(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 523 571**

(51) Int. CI.:

G06F 7/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.03.2011 E 11720313 (3)**

(97) Fecha y número de publicación de la concesión europea: **03.09.2014 EP 2553567**

(54) Título: **Generador de secuencias caóticas y sistema de generación correspondiente**

(30) Prioridad:

29.03.2010 FR 1052288

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.11.2014

(73) Titular/es:

UNIVERSITÉ DE NANTES (100.0%)
1, quai de Tourville
44000 Nantes , FR

(72) Inventor/es:

EL ASSAD, SAFWAN y
NOURA, HASSAN

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Generador de secuencias caóticas y sistema de generación correspondiente.

La presente invención se refiere a un generador de secuencias caóticas de valores enteros.

También se refiere a un sistema de generación de secuencias caóticas, a un sistema de encriptado, a un procedimiento de medición de la longitud de la órbita de una secuencia caótica discreta y a un programa informático correspondientes.

Más particularmente, la invención se refiere al campo de la seguridad de los datos compartidos, transmitidos y almacenados en redes de transmisión de información.

La transferencia de datos confidenciales (documentos de empresa, informes médicos, resultados de investigación, información personal de tipo fotos y vídeos, etc.) en un entorno abierto utilizando los canales habituales de comunicación (cables, Internet, móviles por radio, satélites,...) se debe realizar con una seguridad máxima y a una velocidad suficiente. Con este fin, los criptosistemas basados en las señales caóticas son adecuados para alcanzar los objetivos mencionados. Un elemento determinante en cualquier criptosistema basado en el caos es el generador de las secuencias caóticas, que sirve para la generación de las claves secretas y para el proceso de cifrado/descifrado de los datos en las operaciones de sustitución y de permutación. La confidencialidad de los datos dependerá, entre otras cosas, del grado del caos (es decir de la aleatoriedad) de las secuencias producidas por el generador de secuencias caóticas utilizado.

No obstante, las señales caóticas no se han utilizado mucho en el estado de la técnica de los sistemas de encriptado, debido a su periodicidad según unos ciclos de longitud finita bastante reducida.

El documento "Design and Analyses of Efficient Chaotic Generators for Crypto-Systems" de Safwan El Assad *et al.* en Advances in Electrical and Electronics Engineering IAENG Special Edition of the World Congress on Engineering and Computer Sciences 2008, Vol. 1, páginas 3 a 12, describe un generador de secuencias caóticas de valores enteros destinados en particular a formar unas claves de encriptado de información, comprendiendo dicho generador por lo menos dos filtros recursivos discretos de orden por lo menos igual a 1 que generan a la salida una secuencia caótica de valores enteros, comprendiendo cada filtro recursivo unos medios de puesta en práctica de una función no lineal, conectados a través de una puerta O exclusiva a unos medios de generación de una secuencia de perturbación.

En el documento mencionado anteriormente, los dos filtros recursivos están montados en serie, lo cual provoca tiempos de cálculo prolongados para la generación de las secuencias caóticas.

El objetivo de la invención es solucionar este problema.

Con este fin, la invención tiene por objeto un generador de secuencias caóticas $e_u(n)$, siendo n un entero estrictamente positivo, de valores enteros representados en un número de bits de cuantificación N determinado, destinados en particular a formar unas claves de encriptado de información, comprendiendo dicho generador por lo menos dos filtros recursivos discretos de orden por lo menos igual a 1 que generan a la salida una secuencia caótica de valores enteros, comprendiendo cada filtro recursivo unos medios de puesta en práctica de una función no lineal *F,* conectados a través de una puerta O exclusiva a unos medios de generación de una secuencia de perturbación $Q(n)$ de valores enteros representados en un número de bits de cuantificación k determinado, caracterizado por que los dos filtros están montados en paralelo, siendo la secuencia caótica $e_u(n)$ de salida del generador igual a una O exclusiva de las secuencias caóticas de salida de los filtros recursivos, y por que los medios de puesta en práctica de la función no lineal comprenden un mapa caótico.

Según otros aspectos de la invención, el generador de secuencias caóticas comprende una o varias de las características siguientes:

- los medios de generación de una secuencia de perturbación en cada filtro comprenden un registro de desfase de reacción de longitud máxima que utiliza un polinomio primitivo de grado k,
- el orden de cada filtro recursivo es inferior o igual a 3,
- los medios de puesta en práctica de la función no lineal comprenden una mapa caótico lineal por tramos PWLCM,
- las secuencias $e_{uj}(n)$ de salida de cada filtro recursivo j = 1,2 vienen dadas por la relación

$$e_{uj}(n) = F\left(X_j(n-1), P\right) \oplus Q(n)$$

en la que

$$F\left(X_j(n-1),P\right)=\begin{cases}\left\lfloor \dfrac{2^N \times X_j(n-1)}{P} \right\rfloor & 0 \le X_j(n-1) \le P \\ \left\lfloor \dfrac{2^N \times \left[X_j(n-1)-P\right]}{2^{N-1}-P} \right\rfloor & P \le X_j(n-1) \le 2^{N-1} \\ \left\lfloor \dfrac{2^N \times \left[2^N-1-X_j(n-1)-P\right]}{2^{N-1}-P} \right\rfloor & 2^{N-1} \le X_j(n-1) \le 2^N - P \\ \left\lfloor \dfrac{2^N \times \left[2^N-1-X_j(n-1)\right]}{P} \right\rfloor & 2^N - P \le X_j(n-1) \le 2^N \end{cases}$$

siendo

$$X_j(n-1)=\mathrm{mod}\left[k_{uj}(n-1)+c_{j1}\times e_{uj}(n-1)+c_{j2}\times e_{uj}(n-2)+c_{j3}\times e_{uj}(n-3),2^N\right]$$

donde

- P es un parámetro de control cuyo valor es inferior a 2^{N-1},
- $k_{uj}(n)$ es la secuencia de entrada del filtro recursivo j,
- c_{j1}, c_{j2}, c_{j3} representan los coeficientes del filtro recursivo j,
- la operación $\lfloor X \rfloor$ consiste en devolver el entero más grande menor o igual a X,
- la operación mod(X,2^N) consiste en efectuar el módulo 2^N de X, y
- los medios de puesta en práctica de la función no lineal comprenden un mapa caótico de tipo "SKEW-Tent".

La invención se refiere asimismo a un sistema de generación de secuencias caóticas que comprende por lo menos un conjunto de 14 generadores de secuencias caóticas según la invención, estando dichos generadores distribuidos en dos grupos de 7 generadores cada uno, caracterizado por que comprende:

- un primer multiplexor analógico que permite seleccionar la salida de un primer generador de entre los generadores del primer grupo,
- un segundo multiplexor analógico que permite seleccionar la salida de un segundo generador de entre los generadores del segundo grupo,

estando las salidas de los dos multiplexores conectadas a una puerta O exclusiva que genera a la salida la secuencia caótica, y

- unos medios de direccionamiento de los multiplexores que comprenden un registro de desfase de reacción conectado a un reloj cuyo periodo es función de la longitud de la secuencia caótica.

Según otros aspectos de la invención, el sistema de generación de secuencias caóticas comprende una o varias de las características siguientes:

- comprende dos conjuntos montados en paralelo de 14 generadores de secuencias caóticas cada uno, siendo la secuencia caótica generada a la salida del sistema de generación igual a una O exclusiva de las secuencias caóticas generadas en la salidas de los dos conjuntos de 14 generadores,
- los polinomios primitivos de los registros de desfase de reacción del primer conjunto de generadores son diferentes de los polinomios primitivos de los registros de desfase de reacción del segundo conjunto de generadores,
- comprende unos medios de eliminación de una cantidad determinada de muestras de las secuencias caóticas generadas por el sistema, y
- comprende unos medios de cuantificación de las secuencias caóticas generadas.

La invención también se refiere a un sistema de encriptado, caracterizado por que comprende un sistema de

generación de secuencias caóticas de este tipo, siendo dicho sistema de generación de secuencias caóticas utilizado para la generación de claves secretas y en los procedimientos de cifrado/descifrado del sistema de encriptado.

