(19)日本国特許庁（ＪＰ）　(12)特　許　公　報（Ｂ２）　(11)特許番号
特許第3507882号
(P3507882)
(45)発行日　平成16年３月15日(2004.3.15)　(24)登録日　平成16年１月９日(2004.1.9)

(51)Int.Cl.[7]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６５０	Ｇ０９Ｃ　1/00	６５０Ｚ
Ｇ０６Ｇ　7/26		Ｇ０６Ｇ　7/26	Ａ
Ｈ０４Ｋ　1/00		Ｈ０４Ｋ　1/00	Ａ

請求項の数７(全 13 頁)

(21)出願番号　特願2000－9224(P2000－9224)
(22)出願日　平成12年１月18日(2000.1.18)
(65)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)
審査請求日　平成12年２月15日(2000.2.15)

(73)特許権者　501203344
独立行政法人農業・生物系特定産業技術研究機構
茨城県つくば市観音台３－１－１
(73)特許権者　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１名)

審査官　青木　重徳

最終頁に続く

(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)【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、下記の一般化ロトカーボルテラ方程式（１）式を演算する

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

（ｘｉ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、μｉｊは前記要素間の相互作用定数、ｒｉ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μｉｊは前記各モジュール内の可変抵

演算回路であって、
［数１］

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μｉｊに固定値ｒｉを担

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

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ｘｉ（ｉ＝１，２，…，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μｉｊ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ロトカー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μｉｊ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ロトカー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、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ｘｉ（ｉ＝１，２，…，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ｘｉと角周波数ωｉ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ｘｉｓｉｎωｉｔを各モジュールから前わせると、前記一般化ロトカー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］

$$\cdots (7)$$

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］

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

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μｉｊを周波数多重化した下記の（９）式に示す電圧値Ｗｉとし、

［数９］

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

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）直流成分のみとし、

［数１０］

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

前記第２の乗算器で、前記ｅＷｉの値と前記積分器の出力ｘｉを乗算し、次段の前記積分器で、その乗算値を積分してｘｉの信号を出力し、次段の第３の乗算器で、そのｘｉ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ｘｉｓｉｎωｉｔ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ロトカー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４】前記周波数シンセサイザによる電圧値Ｗｉ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ロトカー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ｅ４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ｅ５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ｅ１の周波数を逓倍すると共にその出力値ｅ２を第２の乗算器の第２の入力値とする第１の周波数逓倍器と、さらに、前記出力値ｅ１の周波数を逓倍すると共にその出力値ｅ３を第１の乗算器の第２の入力値とする第２の周波数逓倍器とを１個のモジュールに備え、

前記（７）式の信号ｘｉ（ｉ＝１，２，…，ｎ）を振幅の大きさがｘｉの交流信号ｘｉｓｉｎ（ｉωｏ）、（ｉ＝１，２，…，ｎ，ωｏは基本角周波数）とし、前記演算回路の加算器の出力値ｅ１をｘｉ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］

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

この生成された信号ｅ５は（７）式の右辺の周波数多重化微分値信号（ｄｅ１／ｄｔ）に相当し、この信号ｅ５は前記加算器において信号ｅ１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ロトカー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、初期値ｅ１｜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。

【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気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マブルに発生でき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、一般化ロトカー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］

この周波数多重化信号ｅ１は基本周波数ωｏ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の周波数逓倍器は信号ｅ１の周波数をα倍（ｎ≪α）して信号ｅ２を出力させ、前記第２の周波数逓倍器は信号ｅ１の周波数をβ倍（α≪β）して信号ｅ３を出力させ、前記周波数シンセサイザは相互作用係数μｉｊ（ｉ＝１，２，…，ｎ；ｊ＝１，２，…，ｎ）をそれぞれ周波数多重化した信号Wを一度に生成させて出力させ、前記第１の乗算器は、信号ｅ３とWの乗算を行わせ、第１のローパスフィルタでβωｏ近傍周波数以上の成分をカットし、信号ｅ４を出力させ、前記第２の乗算器は信号ｅ２とｅ４の乗算を行わせ、第２のローパスフィルタでαωｏ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ｅ５を出力させ、

