t) \quad (13)$$

となる。この加算演算はオイラー法による積分演算そのものであるから、加算器Bと遅延回路Vからなる閉ループ回路によって(7)式の積分演算が実行される。

【0030】さて、次の大きな問題は、いかにして周波数多重化微分値信号 de_1/dt をできるだけ単純な回路で得るかである。この問題の解決に当たって本発明で

$$e_2 = x_1 \sin(\alpha\omega_0 t) + x_2 \sin(2\alpha\omega_0 t) + \dots + x_n \sin(n\alpha\omega_0 t) \quad (14)$$

同様に第1の周波数通倍器2, H2は、信号 e_1 の周波数を β 倍して()、信号 e_3 を出力する。

$$e_3 = x_1 \sin(\beta\omega_0 t) + x_2 \sin(2\beta\omega_0 t) + \dots + x_n \sin(n\beta\omega_0 t) \quad (15)$$

周波数シンセサイザF2は相互作用係数 μ_{ij} ($i = 1, 2, \dots, n; j = 1, 2, \dots, n$) を周波数多重化

$$W = \mu_{11} \sin(\beta\omega_0 + \alpha\omega_0 + \omega_0 t) + \mu_{12} \sin(2\beta\omega_0 + \alpha\omega_0 + \omega_0 t) + \dots + \mu_{1n} \sin(n\beta\omega_0 + \alpha\omega_0 + \omega_0 t) \\ + \mu_{21} \sin(\beta\omega_0 + 2\alpha\omega_0 + 2\omega_0 t) + \mu_{22} \sin(2\beta\omega_0 + 2\alpha\omega_0 + 2\omega_0 t) + \dots + \mu_{2n} \sin(n\beta\omega_0 + 2\alpha\omega_0 + 2\omega_0 t) \\ M \\ + \mu_{n1} \sin(\beta\omega_0 + n\alpha\omega_0 + n\omega_0 t) + \mu_{n2} \sin(2\beta\omega_0 + n\alpha\omega_0 + n\omega_0 t) + \dots + \mu_{nn} \sin(n\beta\omega_0 + n\alpha\omega_0 + n\omega_0 t) \quad (16)$$

を出力する。

【0032】まず、第1の乗算器1, T4は e_3 とWの乗算を行い、 e_3 とWに含まれる交流信号の和周波数および差周波数からなる信号を生成する。この信号に対し

$$e_4 = \left(\sum_{j=1}^n \mu_{1j} x_j\right) \sin(\alpha\omega_0 + \omega_0 t) + \left(\sum_{j=1}^n \mu_{2j} x_j\right) \sin(2\alpha\omega_0 + 2\omega_0 t) + \dots + \left(\sum_{j=1}^n \mu_{nj} x_j\right) \sin(n\alpha\omega_0 + n\omega_0 t) \quad (17)$$

【0033】次に、第2の乗算器2, T5は e_2 と e_4 の乗算を行い、第2のローパスフィルタLPF2, L2は ω_0 の近傍周波数以上の周波数成分をカットし、以

【0029】ここで加算器Bにおいて周波数多重化信号 e_1 に加算される信号(第2のローパスフィルタL2からの出力信号)が(7)式の左辺で定義される微分値 dx_i/dt ($i = 1, 2, \dots, n$) を同様に周波数多重化した周波数多重化微分値信号 de_1/dt であるとする。すなわち、

[数12]

[数13]

は、2つの周波数の異なる信号が乗算されると、両者の差分周波数に相当するビート(唸り)信号が発生するという現象を以下のように2回利用する。

【0031】第1の周波数通倍器1, H1は、信号 e_1 の周波数を α 倍して()、信号 e_2 を出力する。

[数14]

[数15]

した信号Wを一度に発生するもので、

[数16]

て、第1のローパスフィルタLPF1, L1は ω_0 の近傍周波数以上の周波数成分をカットし、以下の信号 e_4 を出力する。

[数17]

下の信号 e_5 を出力する。

[数18]

$$e_5 = x_1 \left(\sum_{j=1}^n \mu_{1j} x_j \right) \sin(\omega_0 t) + x_2 \left(\sum_{j=1}^n \mu_{2j} x_j \right) \sin(2\omega_0 t) + \dots + x_n \left(\sum_{j=1}^n \mu_{nj} x_j \right) \sin(n\omega_0 t)$$