La invención también se refiere a un procedimiento de medición de la longitud de la órbita, formada por un transitorio y por un ciclo, de una secuencia caótica discreta de muestras, siendo la longitud de dicha órbita igual a la suma de las longitudes del transitorio y del ciclo de la secuencia, caracterizado por que comprende las etapas de:

- generación de una subsecuencia inicial que consiste en un número N_t determinado de muestras de la secuencia caótica;
- únicamente si la subsecuencia no comprende ningún ciclo, generación iterativa de una subsecuencia siguiente que consiste en un número N'_t determinado de muestras de la secuencia caótica hasta que la subsecuencia global formada por todas las subsecuencias generadas comprenda un ciclo, y
- cálculo de la longitud de la órbita de la secuencia caótica a partir de las longitudes del transitorio y del ciclo de la subsecuencia global.

La invención se refiere asimismo a un procedimiento de medición del valor de la órbita de un filtro recursivo discreto del generador de secuencias caóticas según la invención, caracterizado por que comprende las etapas del procedimiento de medición mencionado anteriormente.

La invención se refiere, por último, a un programa informático que comprende instrucciones de código que, cuando se ejecuta este programa en un ordenador, permiten la puesta en práctica de las etapas de un procedimiento de medición de este tipo.

Así, la invención permite paliar los inconvenientes del generador de secuencias caóticas del documento mencionado anteriormente proponiendo un montaje en paralelo de los dos filtros recursivos del generador.

Asimismo, el sistema de generación de secuencias caóticas según la invención que comprende una pluralidad de generadores de secuencias caóticas permite generar unas señales caóticas discretas de periodos muy largos, pudiendo alcanzar varios siglos. Esto es muy importante para la seguridad de los datos, ya que con unas secuencias caóticas no repetitivas de este tipo, es posible generar unas claves de encriptado de gran tamaño.

Además, el procedimiento de medición de la longitud de la órbita de una secuencia caótica según la invención permite medir con precisión la longitud de la órbita de cualquier secuencia caótica de manera rápida y eficaz.

A continuación se describirán unos modos de realización de la invención de manera más precisa, pero no limitativa, en referencia a los dibujos adjuntos, en los que:

- la figura 1 es un esquema sinóptico que ilustra la estructura y el funcionamiento de un generador de secuencias caóticas según la invención,
- la figura 2 es un esquema sinóptico que ilustra el principio de la perturbación de secuencias caóticas,
- la figura 3 es un esquema sinóptico que ilustra la estructura y el funcionamiento de un sistema de generación de secuencias caóticas según la invención,
- la figura 4 es un organigrama que ilustra el funcionamiento del procedimiento de medición de la longitud de la órbita de una secuencia caótica según la invención, y
- la figura 5 es un organigrama que ilustra el funcionamiento del procedimiento de medición de la longitud de la órbita de una secuencia caótica generada por un filtro recursivo de orden 3.

La figura 1 ilustra un generador 2 de secuencias caóticas $e_u(n)$, siendo n un entero estrictamente positivo, de valores enteros representados en un número de bits de cuantificación N determinado.

La secuencia caótica $e_u(n)$ generada está destinada en particular a formar unas claves de encriptado de información y a ser utilizada en los procesos de cifrado/descifrado en las operaciones de sustitución y de permutación para la seguridad de los datos compartidos, transmitidos y almacenados.

El generador 2 comprende por lo menos dos filtros recursivos discretos 4 y 6 de orden por lo menos igual a 1 y preferentemente igual a 3 como en la figura 1. No obstante, es posible utilizar filtros recursivos 4 y 6 de orden 1 o 2.

El primer filtro recursivo 4 genera a la salida una secuencia caótica $e_{u1}(n)$ de valores enteros.

El segundo filtro recursivo 6 genera a la salida una secuencia caótica $e_{u2}(n)$ de valores enteros.

Los filtros recursivos 4, 6 comprenden unos medios de puesta en práctica de una función no lineal F 8, 10 respectivamente conectados a través de una puerta O exclusiva 12, 14 respectivamente a unos medios de generación de una secuencia de perturbación *Q(n)* 16, 18 respectivamente.

Los medios de generación de una secuencia de perturbación 16, 18 en los filtros recursivos 4, 6 respectivamente comprenden un registro de desfase de reacción de longitud máxima m-LFSR ("Maximal-Length Linear Feedback Shift Register") 16, 18 respectivamente.

El papel de la secuencia de perturbación se describirá con más detalle con referencia a la figura 2.

Según la invención, los dos filtros recursivos 4 y 6 están montados en paralelo de manera que la secuencia caótica $e_u(n)$ a la salida del generador 2 es igual a una O exclusiva 20 de las secuencias caóticas $e_{u1}(n)$ y $e_{u2}(n)$ a la salida de los filtros recursivos 4, 6.

Los dos filtros recursivos 4, 6 comprenden entradas libres $k_{u1}(n)$ y $k_{u2}(n)$ respectivamente.

En el caso de filtros recursivos 4, 6 de orden 3, como se presentan en la figura 1, cada uno de los filtros 4, 6 comprende tres retardos 22, 24, 26 y 28, 30, 32 respectivamente, tres operadores multiplicadores de ganancia c_{11}, c_{12} y c_{13} para el primer filtro recursivo 4 y c_{21}, c_{22}, c_{23} para el segundo filtro recursivo 6 y tres sumadores módulo 2^N 34, 36, 38 y 40, 42, 44 respectivamente.

Los medios de puesta en práctica de una función no lineal 8, 10 comprenden unos circuitos que realizan la función xlogx o la función xexp[cos (x)] o bien un mapa de Chebyshev o un mapa SKEW-Tent o incluso un mapa caótico lineal por tramos PWLCM ("Piecewise Linear Chaotic Map").

Las simulaciones efectuadas por los inventores indican que el mapa PWLCM es el que da los mejores resultados en cuando a eficacia con respecto al criptoanálisis y a la simplicidad de realización.

En el modo de realización de la figura 1 que utiliza un mapa PWLCM, la salida $e_u(n)$ del generador 2 verifica la relación $e_u(n) = e_{u1}(n) \oplus e_{u2}(n)$ con

$$\underset{j=1,2}{e_{uj}(n)} = F\left[X_j(n-1), P\right] \oplus Q(n)$$

en la que:

$$F\left[\underset{j=1,2}{X_j(n-1)}, P\right] = \begin{cases} \left\lfloor \dfrac{2^N \times X_j(n-1)}{P} \right\rfloor & 0 \le X_j(n-1) \le P \\ \left\lfloor \dfrac{2^N \times \left[X_j(n-1) - P\right]}{2^{N-1} - P} \right\rfloor & P \le X_j(n-1) \le 2^{N-1} \\ \left\lfloor \dfrac{2^N \times \left[2^N - 1 - X_j(n-1) - P\right]}{2^{N-1} - P} \right\rfloor & 2^{N-1} \le X_j(n-1) \le 2^N - P \\ \left\lfloor \dfrac{2^N \times \left[2^N - 1 - X_j(n-1)\right]}{P} \right\rfloor & 2^N - P \le X_j(n-1) \le 2^N \end{cases}$$

siendo:

$$\underset{j=1,2}{X_j(n-1)} = \mathrm{mod}\left[k_{uj}(n-1) + c_{j1} \times e_{uj}(n-1) + c_{j2} \times e_{uj}(n-2) + c_{j3} \times e_{uj}(n-3), 2^N\right]$$

donde P es un parámetro de control que verifica $0 < P < 2^{N-1}$,

- $k_{uj}(n)$ es la secuencia de entrada del filtro recursivo *j*,

- c_{j1}, c_{j2}, c_{j3} representan los coeficientes del filtro recursivo j,

la operación $\lfloor X \rfloor$ devuelve el entero más grande menor o igual a x (función "Floor") y la operación mod (X,2^N) consiste en efectuar el módulo 2^N de X.