［数１８］

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

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

ここで、ｘｉ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）、μｉｊは要素間の相互作用定数、ｒｉ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μｉｊを変えることで、様々に変化するｘｉ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、一般化ロトカー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ーボルテラ方程式（１）式を演算する演算回路であって、

［数１］

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

（ｘｉ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、μｉｊは前記要素間の相互作用定数、ｒｉ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μｉｊ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μｉｊに固定値ｒｉを担わせると、前記一般化ロトカー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］

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

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ｘｉ（ｉ＝１，２，…，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μｉｊ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ロトカー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μｉｊ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。

【０００８】また、請求項１又は２記載の（７）式に変形した一般化ロトカー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ｘｉ（ｉ＝１，２，…，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ｘｉと角周波数ωｉ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ｘｉｓｉｎωｉｔ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］

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

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μｉｊを周波数多重化した下記の（９）式に示す電圧値Ｗｉとし、

［数９］

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

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）直流成分のみとし、

［数１０］

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

前記第２の乗算器で、前記ｅＷｉの値と前記積分器の出力ｘｉを乗算し、次段の前記積分器で、その乗算値を積分してｘｉの信号を出力し、次段の第３の乗算器で、そのｘｉ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ｘｉｓｉｎωｉｔ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ロトカー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Ｗｉ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。

【００１０】また、請求項１又は２記載の（７）式に変形した一般化ロトカー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ｅ４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ｅ５を入力値の１つとして入力する加算器と、その出力値ｅ１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ｅ１の周波数を逓倍すると共にその出力値ｅ２を第２の乗算器の第２の入力値とする第１の周波数逓倍器と、さらに、前記出力値ｅ１の周波数を逓倍すると共にその出力値ｅ３を第１の乗算器の第２の入力値とする第２の周波数逓倍器とを１個のモジュールに備え、前記（７）式の信号ｘｉ（ｉ＝１，２，…，ｎ）を振幅の大きさがｘｉの交流信号ｘｉｓｉｎ（ｉω０）、（ｉ＝１，２，…，ｎ，ω０は基本角周波数）とし、前記演算回路の加算器の出力値ｅ１をｘｉ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］

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

この周波数多重化信号ｅ１は基本周波数ω０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の周波数逓倍器は信号ｅ１の周波数をα倍（ｎ≪α）して信号ｅ２を出力させ、前記第２の周波数逓倍器は信号ｅ１の周波数をβ倍（α≪β）して信号ｅ３を出力させ、前記周波数シンセサイザは相互作用係数μｉｊ（ｉ＝１，２，…，ｎ；ｊ＝１，２，…，ｎ）をそれぞれ周波数多重化した信号Ｗを一度に生成させて出力させ、前記第１の乗算器は、信号ｅ３とＷの乗算を行わせ、第１のローパスフィルタでβω０近傍周波数以上の成分をカットし、信号ｅ４を出力させ、前記第２の乗算器は信号ｅ２とｅ４の乗算を行わせ、第２のローパスフィルタでαω０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ｅ５を出力させ、

［数１８］

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

この生成された信号ｅ５は（７）式の右辺の周波数多重化微分値信号（ｄｅ１／ｄｔ）に相当し、この信号ｅ５は前記加算器において信号ｅ１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ロトカー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、初期値ｅ１｜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。

【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。

【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は一般化ロトカー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、Ｍｉ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Ｐｉｊと１個の出力端子Ｑｉを有する。第１のモジュールＭ１の出力端子Ｑ１と各モジュールの第１の入力端子Ｐ１１，Ｐ２１，…，Ｐｎ１に接続する第１の接続線と、第２のモジュールＭ２の出力端子Ｑ２と各モジュールの第２の入力端子Ｐ１２，Ｐ２２，…，Ｐｎ２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Ｑｎと各モジュールの第ｎ番目の入力端子Ｐ１ｎ，Ｐ２ｎ，…，Ｐｎｎ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Ｐｉｊとそれぞれ接続するｎ個の可変抵抗器群Ｖｉｊ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。一般化ロトカー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Ｍｉ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、μｉｊは各モジュール内の可変抵抗器Ｖｉｊの値に相当し、ｒｉ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]

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

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

[数３]

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

ただし、

[数４]

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

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ｒｉ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μｉ１に担わせて、μｉ１がｒｉの値であると仮定すると、

[数５]

