(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 595 483**

(51) Int. CI.:

H04L 9/00 (2006.01)
H04L 9/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.05.2013 PCT/EP2013/060662**

(87) Fecha y número de publicación internacional: **28.11.2013 WO13174944**

(96) Fecha de presentación y número de la solicitud europea: **23.05.2013 E 13725350 (6)**

(97) Fecha y número de publicación de la concesión europea: **29.06.2016 EP 2856693**

(54) Título: **Procedimiento para generar una secuencia seudo-aleatoria, y procedimiento para codificar o decodificar un flujo de datos**

(30) Prioridad:

24.05.2012 EP 12382201
14.08.2012 US 201261682964 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.12.2016

(73) Titular/es:

ENIGMEDIA S.L. (100.0%)
C/ Portuetxe 23B, Oficina 3-12
20018 San Sebastián, Gipuzkoa, ES

(72) Inventor/es:

VIDAL CASSANYA, GERARD

(74) Agente/Representante:

ARIAS SANZ, Juan

DESCRIPCIÓN

Procedimiento para generar una secuencia seudo-aleatoria, y procedimiento para codificar o decodificar un flujo de datos

OBJETO DE LA INVENCIÓN

La presente invención se refiere a un procedimiento para codificar un primer flujo de datos, dando lugar a un segundo flujo de datos codificados, y a un procedimiento para decodificar este segundo flujo de datos, donde la codificación es el resultado de comparar el primer flujo de datos con un tercer flujo de datos formado por una secuencia seudo-aleatoria, mediante una operación de comparación exclusiva (XOR). En concreto, la invención se refiere a los procedimientos basados en procedimientos de codificación hipercaóticos para generar las secuencias seudo-aleatorias utilizadas en la codificación y la decodificación.

ANTECEDENTES DE LA INVENCIÓN

La presente invención se enmarca dentro del campo de la codificación de flujos de información en comunicaciones seguras. En concreto, se enmarca dentro del campo de los procedimientos basados en sistemas hipercaóticos, algunos de los cuales son conocidos en el estado de la técnica.

En un caso simple de comunicación donde un mensaje se envía desde un transmisor A hasta un receptor B, el mensaje está codificado por un procedimiento de tal manera que A y B puedan codificar y decodificar, respectivamente.

La información codificada se llama cifra o mensaje cifrado y se envía a través del canal de comunicación. El mensaje está formado por un flujo de bits de una longitud cualquiera, y A y B generan una secuencia binaria para la codificación y la decodificación, respectivamente. Estas secuencias binarias son las secuencias de cifrado.

Si se cifra el mensaje desde A haciendo una operación binaria XOR, cuya tabla se muestra en la Tabla 1, con una secuencia de cifrado para A, en B se recupera el mensaje original si la secuencia de cifrado aplicada en A es la misma que la secuencia de cifrado aplicada en B.

Tabla 1: Tabla de XOR

Mensaje original (M)	Secuencia de cifrado (S)	Mensaje cifrado (M XOR S)
0	0	0
0	1	1
1	0	1
1	1	0

La invención se basa en las aportaciones publicadas en la tesis del mismo autor “Vidal, G. Sincronización y control de sistemas dinámicos en régimen de caos espacio-temporal (Tesis de Doctorado, Universidad de Navarra, España, 2010)”, donde se detalla el procedimiento de obtención de las secuencias aleatorias, basado en sistemas hipercaóticos, y donde las secuencias son generadas a partir de un sistema dinámico.

Un sistema dinámico es un sistema cuyo estado evoluciona con el tiempo. El comportamiento en dicho estado se puede modelizar determinando las ecuaciones de comportamiento del sistema tras identificar los elementos que intervienen y sus relaciones. Un sistema dinámico modelizado mediante una ecuación diferencial o un sistema de ecuaciones diferenciales admite ser descrito en cuanto a su comportamiento, mediante la solución de dicha ecuación o sistema de ecuaciones. En particular, es posible expresar una ecuación diferencial de un problema de valor inicial de primer orden de la forma $x'(t) = f(t, x(t))$, donde $x(t)$ es la solución del sistema en función del tiempo t, y donde las condiciones iniciales son $x(t_0) = x_0$. Si, en lugar de una ecuación diferencial ordinaria, el sistema requiere el uso de más variables, entonces x es una variable vectorial perteneciente al espacio R^n, siendo n la dimensión del sistema de ecuaciones y donde cada componente del vector x es una variable en función del tiempo.

La criptografía caótica se basa en el uso de la teoría del caos sobre sistemas de comunicaciones seguras. La teoría del caos estudia los sistemas deterministas con una alta sensibilidad de respuesta a un pequeño cambio en las condiciones iniciales.

Los sistemas A y B están sincronizados al iniciarse la codificación. Esto implica que en ambos se está generando la misma secuencia aleatoria para poder codificar y decodificar el mensaje utilizando el operador XOR en ambos extremos de la comunicación. Si no existe esta sincronización, el mensaje decodificado no resulta ser el mensaje originalmente codificado.

El procedimiento descrito en el documento de tesis anteriormente citado propone un procedimiento de generación de las secuencias aleatorias donde ambos sistemas A y B resuelven sendos sistemas de ecuaciones diferenciales. El objetivo es buscar un cifrado que cumpla la aproximación teórica de C.E. Shannon “Shannon, C. E. [1949] “Teoría

de la comunicación de sistemas de secretos", Bell System Technical Journal 28, págs. 656 a 715", que afirma que una condición necesaria y suficiente para que un mensaje sea "perfectamente secreto" es que el cifrado no dependa probabilísticamente del mensaje; de esta manera, no se puede hacer un enfoque probabilístico para descubrir propiedades del mensaje. Otra importante conclusión que hace Shannon es que, si la longitud de la clave no es un inconveniente, el cifrado de Vernam es el más adecuado. Un cifrado de Vernam tiene 3 características fundamentales:

1. La clave, en nuestro caso la secuencia de cifrado, debe ser tan larga como el mensaje a cifrar.

2. Una vez que la clave se ha usado, ésta ya no se puede reutilizar. Por esta razón, el cifrado de Vernam se llama también "libreta de un solo uso".

3. La clave está compuesta por una lista de símbolos aleatorios uniformemente distribuidos.

La primera propiedad exige que la clave sea suficientemente larga. En teoría, al usar un sistema dinámico caótico, las trayectorias pueden ser todo lo largas que sea necesario, sin llegar a ser nunca periódicas. No es posible tener una secuencia infinitamente larga en un ordenador, pero se puede implementar con suficiente precisión para integrar periodos de tiempo sin que los errores de redondeo afecten al procedimiento, y que estos periodos de tiempo sean suficientemente largos como requieran los casos a tratar.

La segunda propiedad es fácilmente realizable por software, prohibiendo repetir valores de condiciones iniciales.

Un caso particular de técnica de cifrado y descifrado, descrito en el documento de tesis, establece dos sistemas de ecuaciones diferenciales asociados a un problema de valor inicial, que están acoplados. Estos sistemas de ecuaciones, uno utilizado para generar la llave de cifrado y el otro para generar la llave de descifrado, son tales que, aun partiendo de condiciones iniciales distintas, debido a los términos acoplados, tras haber integrado un determinado periodo de tiempo, terminan evolucionando conforme a la misma solución.

Para llevar a cabo el acoplamiento asegurando la autenticidad de los extremos de comunicación, existen dos opciones: o bien los valores de los parámetros de acople del sistema dinámico son públicos, y hay una tercera entidad para poder autenticar el receptor del mensaje, o bien se intercambian los valores de los parámetros dinámicos por un canal seguro, como, por ejemplo, usando claves de RSA (*Rivest, Shamir y Adleman*) o claves de Diffie-Hellman.

La segunda propiedad es también realizable por software, prohibiendo repetir factores de acople.

En la mayoría de los casos conocidos del estado de la técnica, estas dos propiedades implican pasar claves enormes a través del canal de comunicaciones, y el coste es excesivo. Sin embargo, en el ejemplo descrito en el documento de tesis solo se transmite un conjunto de parámetros. Estos parámetros dan acceso a un conjunto de claves, que son tantas como puntos "digitales" hay en el espacio de fases, donde están encerradas las trayectorias. Pero para conocer la clave concreta hay que llevar a cabo el proceso de sincronización entre los sistemas A y B; esto es, es necesario integrar en ambos sistemas un tiempo suficiente como para que se considere que la solución obtenida en uno y otro sistema en función del tiempo es la misma, o que su diferencia está por debajo de un valor de umbral muy reducido o de un valor denominado "error de máquina" si se trabaja con un ordenador.