El generador 2 produce unos valores caóticos enteros y no reales. Esto es primordial, ya que en este caso, los valores generados en la emisión y en la recepción dependen solamente del número N seleccionado y no de la precisión de los medios de cálculo utilizados. De lo contrario, la clave secreta puede ser interpretada de manera diferente en la recepción con respecto a la emisión y vista la extremada sensibilidad del sistema con la clave secreta, los valores generados en la emisión y en la recepción corren el riesgo de ser diferentes. No obstante, se debe observar que la operación de discretización degrada las dinámicas caóticas del mapa caótico inicial (antes de la discretización ya que: $X(n) \neq 2^N \times x(n)$ donde $x(n) \in \mathbf{R}\{0,1\}$ donde $\mathbf{R}\{0,1\}$ designa el conjunto de números reales comprendidos entre 0 y 1.

La cascada de dos filtros recursivos en paralelo permite aumentar la longitud del ciclo con respecto a la utilización de un solo filtro. En efecto, si se designa mediante l_1 la longitud del ciclo del primer filtro 4 y mediante l_2 la longitud del ciclo del segundo filtro 6, entonces la longitud l del ciclo de generador compuesto por dos filtros recursivos en paralelo es el mínimo común múltiplo (mcm) de l_1 y de l_2, es decir:

$$l = \text{mcm}\ (l_1, l_2),$$

siendo $1 \leq l_1 \leq (2^N-1)^3$, $1 \leq l_2 \leq (2^N-1)^3$.

Si el máximo común divisor (mcd) de l_1 y l_2 es igual a la unidad, es decir:

$$\text{mcd}\ (l_1, l_2) = 1$$

entonces:

$$l = l_1 \times l_2$$

Además, el generador 2 integra una técnica de perturbación de la órbita caótica, lo cual permite no solamente resolver el problema de la degradación de las dinámicas caóticas, sino también aumentar considerablemente la longitud de los ciclos y garantizar una seguridad máxima.

La figura 2 ilustra el principio de la perturbación de una secuencia caótica generada por un generador caótico estándar, tal como un mapa PWLCM 46 que forma parte de un filtro recursivo 47 de orden 1.

La secuencia de perturbación $Q(n)$ generada con la ayuda de un registro de desfase de reacción 48 de longitud máxima tiene la función de perturbar la órbita caótica del generador 46 permitiéndole así acceder a una nueva órbita.

El registro de desfase de reacción 48 utiliza un polinomio primitivo de grado k, de manera que la secuencia de perturbación $Q(n)$ generada está representada en k bits.

El registro 48 se caracteriza por una buena función de autocorrelación, una distribución casi uniforme, un ciclo de longitud máxima igual a 2^k-1 y una fácil implementación en software o hardware.

Partiendo de la ecuación del generador 46:

$$X(n)=F[X(n-1)] \in 2^N-1\ n=1,2,....$$

donde cada valor $X(n)$ está representado por N bits:

$$X(n) = x_{N-1}(n)x_{N-2}(n)\ldots x_i(n) \ldots x_{0(n)} \quad x_i(n) \in A_b = [0,1]$$
$$i = 0, 1, \ldots N-1.$$

Por otro lado, indicando como Δ el reloj del registro 48, la perturbación sólo se aplica a la secuencia caótica generada por el generador 46 si n = m x Δ, siendo m un entero, es decir para n = 0 y todas las Δ iteraciones. El reloj Δ del registro 48 representa por lo tanto el ciclo mínimo del filtro recursivo 47 sin perturbación.

En efecto, si:

$$e_{nj}(n) = x_{j,N-1}(n)x_{j,N-2}(n)....x_{j,i}(n)....x_{j,0}(n) \quad x_{j,i}(n) \in A_b = [0,1]$$
$$i = 0,1,...N-1; \quad j = 1,2$$

entonces:

$$x_{j,i}(n) = \begin{cases} F[x_{j,i}(n-1), P] & k \le i \le N-1 \\ F[x_{j,i}(n-1), P] \oplus Q_i(n) & 0 \le i \le k-1 \end{cases}$$

donde $F[x_{j,i}(n\text{-}1)]$ representa el i-ésimo bit de $F[X_j(n\text{-}1), P]$ y $Q_i(n)$ representa el i-ésimo bit de la secuencia de perturbación, de tal manera que:

$$Q_{k-1}^{+}(n) = Q_k(n) = g_0 Q_0(n) \oplus g_1 Q_1(n) \oplus ... g_{k-1} Q_{k-1}(n)$$

donde n=0,1,2,..., $[g_0, g_1,..., g_k\text{-}1]$ son los coeficientes del polinomio primitivo del registro de desfase 48 y $[Q_0, Q_1,..., Q_k\text{-}1]$ representa el valor inicial no nulo del registro 48. Se observará que la secuencia perturbadora se aplica en los k bits de bajo peso de F[X(n-1)].

Si $n \neq m \times \Delta$, m = 0, 1, 2,..., la salida del generador de secuencias caóticas no está perturbada, por lo tanto:

$$X(n) = F[X(n\text{-}1)]$$

El periodo del filtro recursivo 47 perturbado viene dado por:

$$L = \sigma \times \Delta \times (2^k\text{-}1)$$

donde σ es un entero positivo. El periodo mínimo del filtro recursivo 47 perturbado es entonces:

$$L_{min} = \Delta \times (2^k\text{-}1).$$

Además, la secuencia perturbadora Q generada por el registro de desfase de reacción 48 presenta una amplitud claramente más baja que la de la secuencia caótica generada por el generador 46 de manera que la relación R entre las dos amplitudes máximas es superior o igual a 40 dB:

$$R = 20\log\left[\frac{\text{Amplitud máxima de la señal caótica}}{\text{Amplitud máxima de la señal perturbadora}}\right] \ge 40 \text{ db}$$

La figura 3 ilustra la estructura de un sistema 100 de generación de secuencias caóticas según la invención.

El sistema 100 de generación comprende veintiocho generadores 101 a 128 de secuencias caóticas análogos al generador 2 de la figura 1.

Los 28 generadores 101 a 128 están distribuidos en dos conjuntos de generadores, comprendiendo el primer conjunto los 14 generadores 101 a 114 y comprendiendo el segundo conjunto los 14 generadores 115 a 128.

Cada conjunto de 14 generadores comprende dos grupos de 7 generadores cuyas salidas están conectadas a las entradas de un multiplexor analógico de 8 a 1.

Así, las salidas de los generadores 101, 103, 105, 107, 109, 111 y 113 están conectadas a las entradas de un multiplexor 130 y las salidas de los generadores 102, 104, 106, 108, 110, 112 y 114 están conectadas a las entradas de un multiplexor 132.

Las salidas de los generadores 115, 117, 119, 121, 123, 125 y 127 están conectadas a las entradas de un multiplexor 134 y las salidas de los generadores 116, 118, 120, 122, 124, 126 y 128 están conectadas a las entradas de un multiplexor 136.

Además, las salidas de los generadores 130 y 132 están conectadas a una puerta O exclusiva 138 y las salidas de los generadores 134 y 136 están conectadas a una puerta O exclusiva 140, estando las salidas de las dos puertas O

exclusiva 138 y 140 conectadas a una puerta O exclusiva 142.

Los multiplexores 130, 132, 134, 136 están conectados a unos medios de direccionamiento de dichos multiplexores que comprenden un registro de desfase de reacción 144 de tres fases conectado a un reloj c_k 146.

Los valores de los bits en las tres fases del registro 144 se indican como Q_2, Q_1, Q_0.

Además, según un modo de realización particular de la invención, el sistema de generación 100 de secuencias caóticas comprende unos medios de eliminación 148 de una cantidad determinada de muestras de las secuencias caóticas generadas por el sistema, por ejemplo un porcentaje p% de muestras.

El sistema de generación 100 también comprende, preferentemente, unos medios de cuantificación 150 de las secuencias caóticas generadas en un número de bits Nq inferior a N.

Los medios de eliminación 148 y los medios de cuantificación 150 permiten aumentar el tamaño de la clave secreta, lo cual tiene como consecuencia una mejora de la seguridad.

Aunque la figura 3 ilustra un sistema de generación 100 que comprende 28 generadores caóticos, en otro modo de realización de la invención no representado se proponen únicamente 14 generadores caóticos, lo cual corresponde a un sistema de generación que consiste en la mitad del sistema 100 de la figura 3.