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

ただし、仮定により、

[数６]

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

である。括弧内の項μｉ１ｘ１を（６）式右辺のΣの中に戻して、

[数７]

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

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Ｖｉｊ（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ｘ１（ｉ＝２，３，…，ｎ）の値が得られる。

【００１５】ｘ１（ｉ＝２，３，…，ｎ）の値の時間変化パターンはμｉｊの設定値（図１の可変抵抗器Ｖｉｊ（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Ｍｉ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Ｖｉｊの値μｉｊ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Ｖｉｊの値μｉｊ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は一般化ロトカー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部を図３に示す。ここで、Ｎｉ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Ｒｉを有する。各モジュールの入出力端子Ｒｉは１本の信号バス結線に接続される。一方、各モジュールＮｉは周波数シンセサイザＦ１の出力値と前記入出力端子Ｒｉ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Ｒｉ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Ｎｉの入出力端子Ｒｉ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Ｎｉの出力値をｘｉｓｉｎωｉｔとすると、各モジュールＮｉ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]

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

である。相互作用係数μｉｊについても、同様に交流信号で表現する。すなわち、ｘ１への相互作用定数を、

[数９]

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

の電圧として供給する。これは各モジュールＮｉの内部または外部に設けた周波数シンセサイザＦ１で個別に生成する。なお、このシンセサイザＦ１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Ｎｉ内ではまず第１の乗算器１，Ｔ１によってｅとＷｉ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ｓｉｎωｉｔ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]

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

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２，Ｔ２は、この信号とｘｉ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Ｓ１によってこの信号を積分し、ｘｉの信号が得られる。次の第３の乗算器３，Ｔ３はｘｉの信号とオシレータ（ＯＳＣ）Ｇで生成した搬送波ｓｉｎωｉｔの信号を乗算し、ｘｉｓｉｎωｉｔの信号を生成する。この信号は、第１の乗算器１，Ｔ１へ入力させると同時に、入出力端子Ｒｉを通じて外部へ出力される。

【００２０】このようなモジュールＮｉ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ー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－Ｆｏｕｌｅｔｈｒｅｔ－，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、一般化ロトカーボルテラ方程式を計算する演算回路の内部に必要となるモジュール間の膨大な結線数（タイプ１ではｎ２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の一般化ロトカーボルテラ方程式の

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）の一般化ロトカーボルテラ方程式の演算を行うことが可能となる。

【００２４】そこで、本発明の第３実施例を図５に示す。図５は一般化ロトカー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Ｆ２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Ｔ４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）Ｌ１と、その出力値ｅ４を入力値の１つとして入力する第２の乗算器Ｔ５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Ｌ２と、その出力値ｅ５を入力値の１つとして入力する加算器Ｂと、その出力値ｅ１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ｅ１の周波数を逓倍すると共にその出力値ｅ２を第２の乗算器Ｔ５の第２の入力値とする第１の周波数逓倍器Ｈ１と、さらに、前記出力値ｅ１の周波数を逓倍すると共にその出力値ｅ３を第１の乗算器Ｔ４の第２の入力値とする第２の周波数逓倍器Ｈ２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ｘｉ（ｉ＝１，２，…，ｎ）を振幅の大きさがｘｉの交流信号ｘｉｓｉｎ（ｉω０）（ｉ＝１，２，…，ｎ）で表現する。ここで、ω０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、ｘｉをω０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]

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

である。図５中では、この周波数多重化信号ｅ１は、遅延回路Ｖの入力値とする。

【００２８】周波数多重化信号ｅ１は遅延回路Ｖで基本周波数ω０の周期（２π／ω０）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ｅ１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。

[数１２]

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

である。加算器Ｂではｅ１とｄｅ１／ｄｔが加算され、

[数１３]

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

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ｄｅ１／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の周波数逓倍器１，Ｈ１は、信号ｅ１の周波数をα倍して（ｎ≪α）、信号ｅ２を出力する。

[数１４]

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

同様に第１の周波数逓倍器２，Ｈ２は、信号ｅ１の周波数をβ倍して（α≪β）、信号ｅ３を出力する。

[数１５]

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

【００２９】ここで加算器Ｂにおいて周波数多重化信号ｅ１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ｄｘｉ／ｄｔ（ｉ＝１，２，…，ｎ）を同様に周波数多重化した周波数多重化微分値信号ｄｅ１／ｄｔであるとする。すなわち、