(18)

これは(2)式の右辺の周波数多重化された表現であり、すなわち周波数多重化微分値信号 de_1/dt に相当する。

【0034】この $e_5 (= de_1/dt)$ は、加算器Bにおいて遅延回路Vを経た信号 e_1 と加算され、先に述べた方法によって式(2)の積分が実行される。

【0035】この方法では、図5の回路を一つ用意するだけで、理論的には任意の n に対して(7)式の演算を行うことが出来る。図2、図4、図5の回路は、(7)式の信号 W と個体数 x_i ($i = 1, 2, \dots, n$) の初期値 $x_i |_{t=0}$ の違いによって、 x_i は様々に異なる時間変化パターンを示す。したがって、 $x_i |_{t=0}$ を暗号化(あるいは変調)したいコード、 W を暗号化のための鍵コードと解釈すると、 x_i の時間変化パターンあるいは時刻 T における信号 $x_i |_{t=T}$ は暗号化(変調)された信号として利用できる。また、これとは逆に W を暗号化(変調)したいコード、 $x_i |_{t=0}$ を暗号化(変調)のための鍵コードとして利用しても良い。以上のように、図2、図4、図5の演算回路を用いて暗号化変調(暗号のエンコード)をすることが可能であり、また、これらの演算回路を用いて鍵コードにより元の信号に復調(暗号のデコード)することができる。

【0036】次に、暗号のデコード方法をさらに詳細に説明する。

【0037】図6はデコード用の本装置60であり、すなわち、本装置を暗号化信号の解読装置に使用する際の構成例である。

【0038】相互作用係数 μ_{ij} ($i, j = 1, 2, 3, \dots, n$) の設定値の値と x_i ($i = 2, 3, \dots, n$) の初期値の値によって x_1 は様々な関数になるが、この性質を利用した暗号化は以下の通りである。 n 個のユニットの出力値は常時固定値を出力する一つのユニットを除いて $n-1$ 個が時間的に変化する変数である。ここでは、説明を簡単にするため、そのうちある2つの変数 x_k と x_l が張る平面(図7)において座標 (x_k, x_l) の点 p の軌道を考える。本回路の任意関数発生機能によって、初期値 A から時間発展すると点 p の軌道は非常に多様なパターンで移動する。そこで、ここでは渦巻き状の軌道を描きながら点1に収束し、初期値 B 及び C から時間発展すると点0に収束する相互作用係数 μ_{ij} ($i, j = 1, 2, 3, \dots, n$) となっているものとし、更に収束点は、この1, 0の2点だけであるものとする。そして、送信者は1または0の1ビット情報を安全に送りたいものとする。

【0039】ここで送信者が「1」という情報を安全に

送りたいとき、送信者はA点に相当する信号を送れば良く、「0」という情報を安全に送りたいとき、送信者はB点に相当する信号を送れば良い。受信者は予め保有していた相互作用係数 μ_{ij} をデコード用本装置60に適用して収束点の情報を正しく知ることができる。例えば、送信者が点Aの情報を送った場合、受信者は点Aの情報と相互作用係数 μ_{ij} の情報をデコード用本装置60に入力し、点1が収束点であること、すなわち送られた情報が1であったことを正しく知ることができる。このとき、相互作用係数 μ_{ij} の組み合わせはほぼ無限大にあるため、相互作用係数の真の値を知らない者は、送信者の情報から相互作用係数 μ_{ij} を推定することはほとんど不可能である。そのため、エンコードに使用した本装置によって暗号化されたコードを解読することは極めて困難である。

【0040】次に、そのエンコード用本装置における暗号のエンコード方法をさらに詳細に説明する。

【0041】(キー(相互作用係数 μ_{ij})) を公開しない場合) 点1に相当するコードを暗号化するためには、以下のように行う。

【0042】(1) 初期値をランダムに発生させ、エンコード用本装置で点1に収束したらその初期値を暗号化されたコードとして採用する。もし、点0に収束したらその初期値は廃棄し、再度、初期値をランダムに発生させる。