La tercera propiedad requiere señales aleatorias; sin embargo, el punto de partida es un sistema determinístico. Para realizar este proceso se aprovechan las propiedades dinámicas del sistema y un proceso de blanqueamiento de la señal. Uno de los mayores problemas de las señales continuas determinísticas, incluso las hipercaóticas, es la facilidad con la que se pueden seguir. Esto significa que un espía podría estimar con más o menos acierto los próximos valores de la señal, conociendo los instantes pasados. De esta manera, el posible espía podría ir acotando las posibles condiciones iniciales, hasta descubrir finalmente la clave. Para evitar este tipo de ataque se usa un proceso de blanqueamiento. El documento de tesis describe un proceso de blanqueamiento, que permite transformar la señal continua en una binaria. Para empezar, se requieren señales continuas que estén sumamente no correlacionadas, minimizando la información estadística que posea el mensaje cifrado.

El documento de tesis describe un procedimiento que se basa en el hecho de que los sistemas hipercaóticos tienen señales continuas cuya auto-correlación temporal se pierde rápidamente. Por otro lado, también es deseable que el sistema generador de secuencias sea de alta dimensión; de esta manera, es más difícil que aparezcan órbitas periódicas en la solución del sistema de ecuaciones que se resuelve, un problema típico cuando se trabaja con caos informatizado. En el caso de haber periodicidad en la solución al sistema de ecuaciones, se está facilitando el trabajo al espía, ya que tendría una referencia temporal con la que medir las estadísticas del sistema.

Otro requisito más que tiene que cumplir el procedimiento de codificación es asegurar que no existe ninguna función biyectiva entre el mensaje cifrado y el original, o lo que en criptografía se conoce como el problema de la función inversa. Para ello se usa el procedimiento de blanqueamiento de la señal, eliminando la mayor parte de la información de fase y amplitud. Así, la función que relaciona el mensaje y la cifra ya no será biyectiva y, por tanto, un mismo flujo de bits cifrado puede tener distintos significados. Sin embargo, al estar los dos sistemas sincronizados, siempre tendrán el mismo mensaje en claro.

El principal problema técnico que presenta el procedimiento de blanqueamiento de la señal que propone el documento de tesis es el alto coste computacional que supone y, además, el no generar una secuencia seudo-aleatoria completamente no correlacionada.

El documento EP0467239A2 divulga un sistema y un procedimiento de cifrado, basados en la matemática de la teoría del caos, que proporcionan protección de datos ante la modificación y uso no autorizados durante su almacenamiento y transmisión.

DESCRIPCIÓN DE LA INVENCIÓN

La presente invención resuelve el problema anteriormente descrito mediante un procedimiento para la generación de una secuencia seudo-aleatoria según la reivindicación 1, un procedimiento para la codificación de un flujo de datos o la decodificación de un flujo de datos codificado según la reivindicación 2, un codificador de mensajes según la reivindicación 14, un decodificador de mensajes cifrados según la reivindicación 15 y un sistema de comunicación según la reivindicación 16. Las reivindicaciones dependientes definen realizaciones preferidas de la invención.

Un primer aspecto inventivo que presenta la invención es un procedimiento para generar una secuencia seudo-aleatoria, que comprende las siguientes etapas:

a) proveer una ecuación diferencial de valor inicial $x' = f(x, t)$,

b) proveer un valor inicial para la ecuación diferencial $x_0 = x(t_0)$,

c) proveer un paso δt de integración para la ecuación diferencial, para la discretización en el tiempo $t_k = t_0 + k \cdot \delta t$, $k = 1, 2, 3 ...$,

d) llevar a cabo la integración numérica de la ecuación diferencial a partir del valor inicial y con el paso δt para la obtención de la aproximación a la solución $x_k = x(t_k)$,

e) generar una primera secuencia de valores llevando a cabo un muestreo entre los valores x_k, representables numéricamente en coma flotante en la forma $0,d_0d_1d_2d_3d_4...d_r...d_w \cdot 10^e$, siendo e el exponente, w la longitud de la mantisa, d_0 el dígito más representativo de la mantisa y d_r un dígito tal que él y todos los dígitos a su izquierda de la aproximación a la solución x_k coinciden con el valor exacto de la solución de la ecuación diferencial,

f) generar la secuencia seudo-aleatoria con los dígitos $d_i...d_r$ de una selección de la secuencia de valores x_k, donde i es un valor entero predeterminado que verifica $0 \leq i \leq r$.

El primer paso para iniciar la generación de la secuencia seudo-aleatoria es establecer el sistema dinámico que servirá para generar la secuencia seudo-aleatoria para el cifrado. El sistema dinámico se define con una ecuación diferencial de solución $x(t)$, abreviadamente expresada como x. Tras proveer un valor inicial y un paso de integración, resultado de una discretización en el tiempo para la integración del problema de valor inicial, se integra numéricamente la ecuación diferencial a partir del valor inicial para calcular la solución $x(t)$. Esto es, la secuencia de valores reales x_k se obtiene al calcular la solución numérica $x(t)$ a la ecuación $x' = f(x,t)$ dado el valor inicial $x_0 = x(t_0)$ para cada instante $t_k = t_0 + k \cdot \delta_t$, $k = 1, 2, 3 ...$

Los valores de la secuencia x_k son representables en coma flotante, donde dicha representación se puede expresar como $x_k = 0,d_0d_1d_2d_3d_4...d_r...d_w \cdot 10^e$, siendo e el exponente, w la longitud de la mantisa, d_0 el dígito más representativo de la mantisa y d_r un dígito tal que él y todos los dígitos a su izquierda de la aproximación a la solución x_k coinciden con el valor exacto de la solución de la ecuación diferencial. Una vez hecho esto, se genera la secuencia seudo-aleatoria con los dígitos $d_i...d_r$ de una selección de la secuencia de valores x_k, donde i es un valor entero predeterminado que verifica $0 \leq i \leq r$; es decir, se toman dígitos del número real que cumplen:

- pertenecen a la mantisa,
- son dígitos que coinciden con la solución exacta de x_k,
- no son los más representativos.

La elección de una selección de x_k da lugar a una colección de valores que serán tanto más no correlacionados cuanto más separados estén en la línea temporal.

La última propiedad de no ser los dígitos más representativos del número real x_k aporta la ventaja de generar una secuencia de valores no correlacionados entre sí en el menor tiempo posible. Al eliminar la dependencia entre dígitos más representativos se obtiene una secuencia cuyos valores son no correlacionados.

Según el estado de la técnica, para reducir el grado de correlación entre muestras se amplía la distancia entre los elementos de la selección x_k. Separar la distancia entre los elementos de la sección x_k implica evaluar muchos puntos intermedios mediante integración numérica hasta llegar a una nueva muestra x_k. A su vez, la integración de cada uno de los pasos supone un coste computacional elevado por el número de funciones y cálculos intermedios

que requiere.

Por el contrario, la invención, aunque reduce el número de dígitos que aprovecha para generar el flujo de datos para la codificación o decodificación, permite reducir drásticamente la distancia en la variable 'tiempo' entre las muestras x_k de la selección. Esto es, para una misma integración se hace uso de un número mucho mayor de muestras, incrementando sensiblemente el volumen de dígitos aleatorios generados no correlacionados para el mismo coste computacional.

Un segundo aspecto inventivo que presenta la invención es un procedimiento para la codificación de un flujo de datos para la transmisión de dichos datos por medio de un flujo codificado, donde la decodificación es el resultado de llevar a cabo la comparación del flujo de datos codificados con un segundo flujo de datos formado por una secuencia seudo-aleatoria, mediante una operación de comparación exclusiva (XOR), o un procedimiento para decodificar un flujo de datos codificados, donde la decodificación es el resultado de comparar el flujo de datos codificados con un segundo flujo de datos formado por una secuencia seudo-aleatoria, por medio de una operación de comparación exclusiva (XOR), caracterizado porque la generación de la secuencia seudo-aleatoria se realiza por medio del procedimiento según el primer aspecto inventivo.

Como se ha explicado con anterioridad, las secuencias generadas en los sistemas A y B deben ser las mismas para que, al aplicar en ambos lados de la comunicación la operación XOR, en B se obtenga el mensaje original. Al resolver la misma ecuación diferencial en ambos sistemas y generar la secuencia seudo-aleatoria siguiendo las mismas etapas se cumple esta condición, y con las mismas ventajas.

En un tercer aspecto inventivo se presenta un codificador de mensajes adaptado para llevar a cabo un procedimiento para codificar un flujo de datos para la transmisión de dichos datos, por medio de un flujo codificado, donde la codificación es el resultado de la comparación del flujo de datos con un segundo flujo de datos formado por una secuencia seudo-aleatoria, por medio de una operación de comparación exclusiva (XOR), caracterizado porque la generación de la secuencia seudo-aleatoria se realiza por medio de un procedimiento según el primer aspecto inventivo.

En un cuarto aspecto inventivo se presenta un decodificador de mensajes cifrados adaptado para llevar a cabo un procedimiento para decodificar un flujo de datos codificados, donde la decodificación es el resultado de la comparación del flujo de datos codificados con un segundo flujo de datos, formado por una secuencia seudo-aleatoria, por medio de una operación de comparación exclusiva (XOR), caracterizado porque la generación de la secuencia seudo-aleatoria se realiza por medio de un procedimiento según el primer aspecto inventivo.