周波数シンセサイザＦ２は相互作用係数μｉｊ（ｉ＝１，２，…，ｎ；ｊ＝１，２，…，ｎ）を周波数多重化した信号Ｗを一度に発生するもので、

[数１６]

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

を出力する。

【００３２】まず、第１の乗算器１，Ｔ４はｅ３とＷの乗算を行い、ｅ３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。この信号に対して、第１のローパスフィルタＬＰＦ１，Ｌ１はβω０の近傍周波数以上の周波数成分をカットし、以下の信号ｅ４を出力する。

[数１７]

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

【００３３】次に、第２の乗算器２，Ｔ５はｅ２とｅ４の乗算を行い、第２のローパスフィルタＬＰＦ２，Ｌ２はαω０の近傍周波数以上の周波数成分をカットし、以下の信号ｅ５を出力する。

[数１８]

$$e_5=x_1\left(\sum_{j=1}^{n}\mu_{1j}x_j\right)\sin(\omega_0)+x_2\left(\sum_{j=1}^{n}\mu_{2j}x_j\right)\sin(2\omega_0)+\cdots+x_n\left(\sum_{j=1}^{n}\mu_{nj}x_j\right)\sin(n\omega_0)$$
（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ｄｅ１／ｄｔに相当する。

【００３４】このｅ５（＝ｄｅ１／ｄｔ）は、加算器Ｂにおいて遅延回路Ｖを経た信号ｅ１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ｘｉ（ｉ＝１，２，…，ｎ）の初期値ｘｉ｜ｔ＝０の違いによって、ｘｉは様々に異なる時間変化パターンを示す。したがって、ｘｉ｜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、ｘｉの時間変化パターンあるいは時刻Ｔにおける信号ｘｉ｜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、ｘｉ｜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μｉｊ（ｉ，ｊ＝１，２，３，…，ｎ）の設定値の値とｘｉ（ｉ＝２，３，…，ｎ）の初期値の値によってｘｉ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ｘｋとｘｌが張る平面平面（図７）において座標（ｘｋ，ｘｌ）の点ｐの軌道を考える。本回路の任意関数発生の機能によって、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μｉｊ（ｉ，ｊ＝１，２，３，…，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μｉｊ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μｉｊの情報をデコード用本装置６

０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μｉｊ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μｉｊ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μｉｊ）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３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μｉｊ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でない相互作用計数でＢ群のユニットと結合してＡ群に影響を与えるとし、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ｘｋ，ｘｌ，ｘａ，ｘｂ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ｘｋ，ｘｌ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ｘａ，ｘｂ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ｘｋ，ｘｌの平面における収束点は変数ｘａ，ｘｂの平面における収束点と１対１に対応し、変数ｘａ，ｘｂの平面の収束点から変数ｘｋ，ｘｌ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ｒｉ）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（ｘｋ，ｘｌ）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（ｘａ，ｘｂ）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μｉｊ及び固定値パラメータｒｉ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ｘｉ（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３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の周波数逓倍器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の周波数逓倍器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　　周波数逓倍器

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

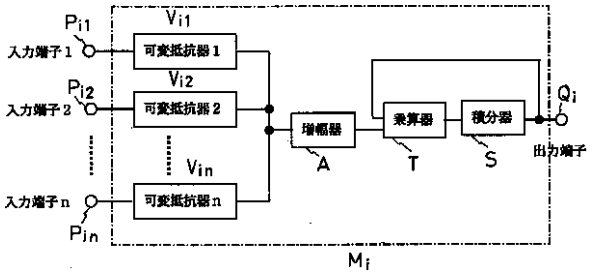
V_{ij}　　任意のモジュールM_iの可変抵抗器

Ｗ，W_i　　相互作用係数μ_{ij}を周波数多重化した電圧値

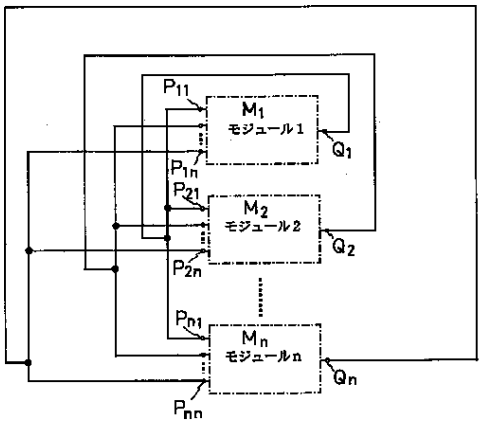
x_i　　システムを構成する要素を代表する個体群ｉの個体数（各モジュールの出力信号）