Las expresiones de los veintiocho polinomios primitivos P-G1 a P-G28 de los registros de desfase de reacción para la perturbación de los 28 generadores 101 a 128 respectivamente de la figura 3 y del polinomio primitivo g del registro de desfase de reacción RDR 144 utilizado para el direccionamiento de los multiplexores 130, 132, 134 y 136 son las siguientes:

$$P-G1: g_1(x) = x^{16} + x^{12} + x^3 + x + 1 \text{ ,donde } [16, 12, 3, 1, 0];$$

$$P-G3: g_3(x) = x^{16} + x^{12} + x^7 + x^2 + 1$$

$$P-G5: g_5(x) = x^{16} + x^9 + x^5 + x^2 + 1$$

$$P-G7: g_7(x) = x^{16} + x^{15} + x^9 + x^4 + 1$$

$$P-G9: g_9(x) = x^{16} + x^{12} + x^9 + x^6 + 1$$

$$P-G11: g_{11}(x) = x^{16} + x^{10} + x^7 + x^6 + 1$$

$$P-G13: g_{13}(x) = x^{16} + x^9 + x^4 + x^3 + 1$$

$$P-G2: g_2(x) = x^{17} + x^3 + 1$$

$$P-G4: g_4(x) = x^{17} + x^{16} + x^3 + x + 1$$

$$P-G6: g_6(x) = x^{17} + x^8 + x^7 + x^6 + x^4 + x^3 + 1$$

$$P-G8: g_8(x) = x^{17} + x^9 + x^8 + x^6 + x^4 + x + 1$$

$$P-G10: g_{10}(x) = x^{17} + x^7 + x^4 + x^3 + 1$$

$$P-G12: g_{12}(x) = x^{17} + x^{12} + x^6 + x^3 + x^2 + x + 1$$

$$P-G14: g_{14}(x) = x^{17} + x^{11} + x^8 + x^6 + x^4 + x^2 + 1$$

$$P-G15: g_{15}(x) = x^{19} + x^5 + x^2 + x + 1$$

$$P-G17: g_{17}(x) = x^{19} + x^{12} + x^{10} + x^9 + x^7 + x^3 + 1$$

$$P-G19: g_{19}(x) = x^{19} + x^{13} + x^8 + x^5 + x^4 + x^3 + 1$$

$$P-G21: g_{21}(x) = x^{19} + x^{18} + x^{17} + x^{16} + x^{12} + x^7 + x^6 + x^5 + x^3 + x + 1$$

$$P-G23: g_{23}(x) = x^{19} + x^9 + x^8 + x^7 + x^6 + x^3 + 1$$

$$P-G25: g_{25}(x) = x^{19} + x^{16} + x^{15} + x^{13} + x^{12} + x^9 + x^5 + x^4 + x^2 + x + 1$$
$$P-G27: g_{27}(x) = x^{19} + x^{18} + x^{15} + x^{14} + x^{11} + x^{10} + x^8 + x^5 + x^3 + x^2 + 1$$

$$P-G16: g_{16}(x) = x^{23} + x^5 + 1$$
$$P-G18: g_{18}(x) = x^{23} + x^{12} + x^5 + x^4 + 1$$
$$P-G20: g_{20}(x) = x^{23} + x^{11} + x^{10} + x^7 + x^6 + x^5 + 1$$
$$P-G22: g_{22}(x) = x^{23} + x^{17} + x^{11} + x^5 + 1$$
$$P-G24: g_{24}(x) = x^{23} + x^{21} + x^7 + x^5 + 1$$
$$P-G26: g_{26}(x) = x^{23} + x^5 + x^4 + x + 1$$
$$P-G28: g_{28}(x) = x^{23} + x^{16} + x^{13} + x^6 + x^5 + x^3 + 1$$

$$RDR: g(x) = x^3 + x + 1$$

El funcionamiento del sistema de generación 100 de secuencias caóticas se describe en la continuación de la descripción con referencia a la figura 3.

En primer lugar, se inicializan los veintiocho generadores 101 a 128 y el registro de desfase de reacción 144.

El conjunto de las condiciones iniciales y de los parámetros de los diferentes generadores y de los diferentes registros de desfase de reacción del sistema 100 forma el tamaño de la clave secreta.

A continuación, en cada estado j = 1, 2,... 7 del registro 144 de 3 fases, sincronizado por el reloj c_k 146, la longitud de la secuencia caótica a la salida de la puerta O exclusiva 142 viene dada por:

$$L_{j\min}{}_{j=1,2,\ldots,7} = \text{mcm}\left[L_{j\min 1}, L_{j\min 2}\right]$$

donde:

- mcm indica el mínimo común múltiplo,
- $L_{jmin\ 1}$ indica la longitud de la secuencia caótica a la salida de la puerta O exclusiva 138 que viene dada por la relación:

$$L_{j\min 1}{}_{j=1,2,\ldots,7} = \text{mcm}\left\{\left[2^{k_{(2j-1)}}-1\right]\times\Delta_{k_{(2j-1)}}, \left[2^{k_{(2j)}}-1\right]\times\Delta_{k_{(2j)}}\right\}$$

en la que:

$\Delta_{k(2j-1)}$ y Δ_{k2j} representan respectivamente los periodos de dos generadores sin perturbación seleccionados (del primer grupo formado por 14 generadores 101 a 114) que llevan los índices (2j-1)+ 100 y 2j+100, siendo j de 1 a 7.

- L_{jmin2} indica la longitud de la secuencia caótica a la salida de la puerta O exclusiva 140 que viene dada por la relación:

$$L_{j\min 2}{}_{j=1,2,\ldots,7} = \text{mcm}\left\{\left[2^{k_{(14+2j-1)}}-1\right]\times\Delta_{k_{(14+2j-1)}}, \left[2^{k_{(14+2j)}}-1\right]\times\Delta_{k_{(14+2j)}}\right\}$$

en la que:

$\Delta_{k(14+2j-1)}$ y $\Delta_{k(14+2j)}$ representan respectivamente los periodos de dos generadores sin perturbación seleccionados (del segundo grupo formado por 14 generadores 115 a 128) que llevan los índices (14+2j-1)+ 100 y (14+2j)+100, siendo j de 1 a 7.

El periodo del reloj c_k 146 del registro de 3 fases 144 viene dado por

$$L_{Ck} = Min\left(L_{j\min_{j=1,2,\ldots,7}}\right)$$

La longitud mínima de la secuencia caótica generada a la salida de los medios de eliminación de muestras 148 viene dada entonces por

$$L_{\min} = 7 \times L_{Ck}\left[1 - p\%\right].$$

Esta longitud es extremadamente larga.

En efecto, el valor del ciclo nominal Δ_{nom} de un generador de secuencias caóticas clásico no perturbado es del orden de $\Delta_{nom} \cong \sqrt{\left(2^N\right)^3} = 2^{3N/2} = 2^{48}$ para N = 32.

Con este fin, el artículo de O.E. Lanford III "Informal Remarks on the Orbit Structure of Discrete Approximation to Chaotic Maps" en Experimental Mathematics, 1998, vol. 7, n° 4, págs. 317-324 da el valor de Δ_{nom} anterior. Este valor se verifica también mediante el procedimiento de medición de órbita según la invención.

La longitud mínima del ciclo del filtro recursivo perturbado 47 es entonces (para un grado mínimo k=16 del registro RDR 48)

$$l_{\min} \cong \Delta_{nom} \times 2^{16} \cong 2^{64}$$

Así, la longitud de la secuencia caótica viene dada por:

$L_{min} = 7 \times 2^{128}$ muestras, lo cual es colosal, siendo la edad del universo del orden de 10^{10} años.

Con una secuencia caótica de este tipo, es posible cifrar prácticamente 10^{32} imágenes diferentes, siendo el tamaño de cada una de 3 x 1024 x 1024 x 32 bits.

Esta secuencia caótica es por lo tanto ideal para su utilización como una máscara desechable para canales de comunicación ultrasecretos como "el teléfono rojo".