【0043】(2) 点1に収束する初期値が得られるまで(1)を繰り返す。点0に相当するコードを暗号化する方法も、上記と同じ方法でできる。

【0044】(一部のキーを公開する場合) 通販においてクレジット番号を暗号化して送る際などには、暗号化のためのキーを郵送などで送る必要があり、これは非常に不便である。そのため、公開鍵暗号方式が必要となる。従来の素数を利用した公開鍵暗号方式は大きな数の素因数分解の計算に非常に大きな手間がかかることを利用しているため、計算機の性能向上や効率的な素因数分解アルゴリズムの開発によって安全性が急速に失われるという欠点を有している。以下の方法は、アナログ演算によるシミュレーションを行いながら暗号化を行うため、第三者が解読のために必要な計算量はほぼ無限大であり、極めて高い安全性を有している。本装置を使って、公開鍵暗号方式の暗号化情報伝送を行う手順は以下の通りである。

【0045】(準備) 本装置を構成する n 個のユニット群を図8のように2分してA群とB群に分ける。A群は暗号送信者が保有するエンコード用本装置のユニット群

で、B群は暗号解読者が保有するデコード用本装置のユニット群である。A群とB群のユニット間の相互作用係数 μ_{ij} は多くが0であり、特定の相互作用係数のみが0でないとする。B群の一部のユニット群のみがA群のユニットと0でない相互作用係数で接続しB群へ影響を与えているとし、その群をC群と呼ぶことにする。また同時に、A群の一部のユニット群も0でない相互作用係数でB群のユニットと結合してA群に影響を与え、その群をD群と呼ぶことにする。この場合も、簡単のため2つの収束点を有するように相互作用係数が設定されていると仮定する。ただし、4つのユニットの出力値 x_k, x_l, x_a, x_b が張る4次元空間において2つの収束点をもつものとする。ここで、変数 x_k, x_l を出力するユニットkとユニットlはA群に属し(ただし、出力値が公開されるC群には属さない)、変数 x_a, x_b を出力するユニットaとbはB群に属するとする(ただし、出力値が公開されるD群には属さない)。変数 x_k, x_l の平面における収束点は変数 x_a, x_b の平面における収束点と1対1に対応し、変数 x_a, x_b の平面の収束点から変数 x_k, x_l の平面における収束点を推定できるよう相互作用係数と成長率(固定値パラメータ r_i)が予め設定されているものとする。送信者はA群に関する情報しか所有していないが受信者からのD群に関する情報を動的に受け取ってA群のユニットの計算を行うことができる。すなわち、送信者はA群及びD群に関する情報から座標(x_k, x_l)の動きをシミュレート(計算)し、受信者はB群及びC群に関する情報から座標(x_a, x_b)の動きをシミュレートすることが出来る。

【0046】(キー情報の公開)情報を暗号化して送りたい送信者は、受信者からA群の相互作用係数 μ_{ij} 及び固定値パラメータ r_i の情報を公開キー情報として受け取るとともに、C群の出力値 x_i (IはC群のユニット番号)の情報を平文(暗号化されていない情報)で受け取る。これらの情報を用いて送信者はA群のシミュレーションを実行する。

【0047】(インタラクティブな平文通信を伴う暗号化)C群の出力値はシミュレーションとともに変動するため、送信者はA群のシミュレーションを行うためにC群の出力値を平文でリアルタイムに受け取りながら、A群のシミュレーションを実行する。同時に、受信者は送信者から平文でD群の情報をリアルタイムに受け取りながら、B群のシミュレーションを実行する。すなわち、受信者と送信者はリアルタイムにD群及びC群の情報を平文で交換しながら送信者はA群のシミュレーションを、送信者はB群のシミュレーションをそれぞれ独立して行う。当然の事ながら第三者はこのインタラクティブな通信には参加できない。暗号化して送りたい情報及びA群の初期値は、第三者及び受信者には未知である。受信者はB群のシミュレーションにおける収束点の位置情

報からA群の収束値に関する情報を推定できる。しかし、第三者はA群の初期値及びB群の情報を所有していないためA群あるいはB群のシミュレーションのいずれも実行出来ない。そのため、暗号化された情報の内容を伺い知ることはできない。

【0048】

【発明の効果】本発明の単純な演算要素による任意関数発生回路並びにそれを用いた暗号化変調方法は次のような効果を奏する。

【0049】(1)シミュレーション計算の高速演算装置となる。すなわち、一般化ロトカ-ボルテラ方程式は生態系の個体数の変動や植物の生長といった生物学的な複雑な動態のモデルとして利用されているため、本発明はこれらのシミュレーション計算の高速化に用いることができる。また、本発明の任意関数発生機能によって市況や経済変動など複雑系一般のシミュレータとしても適用可能であり、複雑系の高速シミュレータとして広い用途を有している。

