(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 848 623**

(21) Número de solicitud: 202130538

(51) Int. CI.:

H04L 9/12 (2006.01)
H04L 9/16 (2006.01)

(12) PATENTE DE INVENCIÓN CON EXAMEN B2

(22) Fecha de presentación:

11.06.2021

(43) Fecha de publicación de la solicitud:

10.08.2021

Fecha de modificación de las reivindicaciones:

08.11.2021

Fecha de concesión:

27.12.2021

(45) Fecha de publicación de la concesión:

04.01.2022

(73) Titular/es:

UNIVERSIDAD POLITÉCNICA DE MADRID (50.0%)
Avda. Ramiro de Maeztu, nº 7
28040 MADRID (Madrid) ES y
SMART HUMAN CAPITAL, S.L. (50.0%)

(72) Inventor/es:

PISARCHIK, Alexander;
MARTÍN PASQUÍN, Fco. Javier y
CHHOLAK, Parth

(74) Agente/Representante:

ELZABURU, S.L.P

(54) Título: **GENERADOR DE SEÑALES PSEUDOALEATORIAS Y SISTEMA DE COMUNICACIONES SEGURAS QUE CONTIENE DICHO GENERADOR**

(57) Resumen:

La presente invención se refiere a un generador de señales pseudoaleatorias y a un sistema de comunicaciones seguras que contiene dicho generador. Tanto el emisor como el receptor del sistema contienen el generador de señales pseudoaleatorias que consiste en un detector de diferencia de fases alimentado por las señales de dos osciladores caóticos acoplados. El cifrado consiste en enmascarar el mensaje o texto plano, dividido en bloques, en la diferencia de fases para conformar el mensaje cifrado que es enviado al receptor mediante el canal de comunicación. El receptor utiliza una misma clave estática que el emisor, para sincronizar sus osciladores con los del emisor mediante un par de claves dinámicas que son generadas y enviadas por el emisor a través de dos canales de sincronización. Por tanto, la diferencia de fases en el receptor será la misma que en el emisor y este será capaz de descifrar el mensaje.

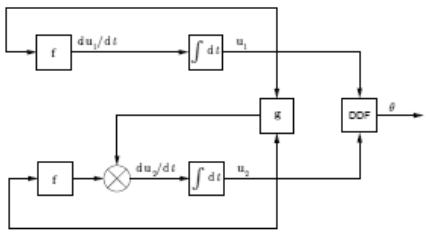

Figura 1

ES 2 848 623 B2

DESCRIPCIÓN

GENERADOR DE SEÑALES PSEUDOALEATORIAS Y SISTEMA DE COMUNICACIONES SEGURAS QUE CONTIENE DICHO GENERADOR

SECTOR DE LA TÉCNICA

La presente invención se enmarca dentro del campo del cifrado de flujos de información en comunicaciones seguras. En concreto, se enmarca dentro del campo de los procedimientos basados en sistemas caóticos.

ANTECEDENTES DE LA INVENCIÓN

En un caso simple de comunicación donde un mensaje se envía desde un emisor hasta un receptor, el mensaje es codificado por el emisor por un procedimiento de tal manera que solo el receptor es capaz de decodificarlo. Al mensaje codificado se le llama mensaje cifrado y es enviado al receptor a través del canal de comunicación. Este mensaje está formado por un flujo de información combinado con una señal de cifrado. Emisor y receptor generan esta señal para el cifrado y descifrado del mensaje, respectivamente.

Utilizar tecnologías de cifrado, autenticación y control de acceso a los sistemas de comunicación segura es una solución adecuada para evitar intentos de espionaje y robo de transmisión de datos. Una contribución para resolver este problema es usar señales generadas por componentes que funcionan en el régimen no lineal, tales como osciladores caóticos. 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 a pequeños cambios en las condiciones iniciales y en los parámetros. En general, los sistemas caóticos muestran repentinos y dramáticos cambios que dan lugar a un comportamiento que describe la evolución temporal no periódica del sistema. Es decir, nunca se repite y aparentemente es aleatoria, pero completamente determinista.

En el estado del arte de sistemas de comunicaciones que usan sistemas caóticos para cifrar información se requiere la transmisión de la clave para el descifrado. Entre las patentes que usan estos métodos podemos mencionar: Bianco US5048086A y Weiss US5479512A, las cuales consisten en generar una secuencia de números aleatorios en formato digital producidos por un sistema caótico, se le adhiere el mensaje a cifrar en formato digital y la señal combinada es transmitida. El receptor extrae el mensaje digital de la señal combinada transmitida usando una clave que genera la misma secuencia de números aleatorios en formato digital, producidos por un sistema caótico. La gran desventaja de este método es la disminución de la seguridad como resultado de transmisión de la clave. Además, este método

dificulta el acceso aleatorio al canal de información, es decir, el receptor debe escuchar el canal desde el inicio de la transmisión por parte del emisor y recuperar el mensaje completo, de lo contrario no podrá acceder siquiera a parte del mensaje que se esté transmitiendo. El acceso aleatorio es necesario para las comunicaciones a tiempo real.