Por otro lado, el tamaño de la clave secreta es muy grande, en comparación con las claves de los generadores de las señales pseudoaleatorias del estado de la técnica. Está formada por cualquier condición inicial y por los parámetros de los diferentes generadores y de los diferentes registros de desfase de reacción. Debido a ello, los diferentes tipos de ataques (exhaustivo, de texto claro elegido, de texto cifrado elegido,...) son prácticamente imposibles de realizar.

Cada generador perturbado presenta una subclave compuesta por:

- 6 condiciones iniciales, es decir 6 x N bits,
- 6 parámetros, es decir 6 x N bits,
- 2 entradas k_u, es decir 2 x N bits.

El registro 144 presenta una subclave compuesta por:

- la condición inicial en N_1 = 16 bits como mínimo y
- Δ en N_2 = 64 bits como mínimo.

Por otro lado, son necesarios 5 bits de los cuales 2 bits son para indicar el multiplexor (1 de 4) utilizado, seguidos de 3 bits para señalar el generador perturbado (1 de 7) utilizado en la entrada del multiplexor en cuestión.

Se requieren también 3 bits como condición inicial para el registro 144 que direcciona los multiplexores 130, 132, 134, 136.

Por último, se requiere un número de bits mínimo N3 # 128 bits para L_{Ck}.

El tamaño de la clave secreta del sistema 100 de generación de la figura 3 es por lo tanto:

$$N_T \cong 28 \times \left[14 \times N + N_1 + N_2\right] + 128 = 14912\ bits$$

Es enorme. A título indicativo, la complejidad de un ataque exhaustivo para una clave de 128 bits es de aproximadamente 2^{127} tentativas, o claves posibles para detectar la clave correcta. Suponiendo que un ordenador pueda probar un millón de claves por segundo, harían falta más de $5x10^{24}$ años para encontrar la clave correcta.

Resulta evidente que el tamaño de la clave secreta puede ser menor a esto, según la aplicación deseada.

La continuación de la descripción haciendo referencia a las figuras 4 y 5 describe el funcionamiento del procedimiento de medición de la longitud de la órbita de una secuencia caótica según la invención.

La órbita de una secuencia caótica está formada por dos partes que son un transitorio y un ciclo. La longitud de la órbita caótica se indica como = c + l donde c es la longitud del ciclo y l es la longitud del transitorio.

En la bibliografía se han dado diversos resultados para esta cuestión y para la simulación de los números aleatorios, pero sin indicar el método de medición utilizado. Estos estudios indican entre otras cosas que: para un número N_o de condiciones iniciales diferentes, el número medio de ciclos diferentes es:

$$\overline{N}_c(N_0) = \sum_{k=1}^{N_0} \frac{1}{2k-1} \cong \frac{1}{2} Ln(N_0) + 0{,}982 \qquad para\ N_0 \geq 2\,.$$

En efecto, determinadas condiciones iniciales no generan nuevos ciclos diferentes.

El sistema 100 de generación representado en la figura 3 genera unos ciclos de longitudes tales que es imposible medirlos.

En efecto, la longitud de un filtro recursivo perturbado solo es del orden de $l_{1pnom} \cong 2^{64}$.

Es necesario por lo tanto disponer de un procedimiento que permita medir órbitas caóticas en un tiempo razonable.

El organigrama de la figura 4 ilustra el funcionamiento del procedimiento de medición de la longitud de una órbita caótica según la invención.

En 200, para cada condición inicial diferente y cada valor de parámetro, se genera una subsecuencia inicial que consiste en un número N_t determinado de muestras de la secuencia caótica.

La etapa 204 prueba si la subsecuencia generada comprende un ciclo o no. Si, en 206, la órbita de la subsecuencia generada consiste únicamente en un transitorio, el proceso de generación continúa en 208 generando en 200 una subsecuencia siguiente que consiste en un número N'_t determinado de muestras de la secuencia caótica.

Preferentemente $N'_t = N_t$ de manera que la subsecuencia global obtenida es de longitud $2N_t$.

La prueba en 204 de la presencia de ciclo se vuelve a iniciar entonces y así sucesivamente hasta que la subsecuencia global comprenda un ciclo en 210.

Así, en un determinado momento, la subsecuencia global de longitud Ng = W x N_t (siendo W un entero positivo) se compone de un transitorio y de un ciclo de longitud no nula.

En 212, la longitud de la órbita de la secuencia caótica se calcula como la suma de las longitudes del transitorio y del ciclo de la subsecuencia global.

El procedimiento de la figura 4 se repite para todas las condiciones iniciales y todos los valores de parámetros.

Un análisis estadístico de las longitudes de las órbitas obtenidas permite entonces fijar el valor de la órbita nominal del generador caótico considerado.

Este procedimiento se ha aplicado al mapa PWLCM solo con N = 32 y al caso del filtro recursivo 4, 6 de orden 3 no perturbado de la figura 1, siendo N = 11.

Esta elección permite realizar un análisis comparativo entre las dos configuraciones consideradas.

La etapa 212 de medición de la longitud de la órbita de la secuencia caótica generada por el filtro recursivo 4, 6 de orden 3 no perturbado se describe más detalladamente con referencia a la figura 5.

Dado que el filtro recursivo 4, 6 comprende tres retardos, la medición de la longitud de la órbita de la secuencia caótica generada por este filtro 4, 6 comprende la búsqueda de los casos en que aparecen tres valores sucesivos partiendo del valor de la última muestra generada, es decir la muestra Ng.

Indicando como Ind(1) la dirección (en el vector línea de las muestras de tamaño Ng) del primer ciclo hallado y como Ind(f) la dirección del último ciclo hallado, la longitud del ciclo se calcula en 220 como c = Ng-Ind(1).

A continuación, en 222, se efectúa el cálculo siguiente: j = Ind(f)-1 y k = Ng-1.

En 224, se efectúa una prueba de igualdad de los valores de las muestras de direcciones j y k.

Si los valores de las muestras de direcciones j y k son iguales, entonces en 226 se decrementan los valores de j y de k, es decir j = j-1 y k = k-1.

Si los valores de las muestras de direcciones j y k son diferentes, entonces se calcula el valor del transitorio l en 228 como igual a j, es decir l = j.

La longitud de la órbita es entonces o = c + l.

La tabla 1 resume los resultados estadísticos obtenidos por el filtro recursivo 4 no perturbado para un número de condiciones iniciales N_o = 34489.

Número de ciclos diferentes	22307 # $2^{14,44}$
Número de transitorios diferentes	22476 # $2^{14,45}$
Número de órbitas diferentes	28049 # $2^{14,77}$
Media de ciclos	24322 # $2^{14,57} > 2^{11+3}$
Media de transitorios	18690 # $2^{14,19} > 2^{N+d}$
Media de órbitas	43237 # $2^{15,4} > 2^{N+1+d}$
Longitud máxima de los ciclos	39368737 # $2^{25,23}$
Longitud máxima de los transitorios	429108 # $2^{18,71}$
Longitud máxima de las órbitas	39368742 # $2^{25,23}$
Longitud mínima de los ciclos	1
Longitud mínima de los transitorios	2
Longitud mínima de las órbitas	14

Tabla 1

La tabla 2 da el porcentaje de las órbitas, ciclos y transitorios obtenidos por intervalo de longitud.

Intervalo en longitud	0-9	10-99	100-999	10^3 -10^4-1	10^4 -10^5-1	10^5-10^6-1	10^6-10^7-1	10^7-10^8-1
Órbita %	0	0,1479	2,5370	21,8852	70,4978	4,9001	0,0058	0,0261
Ciclo %	0,1682	1,4497	9,9771	37,2438	50,3465	0,7829	0,0058	0,0261
Transitorio %	0,1769	1,5135	9,8089	36,9161	50,7785	0,8061	0	0

Tabla 2

Cabe destacar que, a partir de la tabla 2, el 70% de las órbitas se encuentran dentro del intervalo de longitudes comprendidas entre 10^4 y 10^5, y el 92% de las órbitas se encuentran dentro del intervalo de longitudes comprendidas entre 10^3 y 10^5.