En un quinto aspecto inventivo se presenta un sistema de comunicación que incluye al menos un codificador según el tercer aspecto inventivo y al menos un decodificador según el cuarto aspecto inventivo.

En una realización particular, el sistema de comunicación es un sistema de comunicaciones móviles. El valor inicial x_0 es provisto a ambos sistemas desde una central de comunicación. Si, por ejemplo, A y B son terminales móviles, esta central de comunicación puede ser la estación base BTS (estación base transceptora). En esta realización, se generan las mismas secuencias aleatorias en ambos extremos del sistema para poder recuperar el mensaje original aplicando el operador XOR. Estas secuencias son iguales debido a que se resuelve la misma ecuación diferencial con el mismo valor inicial.

DESCRIPCIÓN DE LOS DIBUJOS

Estas y otras características y ventajas de la invención se pondrán más claramente de manifiesto a partir de la siguiente descripción detallada de una forma preferida de realización, dada únicamente a título de ejemplo ilustrativo y no limitativo, con referencia a las figuras que se acompañan.

La figura 1 ilustra una realización de una comunicación entre dos terminales A y B y de los elementos que participan en la codificación.

La figura 2 representa una realización de una solución a la ecuación diferencial $x' = f(x, t)$.

La figura 3 representa los valores muestreados y no correlacionados, marcados con una X.

La figura 4 representa una realización particular del sistema donde se ilustran diferentes elementos funcionales, tales como el módulo que resuelve un sistema de ecuaciones diferenciales, expresable en la forma $x'_s = f_s(x_1,x_2,...,x_n,p_1,p_2, ...,p_m,t)$, s = 1 ...n, el módulo que selecciona un intervalo de dígitos de cada x_k, y un módulo generador de las filas de una matriz que denominaremos la matriz de expansión M_e, entre otros.

EXPOSICIÓN DETALLADA DE LA INVENCIÓN

La presente invención es de aplicación en los procesos de codificación de mensajes en la transmisión entre dos extremos en un sistema de comunicación. Así, como se ilustra en la figura 1, en un primer extremo de la comunicación (A) se codifica un mensaje (M) utilizando el operador XOR con la secuencia de cifrado (S). Por el canal de transmisión se envía el mensaje cifrado (M XOR S). En el extremo opuesto de la comunicación (B) se

decodifica el mensaje cifrado aplicando de nuevo el operador XOR. La invención se centra en la generación de las secuencias de codificación (S), que son idénticas en cada extremo de la comunicación, para poder obtener el mensaje (M) aplicando el operador XOR en B. La secuencia de codificación (S) es una secuencia seudo-aleatoria.

La invención presenta un procedimiento para la codificación de un flujo de datos para la transmisión de dichos datos mediante un flujo codificado, donde la codificación es el resultado de llevar a cabo la comparación del flujo de datos con un segundo flujo de datos formado por una secuencia seudo-aleatoria, mediante una operación de comparación exclusiva (XOR), caracterizado porque la generación de la secuencia seudo-aleatoria comprende las siguientes etapas:

a) proveer una ecuación diferencial de valor inicial $x' = f(x, t)$,

b) proveer un valor inicial para la ecuación diferencial $x_0 = x(t_0)$,

c) proveer un paso δ_t de integración para la ecuación diferencial, para la discretización en el tiempo $t_k = t_0 + k \cdot \delta_t$, $k = 1, 2, 3 ...$,

d) llevar a cabo la integración numérica de la ecuación diferencial a partir del valor inicial y con el paso δ_t para la obtención de la aproximación a la solución $x_k = x(t_k)$,

e) generar una primera secuencia de valores llevando a cabo un muestreo entre los valores x_k representables numéricamente en coma flotante en la forma $0,d_0d_1d_2d_3d_4...d_r...d_w \cdot 10^e$, siendo e el exponente, w la longitud de la mantisa, d_0 el dígito más representativo de la mantisa y d_r un dígito tal que él y todos los dígitos a su izquierda de la aproximación a la solución x_k coinciden con el valor exacto de la solución de la ecuación diferencial,

f) generar la secuencia seudo-aleatoria con los dígitos $d_i...d_r$ de una selección de la secuencia de valores x_k, donde i es un valor entero predeterminado que verifica $0 \leq i \leq r$.

La invención también presenta un procedimiento para la decodificación de un flujo de datos codificado mediante el procedimiento de acuerdo al primer aspecto inventivo, donde la decodificación es el resultado de llevar a cabo la comparación del flujo de datos codificados con un segundo flujo de datos formado por una secuencia seudo-aleatoria, mediante una operación de comparación exclusiva (XOR), caracterizado porque la generación de la secuencia seudo-aleatoria comprende las etapas a) a f) de un procedimiento según el primer aspecto inventivo.

Para ilustrar las ventajas descritas, se toma como realización la ilustración de la figura 2, donde se representa mediante una curva continua la solución de la ecuación diferencial $x' = f(x, t)$ para un determinado valor inicial. Tras la selección de un paso de integración, se obtiene una aproximación numérica mediante un procedimiento de integración de problemas de valor inicial, por ejemplo, haciendo uso de un procedimiento de cálculo explícito.

Aun así, los valores de la solución entre pasos consecutivos están sumamente correlacionados y es necesario llevar a cabo la integración de un conjunto elevado de pasos de integración para poder tomar dicho valor para utilizar sus dígitos para generar la secuencia de cifrado o descifrado.

Se toma como ejemplo la integración de un problema de valor inicial que permite obtener una solución seudo-aleatoria como la mostrada en la figura 2, donde se ilustra el espacio temporal desde 0 a 500 segundos. Se lleva a cabo una selección de tres valores extraídos a partir de los valores resultantes del procedimiento numérico de integración, destacados en la figura 3 sobre la curva de la solución obtenida mediante el mismo procedimiento de integración. De estos tres valores, las mantisas son las siguientes:

0,71(11)76 (para t=0s)

-0,28(60)51(para t=160s)

-0,49(14)38 (para t=320s).

Los exponentes de cada uno de los tres valores se han tenido en cuenta solo para establecer que el primer dígito a la derecha de la coma decimal es el primer dígito no nulo de la mantisa.

En esta secuencia de valores se han destacado entre paréntesis los dígitos que dejan a la izquierda a los dígitos más significativos y a la derecha los dígitos que pueden estar afectados por los errores de redondeo debidos a la arquitectura del ordenador donde se ejecuta la integración.

Esta selección de dígitos menos significativos elimina la dependencia temporal entre valores.

Si bien un número real es representable de muchas formas, el procedimiento considera los dígitos que resultan de esta representación particular (independientemente del exponente).

Un procedimiento que toma un conjunto de dígitos descartando:

• los dígitos más significativos y

• los dígitos que corresponden a errores de redondeo,

es una forma de llevar a cabo la invención con un modo particular de representación de los valores reales (de los valores que pertenecen al cuerpo de los números reales), ya que son también representables en la forma que indica la etapa e) de un procedimiento para la codificación de un flujo de datos como el descrito previamente.

El paréntesis de la izquierda y el paréntesis de la derecha están en la posición que deja en su interior a los dígitos $d_i...d_r$ correspondientes a la etapa f) del procedimiento de acuerdo a la reivindicación 1. En función de cada ejemplo, las posiciones de los paréntesis, y por tanto el rango de dígitos $d_i...d_r$, serán distintos y estarán pre-establecidos antes de aplicar la integración.

La concatenación de los dígitos entre paréntesis dará lugar a la secuencia: 116014. Dado que una de las ventajas del procedimiento reivindicado permite tomar muestras más cercanas en el tiempo, para un mismo intervalo de tiempo, es posible hacer uso de más valores que proveen dígitos para la generación de la secuencia, siempre verificando las propiedades de no correlación.

En una realización de la invención, en los procedimientos para la codificación y la decodificación, en la etapa d) se lleva a cabo la integración numérica, no de una ecuación diferencial, sino de un sistema de n ecuaciones diferenciales con n incógnitas; esto es, $x'_s = f_s(x_1,x_2, \dots ,x_n,p_1,p_2, \dots ,p_m,t)$, $s = 1 \dots n$, siendo n el número de incógnitas, y m el número de parámetros, p_j, $j = 1 \dots m$, tal que la secuencia seudo-aleatoria en la etapa f) se genera a partir de una de las n variables, preseleccionada del sistema de ecuaciones diferenciales. El sistema de ecuaciones aporta la ventaja de que la variable de interés depende de la variabilidad de otras variables y por tanto es menos probable que un espía pueda lograr reproducir la misma secuencia seudo-aleatoria para descifrar el mensaje codificado durante la transmisión desde A hasta B.