【0050】(2)複雑な波形の発生装置とすることができる。これによって非常に複雑な波形を比較的単純な回路で生成することが出来、回路パラメータの一部を少し変えるだけで波形を様々に変えることができる。パラメータによって周期的あるいは非周期的な波形が生じるため、電子楽器やゲーム機器の音源等に利用できる。微少なパラメータの変化で波形を不規則に変えることができるため、害鳥獣の威嚇や防犯用の警報サイレン等にも適している。

【0051】(3)暗号化装置に適用できる。すなわち、一般化ロトカ-ボルテラ方程式は、パラメータによっては複数の安定点を持ち、初期値の違いによって異なる安定点に収束する。初期値の集合は無限にあり、安定点の数は有限である。そこで、安全に伝送したい情報を安定点の位置情報としてコーディングし、送信者はその安定点に収束する初期値の集合から一つの初期値をランダムに選んで送る。受信者は、同じ値のパラメータの回路を用いて収束点の値を知ることができるが、パラメータの値を知らない第三者には解読することはほとんど不可能である。この方法により、本発明は高速かつ極めて安全性の高い暗号化装置として利用できる。

【0052】(4)パターン認識装置として利用できる。すなわち、前記の暗号化と同じ複数の安定点を持つ回路を使い、初期値ベクトルを入力パターン、収束点を識別結果とすると、予め適切なパラメータを用意しておけば、高速のパターン認識装置として利用できる。なお、適切なパラメータを決定するには既存の非線形最適化アルゴリズムを用いれば良い。

【0053】(5)スペクトラム拡散通信のためのエンコーダ及びデコーダとすることができる。すなわち、複数の安定点を持つ回路は、ある軌道を描いて安定点に到達する。この種の非線形システムは、一般に多少のノイ

ズが混入しても、同じ安定点に到達するロバストネスを有している。また、 n が大きいほど、ノイズに対してロバストにすることができる。そこで、できるだけ n が大きなタイプ2またはタイプ3の回路を想定する。このとき、タイプ2では第3の乗算器3の出力、タイプ3の回路では第2の周波数通倍器2の出力は低周波領域から高周波領域までを含む非常に幅の広いスペクトラムを有する信号になっている。この信号を周波数変調して送信すると、極めて広帯域の送信波にすることができる。受信側では復調した信号を、同じ回路定数を有する回路にこの信号を、送信側と同じ部位（タイプ2では第3の乗算器3の出力、タイプ3の回路では第2の周波数通倍器2の出力）に入力する。混入したノイズが少なければ、送信者とほとんど同じ軌道を描いて正しい安定点に到達し、受信者は正しい情報を得る。復調信号に大きなノイズが含まれていても引き込みによって、送信者と同じ安定点に到達する確率の方が多少大きくなる。この確率は n が大きいほど大きくできる。

【図面の簡単な説明】

【図1】本発明の単純な演算要素による任意関数発生回路の第1実施例のモジュール部のブロック図である。

【図2】本発明の第1実施例の演算回路全体のブロック図である。

【図3】本発明の単純な演算要素による任意関数発生回路の第2実施例のモジュール部のブロック図である。

【図4】本発明の第2実施例の演算回路全体のブロック図である。

【図5】本発明の単純な演算要素による任意関数発生回路の第3実施例の演算回路全体のブロック図である。な

お、その演算回路は1個のモジュールからなる。

【図6】本発明の回路を使用したデコード用装置の説明図である。

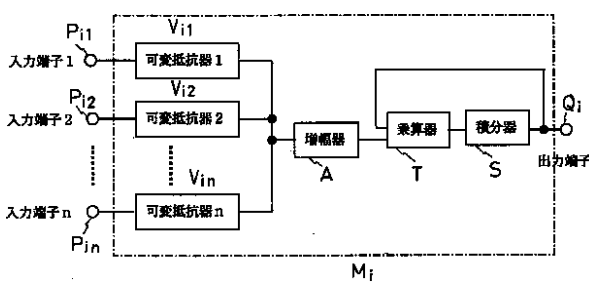
【図7】2つのモジュール出力が張る平面における x_i の時間経過軌道を示す図である。