Las tablas 3, 4 y 5 dan el número de ciclos, de transitorios y de órbitas y sus frecuencias correspondientes.

Número de ciclos	15331	4228	1465	688	296	152	68	47	22	5	2	1	1	1	1
Frecuencia-ciclo	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Tabla 3

Número de transitorios	15638	4116	1485	624	297	178	67	34	15	10	8	2	1	1
Frecuencia-transitorio	1	2	3	4	5	6	7	8	9	10	11	12	13	14

Tabla 4

Número de órbitas	22799	4291	766	158	32	3
Frecuencia-órbita	1	2	3	4	5	6

Tabla 5

La tabla 6 resume los resultados estadísticos obtenidos por el mapa PWLCM para el mismo número de condiciones iniciales N_o = 34489.

Número de ciclos diferentes	$27307\# 2^{14,73}$
Número de transitorios diferentes	$27203\# 2^{14,72}$
Número de órbitas diferentes	$30027\# 2^{14,87}$
Media de ciclos	$32402\# 2^{14,98}$
Medias de transitorios	$32224\# 2^{14,97}$
Media de órbitas	$64626\# 2^{15,98}$
Longitud máxima de los ciclos	$1211239\# 2^{20,2}$
Longitud máxima de los transitorios	$779792\# 2^{19,5727}$
Longitud máxima de las órbitas	$1317077\# 2^{20,33} < 2^{32}-1$
Longitud mínima de los ciclos	1
Longitud mínima de los transitorios	0
Longitud mínima de las órbitas	107

Tabla 6

La tabla 7 da el porcentaje de órbitas, ciclos y transitorios obtenidos por intervalo de longitud.

Intervalo en longitud	0-9	$10\text{-}10^2\text{-}1$	$10^2\text{-}10^3\text{-}1$	$10^3\text{-}10^4\text{-}1$	$10^4\text{-}10^5\text{-}1$	$10^5\text{-}10^6\text{-}1$	$10^6\text{-}10^7\text{-}1$	$10^7\text{-}10^8\text{-}1$
Órbita %	0	0	0,026	2,2645	81,9914	15,7152	0,0029	0
Ciclo %	0,0174	0,2349	2,3196	21,1256	72,8783	3,4214	0,0010	0
Transitorio %	0,0261	0,2378	2,308	21,0879	73	3,3373	0	0

Tabla 7

Cabe destacar que, a partir de la tabla 7, el 82% de órbitas se encuentran dentro del intervalo de longitudes comprendidas entre 10^4 y 10^5, y aproximadamente el 98% de órbitas se encuentran dentro del intervalo de longitudes comprendidas entre 10^3 y 10^6

Las tablas 8, 9 y 10 dan el número de ciclos, de transitorios y de órbitas y sus frecuencias correspondientes.

Número de ciclos	21415	4784	952	133	20	3
Frecuencia-ciclo	1	2	3	4	5	6

Tabla 8

Número de transitorios	21324	4726	941	179	25	7	1
Frecuencia-transitorio	1	2	3	4	5	6	7

Tabla 9

Número de órbitas	26010	3607	378	29	3
Frecuencia-órbita	1	2	3	4	5

Tabla 10

Así, los resultados obtenidos por el mapa PWLCM con N = 32 bits son muy parecidos a los resultados obtenidos con el filtro recursivo de tres retardos, siendo N = 11. La regla analítica $\Delta_{nom} \cong \sqrt{\left(2^N\right)^3} = 2^{3N/2} = 2^{48}$ para N = 32, en el caso del filtro recursivo se puede estimar mediante extrapolación a partir de los resultados experimentales, mediante el valor $\Delta_{nom} \cong 2^{45}$. Por lo tanto, la longitud mínima de la secuencia caótica a la salida del sistema 100 de generación es $L_{min} > 7 \times 2^{128}$ muestras. Con esta secuencia se pueden cifrar aproximadamente 10^{32} imágenes diferentes de tamaño cada una: 3 x 1024 x 1024 x 32 bits.

Así, los resultados experimentales descritos anteriormente muestran que el generador caótico según la invención se

puede utilizar sin temor en cualquier aplicación que se refiere a la seguridad de los datos.

REIVINDICACIONES

1. Generador (2) de secuencias caóticas $e_u(n)$, siendo n un entero estrictamente positivo, de valores enteros representados en un número de bits de cuantificación N determinado, destinados en particular a formar unas claves de encriptado de información, comprendiendo dicho generador (2) por lo menos dos filtros recursivos (4, 6) discretos de orden por lo menos igual a 1 que generan a la salida una secuencia caótica de valores enteros, comprendiendo cada filtro recursivo (4, 6) unos medios de puesta en práctica (8, 10) de una función no lineal *F*, conectados a través de una puerta O exclusiva (12, 14) a unos medios de generación de una secuencia de perturbación *Q*(*n*) de valores enteros representados en un número de bits de cuantificación k determinado, caracterizado por que los dos filtros (4, 6) están montados en paralelo, siendo la secuencia caótica $e_u(n)$ de salida del generador (2) igual a una O exclusiva (20) de las secuencias caóticas de salida de los filtros recursivos (4, 6), y por que los medios de puesta en práctica (8, 10) de la función no lineal comprenden un mapa caótico.

2. Generador (2) de secuencias caóticas según la reivindicación 1, caracterizado por que los medios de generación de una secuencia de perturbación en cada filtro (4, 6) comprenden un registro de desfase de reacción (16, 18) de longitud máxima que utiliza un polinomio primitivo de grado k.

3. Generador (2) de secuencias caóticas según la reivindicación 1 o 2, caracterizado por que el orden de cada filtro recursivo es inferior o igual a 3.

4. Generador (2) de secuencias caóticas según cualquiera de las reivindicaciones 1 a 3, caracterizado por que los medios de puesta en práctica (8, 10) de la función no lineal comprenden un mapa caótico lineal por tramos PWLCM.

5. Generador (2) de secuencias caóticas según las reivindicaciones 3 y 4, caracterizado por que las secuencias $e_{uj}(n)$ de salida de cada filtro recursivo j = 1,2 vienen dadas por la relación $e_{uj}(n) = F(X_j(n\text{-}1),P) \oplus Q(n)$

en la que

$$F(X_j(n-1),P)=\begin{cases}\left\lfloor \dfrac{2^N \times X_j(n-1)}{P} \right\rfloor & 0 < X_j(n-1) \le P \\ \left\lfloor \dfrac{2^N \times [X_j(n-1)-P]}{2^{N-1}-P} \right\rfloor & P \le X_j(n-1) \le 2^{N-1} \\ \left\lfloor \dfrac{2^N \times [2^N-1-X_j(n-1)-P]}{2^{N-1}-P} \right\rfloor & 2^{N-1} \le X_j(n-1) \le 2^N - P \\ \left\lfloor \dfrac{2^N \times [2^N-1-X_j(n-1)]}{P} \right\rfloor & 2^N - P \le X_j(n-1) \le 2^N \end{cases}$$

siendo

$$X_j(n-1) = \mathrm{mod}\left[k_{uj}(n-1) + c_{j1} \times e_{uj}(n-1) + c_{j2} \times e_{uj}(n-2) + c_{j3} \times e_{uj}(n-3), 2^N\right]$$

donde

- *P* es un parámetro de control cuyo valor es inferior a 2^{N-1},
- $k_{uj}(n)$ es la secuencia de entrada del filtro recursivo j,
- c_{j1}, c_{j2}, c_{j3} representan los coeficientes del filtro recursivo j,
- la operación $\lfloor X \rfloor$ consiste en devolver el entero más grande menor o igual a *X*,
- la operación mod($X,2^N$) consiste en efectuar el módulo 2^N de *X*.

6. Generador (2) de secuencias caóticas según cualquiera de las reivindicaciones 1 a 3, caracterizado por que los medios de puesta en práctica de la función no lineal comprenden un mapa caótico de tipo "SKEW-Tent".