En una realización de los procedimientos se llevan a cabo las siguientes etapas:

• se determina un tiempo de integración T,

• se propone un sistema de ecuaciones perturbado, expresable de la forma:

$$x'^{A}_{1} = f_1(x_1, x_2, \dots, x_n, p_1, p_1, \dots, p_m, t) + \varepsilon^{A}_{1}(x^{B}_{1} - x^{A}_{1})$$

$$x'^{A}_{2} = f_2(x_1, x_2, \dots, x_n, p_1, p_1, \dots, p_m, t) + \varepsilon^{A}_{2}(x^{B}_{2} - x^{A}_{2})$$

...

$$x'^{A}_{n} = f_n(x_1, x_2, \dots, x_n, p_1, p_1, \dots, p_m, t) + \varepsilon^{A}_{n}(x^{B}_{n} - x^{A}_{n})$$

para la generación de la secuencia de codificación, así como valores iniciales; y,

• se propone un sistema de ecuaciones perturbado, expresable de la forma:

$$x'^{B}_{1} = f_1(x_1, x_2, \dots, x_n, p_1, p_1, \dots, p_m, t) + \varepsilon^{B}_{1}(x^{A}_{1} - x^{B}_{1})$$

$$x'^{B}_{2} = f_2(x_1, x_2, \dots, x_n, p_1, p_1, \dots, p_m, t) + \varepsilon^{B}_{2}(x^{A}_{2} - x^{B}_{2})$$

...

$$x'^{B}_{n} = f_n(x_1, x_2, \dots, x_n, p_1, p_1, \dots, p_m, t) + \varepsilon^{B}_{n}(x^{A}_{n} - x^{B}_{n})$$

para la generación de la secuencia de decodificación, así como valores iniciales no necesariamente coincidentes con los valores iniciales propuestos para la generación de la secuencia de codificación,

• con anterioridad a la codificación y decodificación de los datos, se lleva a cabo la generación de una primera secuencia de codificación y una primera secuencia de decodificación, integrando uno y otro sistema de ecuaciones perturbado a lo largo del tiempo T, donde ambos sistemas están acoplados mediante los términos multiplicados por $\varepsilon^{A}_{S}, \varepsilon^{B}_{S}, S = 1..n,$ siendo $\varepsilon^{A}_{S}, \varepsilon^{B}_{S}$ valores positivos en los que al menos uno, en el sistema asociado a la codificación, y otro, en el sistema asociado a la decodificación, es no nulo, de tal modo que, durante la integración se lleve a cabo un intercambio al menos de los valores de las variables x_1, x_2,... ,x_n que están multiplicadas por un valor $\varepsilon^{A}_{S}, \varepsilon^{B}_{S}, S = 1..n..$, n no nulo, a través de un canal de intercambio hasta la convergencia de ambos sistemas,

• se provee la secuencia de codificación y decodificación de datos integrando las mismas ecuaciones a partir de los

valores alcanzados en la integración llevada a cabo en la etapa anterior, tomados como condición inicial de forma independiente, sin intercambio de valores de acoplamiento y sin incorporar los términos con $\varepsilon_S^A, \varepsilon_S^B, S = 1..n$.

La ventaja de utilizar un sistema de ecuaciones perturbado es que al introducir los factores de acople $\varepsilon_S^A, \varepsilon_S^B, S = 1..n$, se consigue que ambos sistemas converjan sin necesidad de que las condiciones iniciales escogidas para la integración durante el tiempo T coincidan en ambos sistemas A y B. Los términos de acople que aparecen expresados de la forma $\varepsilon_i^A, (x_i^B - x_i^A)$ se pueden interpretar como señales de retroalimentación. Cuando los sistemas están en un régimen de sincronización completa estos términos se anulan. En ese momento, los dos sistemas A y B reproducen la misma trayectoria. La medida de la diferencia $(x_i^B - x_i^A)$, comparada con un valor de umbral pequeño y preestablecido, es un ejemplo de criterio para determinar si los sistemas están sincronizados.

Esto quiere decir que, si al sistema A le llega el valor x_i^B y además $x_i^A = x_i^B$ durante un cierto tiempo, quiere decir que los sistemas estarán sincronizados. De esta forma no es necesario compartir información previa a la integración, de manera que se tiene una comunicación segura sin intercambio de información susceptible de ser interceptada por un espía. Este es un caso de cifrado simétrico.

Esta situación implica que es necesario que ambos sistemas comuniquen sus variables por un canal público para que en ambos extremos de la comunicación, A y B, se sepa cuándo se ha llegado a la sincronización, que es el momento en el que las variables en ambos sistemas tienen el mismo valor. Este intercambio de variables se realiza en intervalos de tiempo que no necesariamente tienen que coincidir con el tiempo de integración, T. En el momento que se detecta que se ha alcanzado la convergencia en los valores de las variables comienza la codificación del mensaje en A y la consiguiente transmisión del mensaje codificado, tomando como valor inicial un valor de la solución en un instante de tiempo tal que pertenezca a la solución obtenida tras asegurar que los sistemas están sincronizados; y por supuesto, en el mismo instante en uno y otro sistema. En una realización este valor es el último valor de la integración alcanzado en ambos sistemas.

En una realización particular de la invención, el intercambio de las variables se realiza sobre un canal de intercambio cifrado mediante clave pública. Esto aporta la ventaja de aportar seguridad al sistema de comunicación ya que, aunque se conozcan los valores de las variables intercambiadas, no es posible deducir la solución puesto que no se conoce el sistema de ecuaciones; incluso en el caso de haber vulnerado este secreto, tampoco sería posible conocer la evolución de la solución dado que los parámetros intercambiados están cifrados.

En una realización particular de la invención, al implementar los procedimientos de codificación y decodificación, tras la etapa f), cada dígito d se representa en binario, con un tamaño pre-establecido de palabra D_1, dando lugar su concatenación a una secuencia binaria.

Esta manera de representar el número real aporta la ventaja técnica de utilizar la representación interna de un ordenador para generar directamente la secuencia seudo-aleatoria. Así, en esta realización se han obtenido resultados que muestran la ventaja de ahorro computacional al tomar los dígitos $d_i...d_r$ de los valores seleccionados de $x_k = x(t_k)$. Así, se tienen dos valores, tomados a partir de x_k y x_k+1, no correlacionados, en un tiempo mucho menor que lo que cuesta encontrar dos valores no correlacionados tomando todos los dígitos sin aplicar el procedimiento conforme a la invención. En la realización particular se toma un valor empírico de d_i para el que se sabe que los valores están no correlacionados en la mitad de tiempo.

El procedimiento según la invención conlleva la selección de un conjunto de dígitos para cada muestra y a la vez permite hacer uso de más muestras en un mismo periodo de integración. Se ha probado que el mayor número de muestras compensa la merma de dígitos y el procedimiento resultante tiene mayor eficacia que los descritos en el estado de la técnica.

Por otra parte, el efecto técnico introducido por la eliminación de bits es que se dificulta llevar a cabo ataques estadísticos para llegar a descifrar la secuencia seudo-aleatoria y así descifrar el mensaje.

En una realización particular, tras la etapa f), a cada dígito d se le hace corresponder una expresión binaria, con un tamaño de palabra D_1, dando lugar su concatenación a una secuencia binaria.

Como ejemplo ilustrativo se toma D_1=5, x_k=0,563124, x_k+1=0,648521, r=6, i=4, de manera que un tramo de la secuencia seudo-aleatoria es:

- $d_4...d_6$ de x_k: 124 ➔ representación en binario de cada dígito con 5 bits: 000010001000100,
- $d_4...d_6$ de x_{k+1}: 521➔ representación en binario de cada dígito con 5 bits: 001010001000001,

por tanto, el tramo de la secuencia seudo-aleatoria generada a partir de la selección de valores x_k y x_k+1 resulta ser la concatenación: 124521 ➔ (y en binario) 000010001000100001010001000001.

En una realización, se pre-establece un tamaño de palabra D_2 y, de la secuencia binaria, se forman dígitos enteros tomando palabras de D_2 bits.

Siguiendo con la realización, si D_2=3, entonces se forman grupos de 3 bits de la secuencia anteriormente generada y se tiene su representación en dígitos decimales:

000010001000100001010001000001➔0210412101

En una realización, antes de la aplicación de la operación de comparación exclusiva (XOR), la secuencia seudo-aleatoria es expandida en una secuencia con mayor número de elementos, según las siguientes etapas:

• se preestablece un valor entero positivo,

• se construyen dos vectores V_1 y V_2, de dimensión DIM, de enteros a partir de la secuencia seudo-aleatoria generada, por ejemplo, tomando DIM valores para completar V_1 y los DIM siguientes valores de la secuencia para completar V_2; y,

• se construye una matriz de expansión M_e de dimensión DIMxDIM a partir del producto $V_1 \cdot V_2^T$, donde V_2^T denota el vector traspuesto de V_2,

• generar la secuencia expandida mediante la concatenación de las filas de la matriz M_e.