【図8】本発明を使用した公開鍵時号方式を説明する図である。

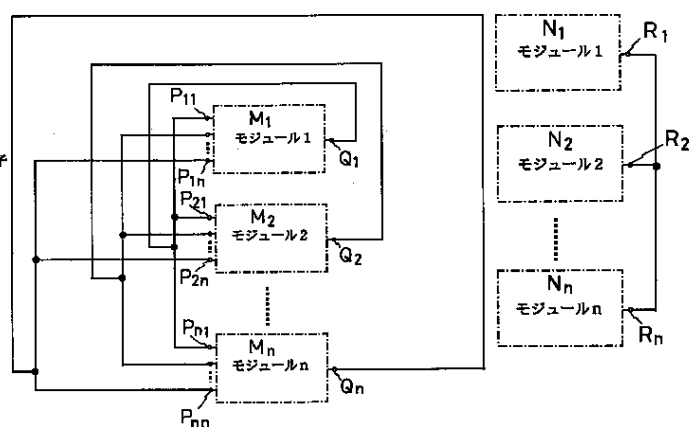
【符号の説明】

- A 増幅器
- B 加算器
- F1, F2 周波数シンセサイザ
- G オシレータ(OSC)
- H1, H2 周波数通倍器
- L, L1, L2 ローパスフィルタ(LPF)
- M_i, N_i 任意のモジュール
- P_{ij} 任意のモジュール M_i の入力端子
- Q_i 任意のモジュール M_i の出力端子
- R_i 任意のモジュール N_i の入出力端子
- r_i 定数値(個体群 i の成長率で各要素間に固定の定数値)
- S, S1 積分器
- T, T1, T2, T3, T4, T5 乗算器
- V_{ij} 任意のモジュール M_i の可変抵抗器
- W, W_i 相互作用係数 μ_{ij} を周波数多重化した電圧値
- x_i システムを構成する要素を代表する個体群 i の個体数(各モジュールの出力信号)
- μ_{ij} 要素間の相互作用定数

【図1】

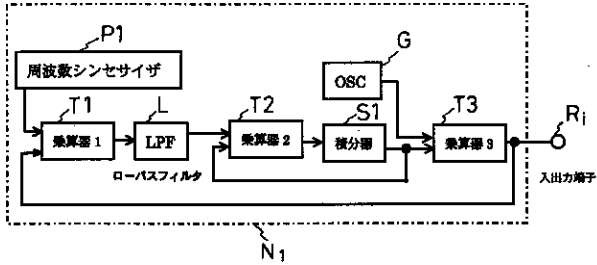


【図2】

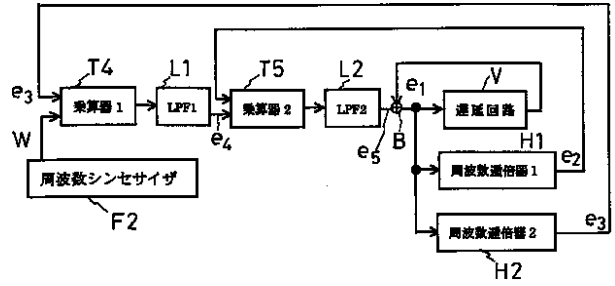


【図4】

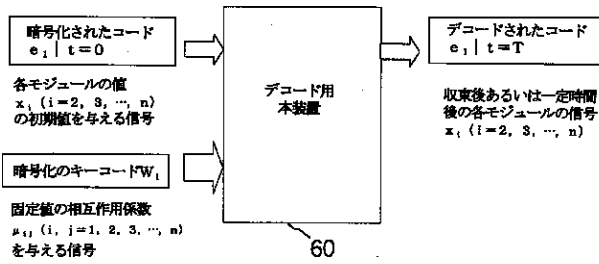
【図3】



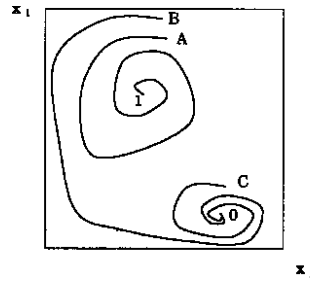
【図5】



【図6】



【図7】



【図8】