7. Sistema de generación de secuencias caóticas que comprende por lo menos un conjunto de 14 generadores de secuencias caóticas según cualquiera de las reivindicaciones 1 a 6, estando dichos generadores (101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128) distribuidos en dos grupos de 7 generadores cada uno, caracterizado por que comprende:

- un primer multiplexor analógico (130, 134) que permite seleccionar la salida de un primer generador de entre los generadores del primer grupo,

- un segundo multiplexor analógico (132, 136) que permite seleccionar la salida de un segundo generador de entre los generadores del segundo grupo,

estando las salidas de los dos multiplexores conectadas a una puerta O exclusiva (138, 140) que genera a la salida la secuencia caótica, y

- unos medios de direccionamiento de los multiplexores que comprenden un registro de desfase de reacción (144) conectado a un reloj (146) cuyo periodo es función de la longitud de la secuencia caótica.

8. Sistema de generación (100) de secuencias caóticas según la reivindicación 7, caracterizado por que comprende dos conjuntos montados en paralelo de 14 generadores de secuencias caóticas cada uno, siendo la secuencia caótica generada a la salida del sistema de generación (100) igual a una O exclusiva (142) de las secuencias caóticas generadas en las salidas de los dos conjuntos de 14 generadores.

9. Sistema de generación (100) de secuencias caóticas según la reivindicación 2 y la reivindicación 8, caracterizado por que los polinomios primitivos de los registros de desfase de reacción del primer conjunto de generadores (101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114) son diferentes de los polinomios primitivos de los registros de desfase de reacción del segundo conjunto de generadores (115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128).

10. Sistema de generación (100) de secuencias caóticas según cualquiera de las reivindicaciones 7 a 9, caracterizado por que comprende unos medios de eliminación (148) de una cantidad determinada de muestras de las secuencias caóticas generadas por el sistema (100).

11. Sistema de generación (100) de secuencias caóticas según cualquiera de las reivindicaciones 7 a 10, caracterizado por que comprende unos medios de cuantificación (150) de las secuencias caóticas generadas.

12. Sistema de encriptado, caracterizado por que comprende un sistema de generación de secuencias caóticas según cualquiera de las reivindicaciones 7 a 11, siendo dicho sistema de generación (100) de secuencias caóticas utilizado para la generación de claves secretas y en los procedimientos de cifrado/descifrado del sistema de encriptado.

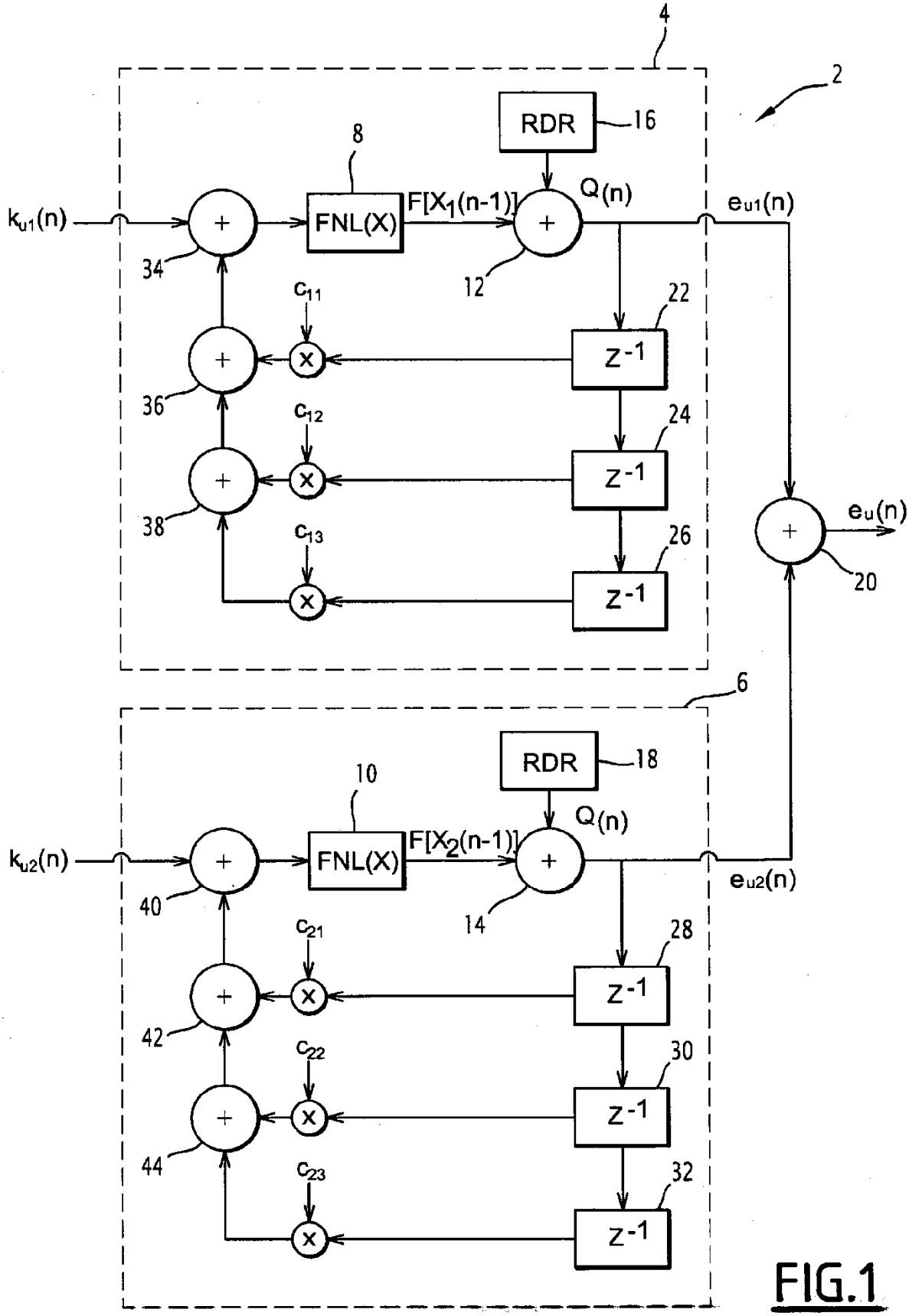
4
2
RDR
16
8
$k_{u1}(n)$
FNL(X)
$F[X_1(n-1)]$
Q(n)
$e_{u1}(n)$
34
12
c_{11}
22
Z^{-1}
36
c_{12}
24
Z^{-1}
38
c_{13}
26
Z^{-1}
$e_u(n)$
20
6
RDR
18
10
$k_{u2}(n)$
FNL(X)
$F[X_2(n-1)]$
Q(n)
$e_{u2}(n)$
40
14
c_{21}
28
Z^{-1}
42
c_{22}
30
Z^{-1}
44
c_{23}
32
Z^{-1}