Siguiendo con la realización, si la secuencia seudo-aleatoria es 02104121.. , entonces, si DIM es 3:

• V_1=021 (vector columna)

• V_2=041 (vector columna)

$$M_e = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} \cdot (0\ 4\ 1) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 8 & 2 \\ 0 & 4 & 1 \end{pmatrix}$$

• secuencia expandida=000082041,

de este modo, ventajosamente partiendo de dos vectores de 3 dígitos, se obtiene una colección de 9 dígitos en esta realización particular que da lugar a un nuevo vector al extraerlos por filas, con lo que con mayor razón se verifica la no correlación o relación entre la secuencia transmitida y las ecuaciones de las que parte, y el grado de aleatoriedad para dificultar la labor de un espía crece. Además, la eficacia computacional aumenta ya que se obtiene un número de dígitos “aumentado” respecto al número de dígitos de partida, por lo que, para generar una secuencia de un número de bits determinado, son necesarios menos bits de entrada.

En una realización particular, tras generar la matriz de expansión se opera de la siguiente manera:

• se pre-establece un valor K_1,

• cada elemento de la matriz M_e, antes de generar la secuencia expendida, es sustituido por el valor resultante de calcular su módulo-K_1.

Siguiendo con el ejemplo, si la matriz de expansión es

$$M_e = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 8 & 2 \\ 0 & 4 & 1 \end{pmatrix}$$

y K_1=3,

entonces, si la operación módulo-K es la operación cuyo resultado toma el resto de dividir un primer número entero entre un segundo número, tenemos:

$M_e = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 1 & 1 \end{pmatrix}$, entonces la secuencia seudo-aleatoria es:

S= 000022011.

Esta manera de operar, donde la operación módulo-K se aplica para valores de K en el rango [1,10], aporta la ventaja de poder operar con números de un solo dígito en el sistema decimal en el rango [0..9]. Esto es ventajoso cuando se tienen matrices cuyos elementos tienen valores muy altos, del orden de las centenas, debido a que M_e es el resultado de un producto, y por tanto es más costoso operar con ellos.

En una realización particular, adicionalmente, se llevan a cabo los siguientes pasos:

• adicionalmente a los vectores V_1 y V_2, se construye un vector V_3, de dimensión DIM, de enteros a partir de la secuencia seudo-aleatoria generada,

• sobre cada una de las filas de la matriz M_e, antes de generar la secuencia expandida mediante la concatenación de las filas de la matriz M_e, cada una de las filas de M_e es rotada circularmente un número entero de veces, en un sentido pre-establecido, de acuerdo al valor entero que establece la misma fila del vector V_3.

Si se toma como ejemplo el ilustrado en realizaciones particulares anteriores, se tiene que la secuencia seudo-aleatoria de partida era s=0210412101.

Por tanto,

• V_1=021 (vector columna)

• V_2=041 (vector columna)

• V_3=210 (vector columna de dimensión DIM = 3)

$$M_e = \begin{pmatrix}1\\2\\0\end{pmatrix}(0\ 4\ 1) = \begin{pmatrix}0&0&0\\0&8&2\\0&4&1\end{pmatrix} \rightarrow \text{rotar filas} \rightarrow \begin{pmatrix}0&0&0\\2&0&8\\0&4&1\end{pmatrix};$$

Así se tiene que la primera fila ha sido rotada 2 veces en el sentido de las agujas del reloj, la segunda fila ha sido rotada 1 vez y la tercera fila ha sido rotada 0 veces. Una vez más, la ventaja es que se aumenta el grado de aleatoriedad y de no correlación que impide que un espía pueda deducir la secuencia de partida y, por lo tanto, las ecuaciones diferenciales que se utilizan para generar la secuencia aleatoria.

En una realización particular, tras generar el vector V_3 se siguen además los siguientes pasos

• se pre-establece un valor K_2, preferentemente el valor DIM,

• cada elemento del vector V_3, antes de llevar a cabo la rotación circular, es sustituido por el valor resultante de calcular su módulo-K_2.

Esto evita que se tengan valores altos de los elementos en V_3, lo que provocaría rotar filas de M_e un número alto de veces, incluso mayor que la propia dimensión de matriz, dando lugar a tareas redundantes. Esta operación optimiza el coste computacional.

Si tomamos un ejemplo ilustrativo en el que los valores de los elementos de V_3 son altos, se tiene:

• la secuencia seudo-aleatoria de partida es s=0210418971,

por tanto,

• V_1=021 (vector columna)

• V_2=041 (vector columna)

• V_3=897(vector columna de dimensión DIM = 3)

$$M_e = \begin{pmatrix}0\\2\\1\end{pmatrix}(0\ 4\ 1) = \begin{pmatrix}0&0&0\\0&8&2\\0&4&1\end{pmatrix} \rightarrow \text{rotar filas} \rightarrow \begin{pmatrix}0&0&0\\0&8&2\\1&0&4\end{pmatrix};$$

Si se rotan las filas el número de veces que dictan las filas del vector V_3, se tiene el mismo resultado que si se rotasen V_3 mod 3 veces, o 2, 0 y 1 vez cada fila, respectivamente.

En una realización particular, en lugar de calcular la matriz M_e completamente para comenzar a operar con la secuencia seudo-aleatoria y con el operador XOR, se calculan las filas de la matriz y se va operando con ellas. No es necesario construir primero la matriz y extraer el flujo de datos después. De esta manera, tal como indica la figura 4, el sistema funciona más rápidamente y no es necesario guardar en memoria toda la matriz, solo la fila que se quiere extraer, operando directamente con ella. Esto aporta eficacia al sistema completo. Ventajosamente, con la matriz de expansión es posible bajar los requisitos de un sistema que implementa el procedimiento, tanto en procesador como en memoria, pudiendo ser implementado en equipos de hardware no muy potentes.

En la figura 4 se muestra el sistema con los elementos funcionales que generan la secuencia seudo-aleatoria (S) con la que se codifica el mensaje (m). En la misma figura se ilustra el sistema A con los diferentes elementos.

Se distingue un primer módulo (1) que resuelve el sistema de ecuaciones:

$$x'^{A}_{1} = f_1(x_1, x_2, \dots, x_n, p_1, p_1, \dots, p_m, t) + \varepsilon^{A}_{1}(x^{B}_{1} - x^{A}_{1})$$

$$x'^{A}_{2} = f_2(x_1, x_2, \dots, x_n, p_1, p_1, \dots, p_m, t) + \varepsilon^{A}_{2}(x^{B}_{2} - x^{A}_{2})$$

...

$$x'^{A}_{n} = f_n(x_1, x_2, \dots, x_n, p_1, p_1, \dots, p_m, t) + \varepsilon^{A}_{n}(x^{B}_{n} - x^{A}_{n})$$

También se distinguen:

• Un segundo módulo (2) que trunca la solución x_k por sus dígitos $d_i...d_r$.

Este segundo módulo (2) permite extraer, para cada muestra x_k, los dígitos que dan lugar a la secuencia seudo-aleatoria que será tratada posteriormente. En una realización, el módulo puede ser un segmento de código de programa informático adaptado para llevar a cabo un procedimiento que selecciona los dígitos correspondientes de valores de números reales representados internamente en un ordenador.

• Un tercer módulo (3) que obtiene los vectores V_1, V_2 y V_3.

Este tercer módulo (3) toma la concatenación de los dígitos procedentes del segundo módulo (2) y los representa de manera que genere vectores V_1, V_2 y V_3, dada una dimensión DIM. El tercer módulo (3), en una realización, es un segmento de código de programa informático adaptado para llevar a cabo un procedimiento que genera los vectores V_1, V_2 y V_3, dada una dimensión preestablecida DIM y una secuencia de valores enteros proporcionados por el segundo módulo (2).

• Un cuarto módulo (4) que obtiene V_1 mod K_1, V_2 mod K_1 y V_3 mod K_2.

El cuarto módulo (4) opera con cada elemento de los vectores V_1, V_2 y V_3, de manera que divida los valores de los elementos entre los valores K_1, K_1 y K_2 y obtenga el resto en cada elemento. El resultado son tres vectores cuyos elementos son los restos obtenidos de la división aplicada por el cuarto módulo (4). En una realización, el cuarto módulo (4) es un segmento de código de programa informático adaptado para llevar a cabo un procedimiento que opera según la manera descrita y obtiene los vectores V_1, V_2 y V_3 desde un módulo tal como el tercer módulo (3), y los valores K_1 pueden estar pre-establecidos.

• Un quinto módulo que genera las filas de la matriz M_e, siendo cada fila: M_e^1 la primera fila, M_e^2 la segunda fila y M_e^3 la tercera fila en la realización ilustrada.