μ_{ij}　　要素間の相互作用定数

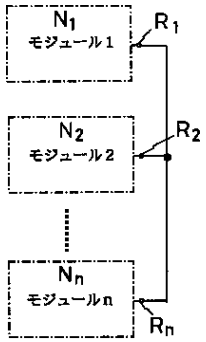
【図１】



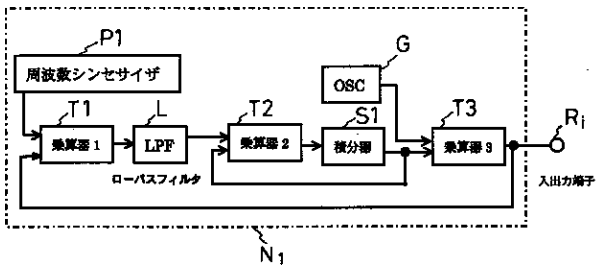
【図２】



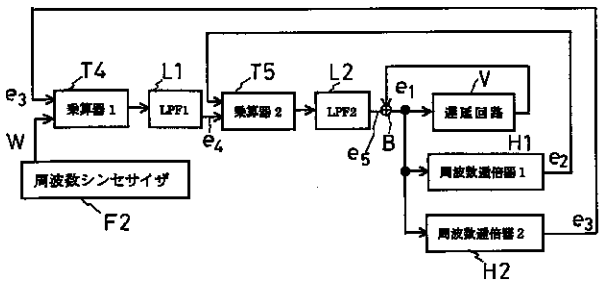
【図４】



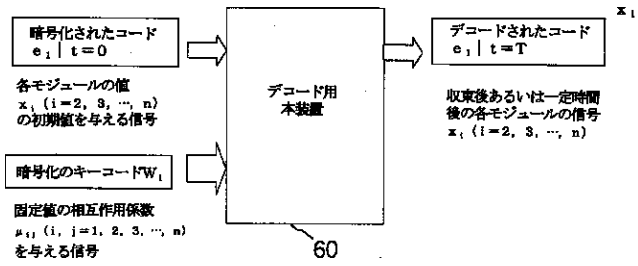
【図３】



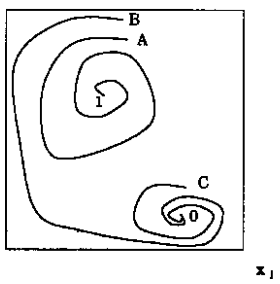
【図５】



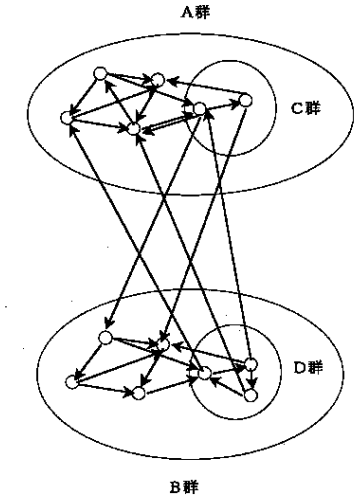
【図６】



【図７】



【図８】



フロントページの続き

(56)参考文献　大黒一弘，“ボルテラの生態系モデルと電子工学への応用”，電子通信学会誌，日本，1979年　９月，Ｖｏｌ．61，Ｎｏ．７，ｐ．750－758
神谷泰史，金沢雄亮，浅井哲也，雨宮好仁，“サブスレッショルド領域で動作するアナログＣＭＯＳ回路によるカオス発生器”，2003年電子情報通信学会総合大会講演論文集，日本，2003年　３月３日，Ｖｏｌ．2003，基礎・境界，ｐ．１

(58)調査した分野(Int.Cl.7，ＤＢ名)
G09C　1/00　650
G06G　7/26
H04K　1/00