FIG.1

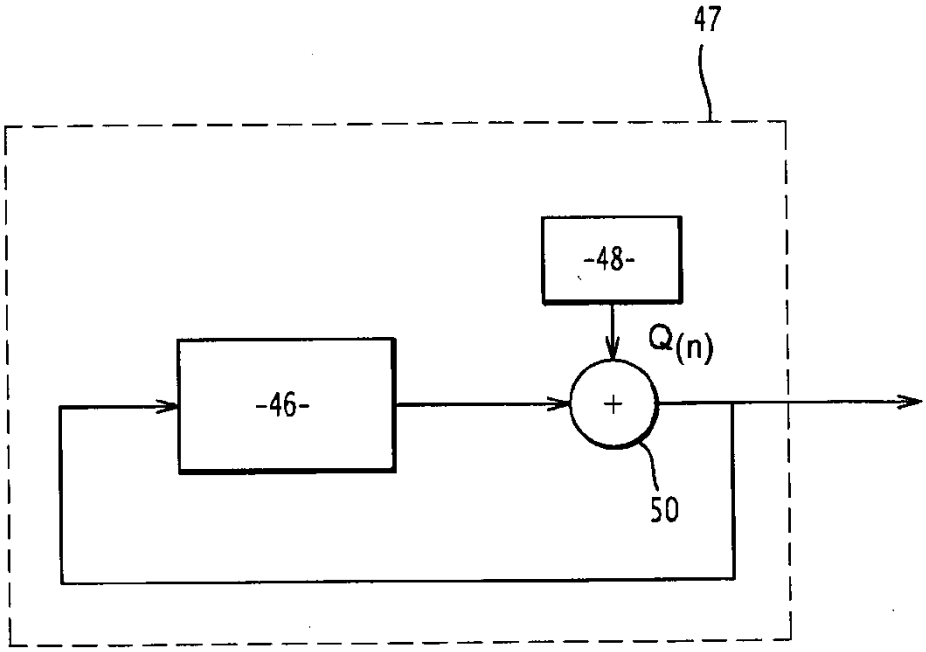

FIG.2

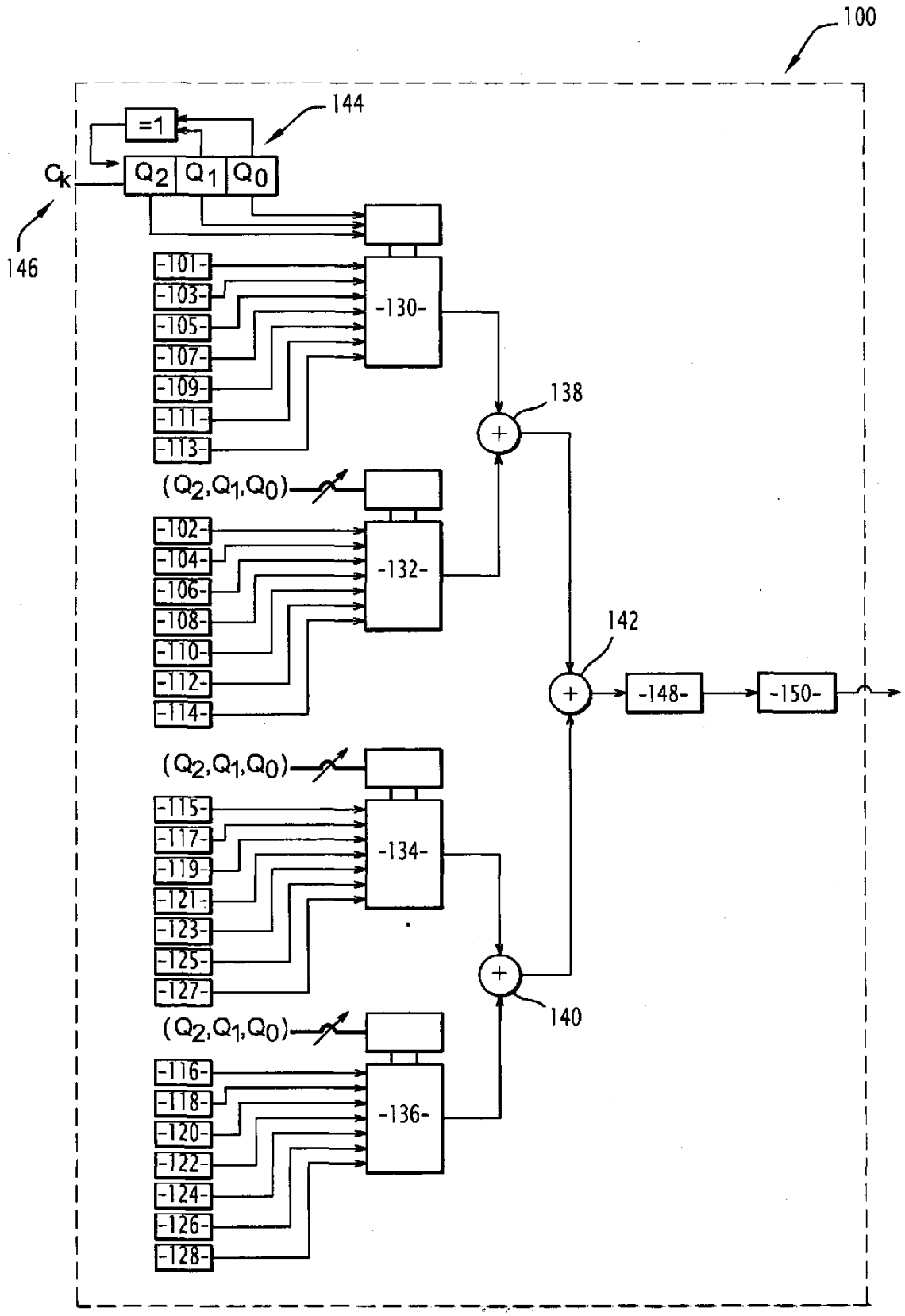
100
144
=1
Q_2 Q_1 Q_0
C_k
146
-101-
-103-
-105-
-107-
-109-
-111-
-113-
-130-
138
(Q_2,Q_1,Q_0)
-102-
-104-
-106-
-108-
-110-
-112-
-114-
-132-
142
-148-
-150-
(Q_2,Q_1,Q_0)
-115-
-117-
-119-
-121-
-123-
-125-
-127-
-134-
140
(Q_2,Q_1,Q_0)
-116-
-118-
-120-
-122-
-124-
-126-
-128-
-136-

FIG.3

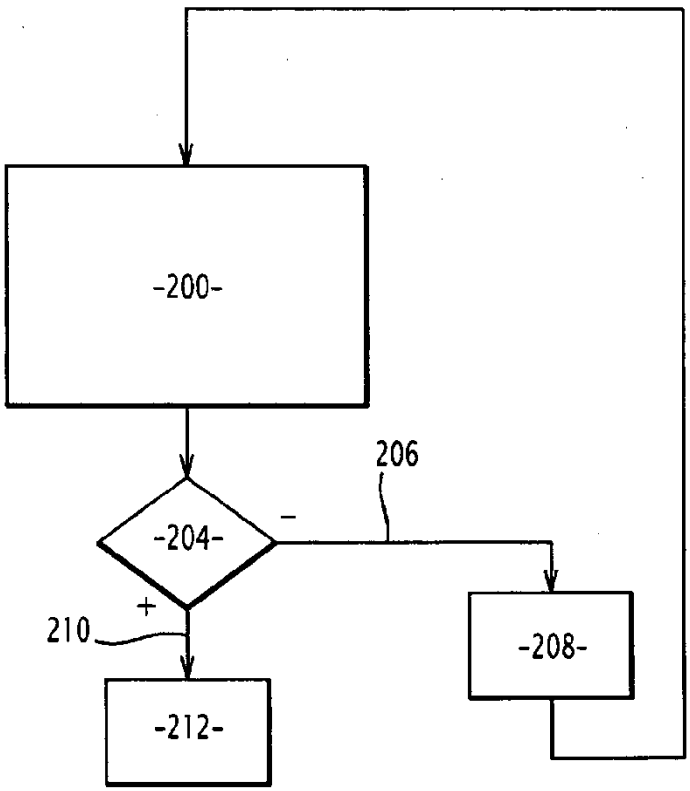

FIG.4

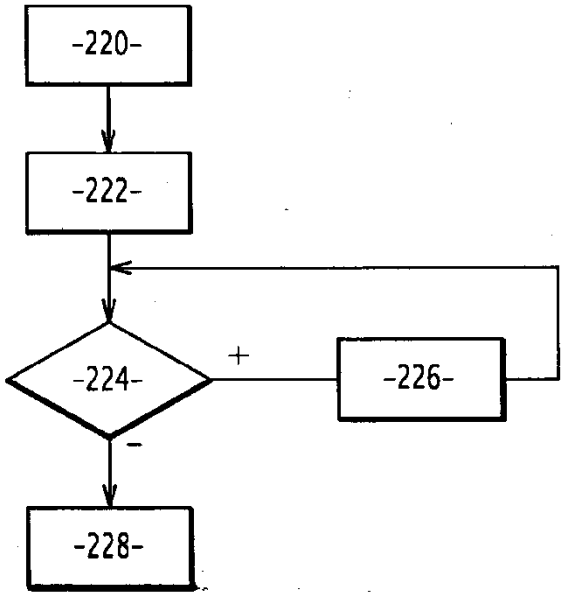

FIG.5