El quinto módulo (5), en una realización, es un segmento de programa informático que opera con los vectores V_1, V_2 y V_3 de la siguiente manera: primero lleva a cabo el producto vectorial $V_1 \cdot V_2^T$. Este producto se puede llevar a cabo por filas sin necesitad de completar la matriz y almacenarla entera. La fila i-ésima de la matriz estará formada por los valores $V_{1i} \cdot V_{2j}$, donde V_{1i} es la componente i-ésima del vector V_1 y V_{2j} es la componente j-ésima del vector V_2, donde j recorrerá todas las columnas de la matriz y del vector V_2. Después de que el módulo obtiene la primera fila, la rota un número de veces igual al valor del primer elemento de V_3 y aporta el resultado. Así opera sucesivamente con cada una de las filas hasta completar la operación $(V_1 \cdot V_2^T)$rot V_3.

La secuencia seudo-aleatoria (s) generada es la concatenación de las filas en orden de generación. Esta secuencia (s) es operada, mediante el operador XOR, con el mensaje original (M) y el resultado es transmitido por el canal de comunicación.

Realización particular

En una realización particular, se parte de una señal, x_k, generada a partir de un sistema dinámico caótico. De esta señal se toman valores concretos y no correlacionados entre sí:

m1=0,98754213

m2=0,98214356

m3=0,61102348

m4=0,62021309

m5=0,41102441

m6=0,35000227

De cada muestra se eliminan los dígitos más significativos y los que dan lugar a errores de redondeo debidos a la arquitectura del ordenador utilizado para la integración, de manera que se obtenga:

s1=75421

s2=21435

s3=10234

s4=02130

s5=10244

s6=00022

El siguiente paso es agrupar estos valores para formar dos vectores v1, v2:

$$v1 = \begin{pmatrix} 75421 \\ 21435 \\ 10234 \end{pmatrix}$$

$$v2 = \begin{pmatrix} 02130 \\ 10244 \\ 00022 \end{pmatrix};$$

Se genera una matriz de expansión con estos dos vectores:

$$v_1 \cdot v_2^T \begin{pmatrix} 76056 & 35306 & 37336 \\ 62408 & 79488 & 21035 \\ 82633 & 42655 & 44934 \end{pmatrix} = M_e$$

Se obtiene el módulo K_1=90107 de cada elemento de la matriz.

A continuación, de la señal de inicio, se toman más muestras m7, m8, m9 y se genera un vector v_3 al que se le aplica el módulo K_2=3, obteniendo el vector:

$$V_3 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix};$$

Por tanto, aplicando la rotación a las filas de la matriz M_e se obtiene:

$$M_e = \begin{pmatrix} 37336 & 760563 & 35306 \\ 79488 & 21035 & 62408 \\ 82633 & 42655 & 44934 \end{pmatrix}.$$

A continuación, cada elemento de la matriz se transforma al formato binario mediante una transformación de elementos decimales a números binarios. Por ejemplo, concatenando los elementos de la matriz en binario, se obtiene la secuencia seudo-aleatoria (de la que se muestra únicamente la que corresponde a los primeros dos números):

$$\underbrace{01001000111011000}_{34336}\ \underbrace{10010100100011000\cdots}_{76056}$$

de tal forma que es esta secuencia la que se mezcla mediante la operación XOR con el mensaje para llegar al flujo de datos cifrado.

Este mismo conjunto de operaciones, llevado a cabo en el sector del receptor, permitirá el descifrado del mensaje.

REIVINDICACIONES

1.- Procedimiento para la generación de una secuencia seudo-aleatoria, caracterizado porque comprende las siguientes etapas:

a) proveer una ecuación diferencial de valor inicial $x' = f(x, t)$,

b) proveer un valor inicial para la ecuación diferencial $x_0 = x(t_0)$,

c) proveer un paso δ_t de integración para la ecuación diferencial, para la discretización en el tiempo $t_k = t_0 + k \cdot \delta t$, $k = 1, 2, 3 ...$,

d) llevar a cabo la integración numérica de la ecuación diferencial a partir del valor inicial y con el paso δ_t para la obtención de la aproximación a la solución $x_k = x(t_k)$,

e) generar una primera secuencia de valores llevando a cabo un muestreo entre los valores x_k representables numéricamente en coma flotante en la forma $0.d_0d_1d_2d_3d_4...d_r...d_w \cdot 10^e$, siendo e el exponente, w la longitud de la mantisa, d_0 el dígito más representativo de la mantisa y d_r un dígito tal que él y todos los dígitos a su izquierda de la aproximación a la solución x_k coinciden con el valor exacto de la solución de la ecuación diferencial,

f) generar la secuencia seudo-aleatoria con los dígitos $d_i...d_r$ de una selección de la secuencia de valores x_k, donde i es un valor entero predeterminado que verifica $0 \leq i \leq r$.

g) la secuencia seudo-aleatoria se expande a una secuencia con un número mayor de elementos, según las siguientes etapas:

- pre-establecer un valor entero positivo DIM,

- construir dos vectores V_1 y V_2, de dimensión DIM, de enteros a partir de la secuencia seudo-aleatoria,

- construir una matriz de expansión M_e, de dimensión DIMxDIM, a partir del producto $V_1 \cdot V_2^T$, donde V_2^T es el vector traspuesto de V_2,

- generar la secuencia expandida por medio de la concatenación de las filas de la matriz M_e.

2.- Procedimiento según la reivindicación 1, en el que, en la etapa d), se lleva a cabo la integración numérica de un sistema de n ecuaciones diferenciales, $x'_s = f_s(x_1, x_2, ..., x_n, p_1, p_2, ..., p_m, t)$, $s = 1 ...n$, siendo n también el número de incógnitas, y conteniendo m parámetros, p_j, $j = 1... m$, tal que la secuencia seudo-aleatoria en la etapa f) se genere a partir de una de las n variables preseleccionadas del sistema de ecuaciones diferenciales.

3.- Procedimiento según cualquiera de las reivindicaciones precedentes, en el que, tras la etapa f), cada dígito d se representa en binario, con un tamaño pre-establecido de palabra D1, dando lugar su concatenación de los dígitos a una secuencia binaria.

4.- Procedimiento según cualquiera de las reivindicaciones precedentes, en el que, tras la etapa f), a cada dígito d se le hace corresponder una expresión binaria, dando lugar su concatenación a una secuencia binaria.

5.- Procedimiento según cualquiera de las reivindicaciones 1 a 3, en el que se pre-establece un tamaño de palabra D_2 y, de la secuencia binaria, se forman dígitos enteros tomando palabras de D_2 bits.

6.- Procedimiento según cualquiera de las reivindicaciones 1 a 5, en el que:

• se pre-establece un valor K_1,

• cada elemento de la matriz M_e, antes de generar la secuencia expendida, es sustituido por el valor resultante de calcular su módulo-K_1.

7.- Procedimiento según cualquiera de las reivindicaciones precedentes, en el que:

• adicionalmente a los vectores V_1 y V_2, se construye un vector V_3 de dimensión DIM de enteros a partir de la secuencia seudo-aleatoria generada,

• sobre cada una de las filas de la matriz M_e, antes de generar la secuencia expandida mediante la concatenación de las filas de la matriz M_e, cada una de las filas de M_e es rotada circularmente un número entero de veces, en un sentido preestablecido, de acuerdo al valor entero que establece la misma fila del vector V_3.

8.- Procedimiento según cualquiera de las reivindicaciones precedentes, en el que:

• se pre-establece un valor K_2, preferentemente el valor DIM,

• cada elemento del vector V_3 es sustituido por el valor resultante de calcular su módulo-K_2.

9.- Procedimiento según cualquiera de las reivindicaciones precedentes, en el que, para llevar a cabo la generación de la secuencia expandida mediante la concatenación de las filas de la matriz M_e se procede llevando a cabo solo el cálculo de los valores de cada fila para evitar el almacenamiento de la matriz completa M_e.

10.- Procedimiento para codificar un flujo de datos para la transmisión de dichos datos, por medio de un flujo codificado, en el que la codificación es el resultado de la comparación del flujo de datos con un segundo flujo de datos formado por una secuencia seudo-aleatoria, por medio de una operación de comparación exclusiva (XOR), o un procedimiento para decodificar un flujo de datos codificados, en donde la decodificación es el resultado de la comparación del flujo de datos codificados con un segundo flujo de datos, formado por una secuencia seudo-aleatoria, por medio de una operación de comparación exclusiva (XOR), caracterizado porque la generación de la secuencia seudo-aleatoria se realiza por medio de un procedimiento de cualquiera de las reivindicaciones precedentes.

11.- Procedimiento según la reivindicación 10, en el que se llevan a cabo las siguientes etapas:

• se determina un tiempo de integración T,

• se propone un sistema de ecuaciones perturbado expresable de la forma:

$$x'^{A}_{1} = f_1(x_1, x_2, \dots, x_n, p_1, p_1, \dots, p_m, t) + \varepsilon^{A}_{1}(x^{B}_{1} - x^{A}_{1})$$

$$x'^{A}_{2} = f_2(x_1, x_2, \dots, x_n, p_1, p_1, \dots, p_m, t) + \varepsilon^{A}_{2}(x^{B}_{2} - x^{A}_{2})$$

...

$$x'^{A}_{n} = f_n(x_1, x_2, \dots, x_n, p_1, p_1, \dots, p_m, t) + \varepsilon^{A}_{n}(x^{B}_{n} - x^{A}_{n})$$

para la generación de la secuencia de codificación, así como valores iniciales; y

• se propone un sistema de ecuaciones perturbado expresable de la forma:

$$x'^{B}_{1} = f_1(x_1, x_2, \dots, x_n, p_1, p_1, \dots, p_m, t) + \varepsilon^{B}_{1}(x^{A}_{1} - x^{B}_{1})$$

$$x'^{B}_{2} = f_2(x_1, x_2, \dots, x_n, p_1, p_1, \dots, p_m, t) + \varepsilon^{B}_{2}(x^{A}_{2} - x^{B}_{2})$$

...

$$x'^{B}_{n} = f_n(x_1, x_2, \dots, x_n, p_1, p_1, \dots, p_m, t) + \varepsilon^{B}_{n}(x^{A}_{n} - x^{B}_{n})$$

para la generación de la secuencia de decodificación así como valores iniciales no necesariamente coincidentes con los valores iniciales propuestos para la generación de la secuencia de codificación,

• con anterioridad a la codificación y decodificación de los datos, se lleva cabo la generación de una primera secuencia de codificación y una primera secuencia de decodificación integrando uno y otro sistema de ecuaciones perturbado a lo largo del tiempo T donde ambos sistemas están acoplados mediante los términos multiplicados por $\varepsilon^{A}_{S}, \varepsilon^{A}_{S}, s = 1..$n, siendo $\varepsilon^{A}_{S}, \varepsilon^{A}_{S}$ valores positivos en los que al menos uno, en el sistema asociado a la codificación y otro en el sistema asociado a la decodificación es no nulo, de tal modo que, durante la integración se lleve a cabo un intercambio al menos de los valores de las variables $x_1, x_2, \dots, x_n$, que están multiplicadas por un valor $\varepsilon^{A}_{S}, \varepsilon^{A}_{S}, s = 1..$n no nulo, a través de un canal de intercambio, hasta la convergencia de ambos sistemas,

• se provee la secuencia de codificación y decodificación de datos integrando las mismas ecuaciones a partir de los valores alcanzados en la integración llevada a cabo en la etapa anterior, tomados como condición inicial de forma independiente sin intercambio de valores de acoplamiento y sin incorporar los términos con $\varepsilon^{A}_{S}, \varepsilon^{A}_{S}, s = 1 \dots n$.

12.- Procedimiento según la reivindicación 11, en el que el canal de intercambio está cifrado mediante clave pública.

13.- Codificador de mensajes adaptado para llevar a cabo un procedimiento para la codificación de un flujo de datos, para la transmisión de dichos datos por medio de un flujo codificado, en el que la codificación es el resultado de la comparación del flujo de datos con un segundo flujo de datos, formado por una secuencia seudo-aleatoria, por medio de una operación de comparación exclusiva (XOR), caracterizado porque la generación de la secuencia seudo-aleatoria se realiza por medio de un procedimiento según cualquiera de las reivindicaciones 1 a 9.

14.- Decodificador de mensajes cifrados, adaptado para llevar a cabo un procedimiento para decodificar un flujo de

datos codificados, en donde la decodificación es el resultado de la comparación del flujo de datos codificados con un segundo flujo de datos, formado por una secuencia seudo-aleatoria, por medio de una operación de comparación exclusiva (XOR), caracterizado porque la generación de la secuencia seudo-aleatoria se realiza por medio de un procedimiento según cualquiera de las reivindicaciones 1 a 9.

15.- Sistema de comunicación que incluye al menos un codificador según la reivindicación 13 y al menos un decodificador según la reivindicación 14.

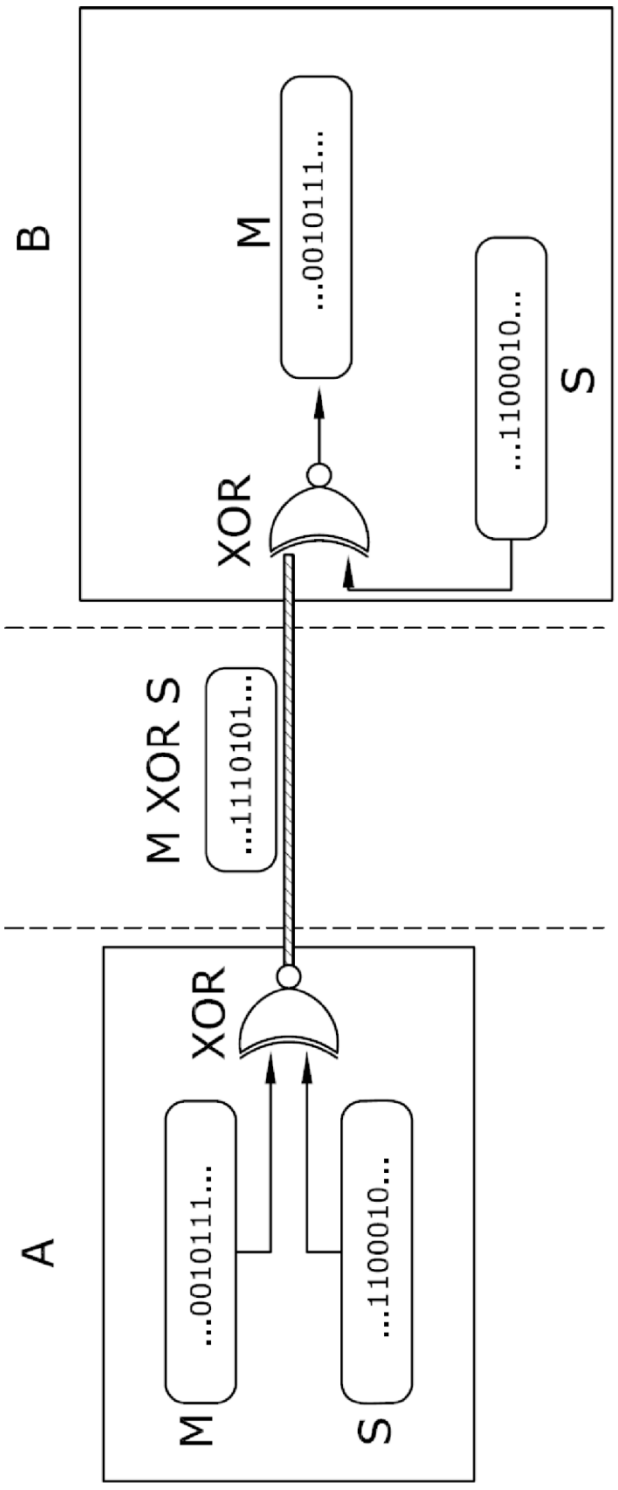
A
M
...0010111...
S
...1100010...
XOR
M XOR S
...1110101...
B
M
...0010111...
...1100010...
S
XOR

FIG.1

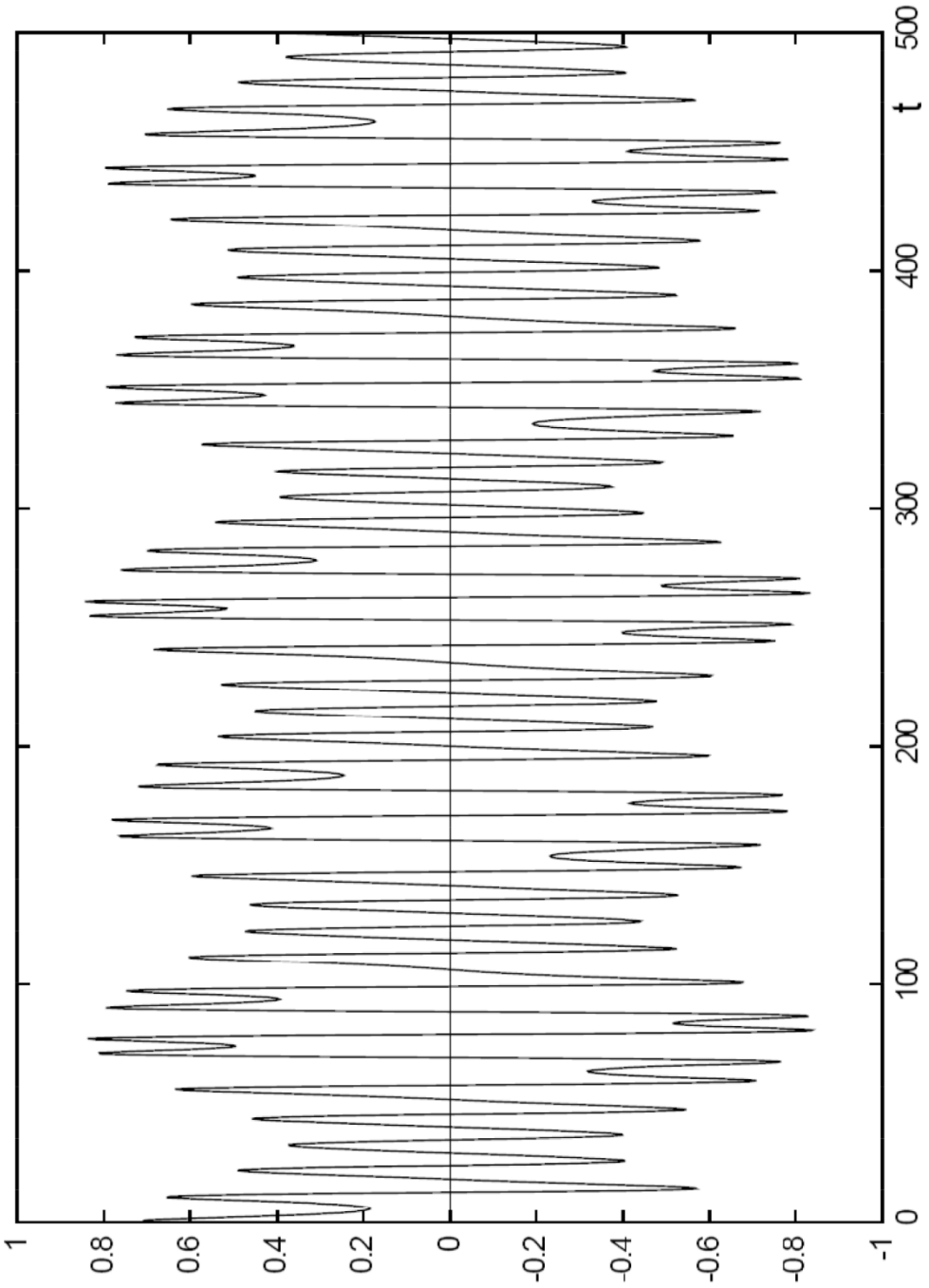

FIG. 2

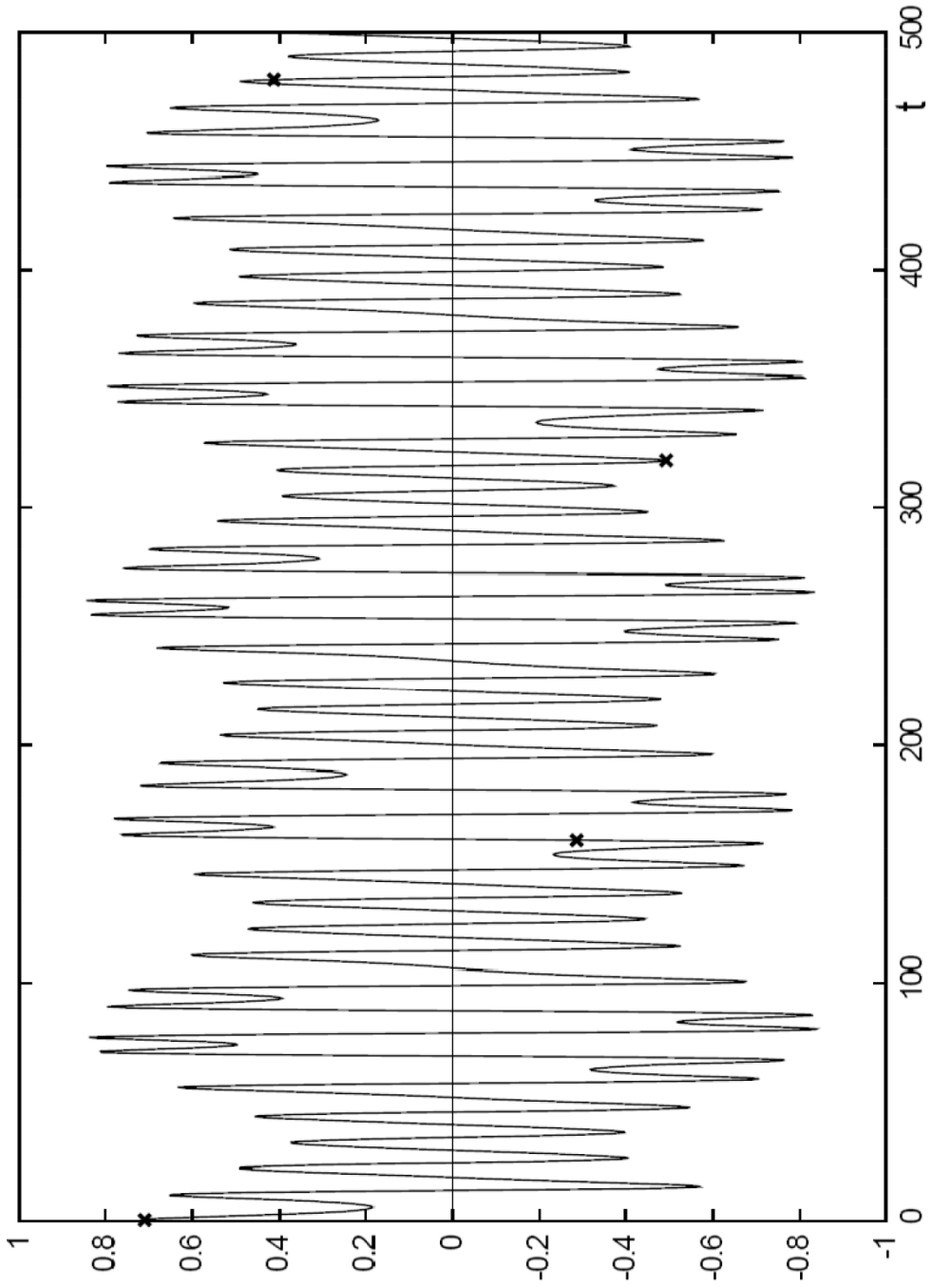

FIG. 3

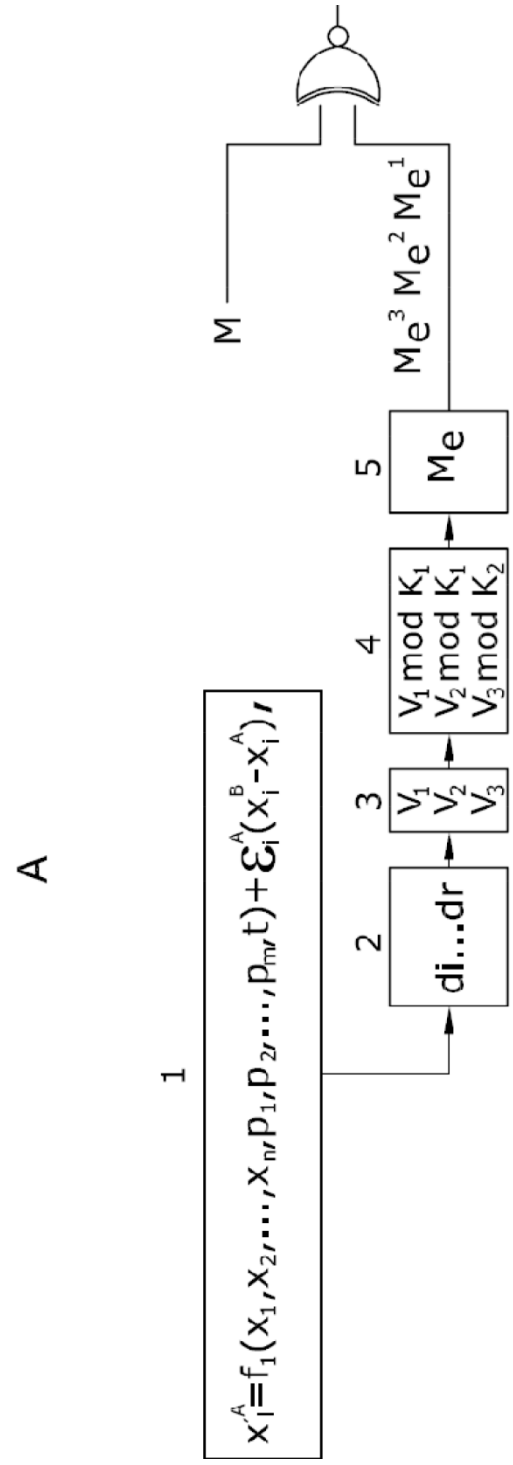
A
1
$x_i^A = f_1(x_1, x_2, \ldots, x_n, p_1, p_2, \ldots, p_m, t) + \varepsilon_i^A(x_i^B - x_i^A)$
2
di...dr
3
V_1
V_2
V_3
4
V_1 mod K_1
V_2 mod K_1
V_3 mod K_2
5
Me
Me^3 Me^2 Me^1
M

FIG.4