Una forma de resolver este problema usando sistemas caóticos para comunicaciones seguras donde no se requiere la transmisión de la clave se muestra en las patentes de Carroll US5473694A y Cuomo US5291555A. En resumen, describen un método que consiste en modular un parámetro de una señal caótica con una señal que transporta la información o se agrega una señal que lleva información a una señal caótica. La señal caótica resultante se transmite usando tecnologías convencionales de transmisión desde un transmisor que contiene un codificador a un receptor que contiene un decodificador. El decodificador en el receptor sincroniza la señal caótica del receptor con la señal caótica original sin la necesidad de intercambio de claves. La comparación de la señal caótica resultante con la señal sincronizada permite extraer la información original. Además, este método admite el acceso aleatorio al canal de información ya que el receptor puede sincronizarse con el emisor en cualquier instante de la transmisión. Sin embargo, estos sistemas de comunicación segura que usan sincronización presentan una deficiencia, si se intercepta la transmisión, es posible reconstruir el espacio de estado para averiguar la dinámica subyacente del codificador de transmisión permitiendo extraer la señal de información utilizando otro sistema no lineal generador de caos u otra tecnología.

Estos sistemas de comunicación segura basados en sincronización de señales caóticas presentan una debilidad contra ataque por sincronización. Los sistemas de comunicación segura basados en sincronización usan sistemas no lineales caóticos acoplados en configuración maestro-esclavo, donde el maestro representa un emisor y el esclavo un receptor, la señal de salida del emisor es usada para cifrar o enmascarar la señal de información.

El ataque de fuerza bruta por sincronización de estos sistemas de comunicación incluye la intercepción del canal de comunicación y la simulación del receptor por un modelo virtual que ajuste todos los parámetros hasta que se alcance la mejor sincronización o el menor error de sincronización. Cuando el emisor y el receptor virtual alcanzan los mismos valores de parámetros, es cuando se tiene sincronización completa entre estos dos sistemas y la extracción de la señal de información se obtiene comparando la señal sincronizada del receptor virtual con la señal del emisor. Ataques de sincronización en sistemas de comunicación seguros basados en señales caóticas se describe en los siguientes artículos: M. Zanin, R. Sevilla-Escoboza, R. Jaimes-Reátegui, J. García-López, G. Huerta-Cuellar & A. N. Pisarchik, "Synchronization Attack to Chaotic Communication Systems", *Discontinuity, Nonlinearity, and Complexity* vol. 2, 333 (2013); y J. H. García-López, R. Jaimes-Reátegui, R. Chiu-Zarate, D. López-Mancilla, R. Ramírez-Jiménez & A. N. Pisarchik, "Secure Computer Communication Based on Chaotic Rössler Oscillators", *The Open Electrical & Electronic Engineering Journal* vol. 2, 41 (2008).

La sensibilidad de sincronización a cambios de parámetros de los sistemas caóticos es crucial para la seguridad de la comunicación. Una pequeña variación en uno de estos parámetros puede producir un error de sincronización tan grande que la recuperación de la señal de información sea imposible. Así mismo, podemos considerar dos tipos de parámetros: los parámetros relacionados con los sistemas caóticos de emisor y receptor, y el parámetro subyacente al tiempo de sincronización. Siendo el valor umbral de este último parámetro primordial para alcanzar sincronización completa. Para valores inferiores a este tiempo de sincronización, no se alcanza la sincronización completa y la recuperación de la información es imposible.

En la siguiente publicación se resuelve el problema del ataque de sincronización mediante la variación de uno de los parámetros de los osciladores del emisor y el receptor de forma simultánea en intervalos de tiempo menores que el tiempo de sincronización: A. N. Pisarchik, M. Jiménez-Rodríguez & R. Jaimes-Reátegui, "How to Resist Synchronization Attacks", *Discontinuity, Nonlinearity, and Complexity* vol. 4, 1 (2015). Básicamente, el parámetro se varía empleando una función que genera una secuencia de valores a partir de una semilla que compone una clave secreta solo conocida por emisor y receptor, por tanto, solo ellos son capaces de sincronizarse. Un atacante que emplee un sistema virtual para intentar la sincronización con el oscilador del emisor, nunca puede alcanzarla dado que antes de que pueda sondear el valor del parámetro, éste cambia y el atacante debe reanudar el proceso. La desventaja de este método es que elimina la posibilidad del acceso aleatorio al canal de información por parte del receptor. Esto es debido a que el receptor no conoce en que instante se comenzó a generar la secuencia de valores que se emplean para variar el parámetro de los osciladores, de manera que, aunque conozca el valor de la semilla, no conseguirá sincronizarse si no comienza a escuchar el canal comunicación en el instante en que comienza la transmisión.

Las referencias tecnológicas encontradas en el estado del arte se basan en el cifrado en flujo, es decir, en combinar la información con una señal pseudoaleatoria. Esta señal suele ser una de las señales producidas por un oscilador caótico en el emisor que generalmente presenta una alta autocorrelación para incrementos de tiempo moderadamente amplios. Esto se traduce en que pueden existir porciones de información en la señal cifrada que correspondan con valores mas o menos similares de la señal pseudoaleatoria en intervalos de tiempo relativamente pequeños. Este comportamiento conlleva la exposición de parte de la información a ataques estadísticos, lo que redunda en una reducción significativa de la seguridad del cifrado.

EXPLICACIÓN DE LA INVENCIÓN

La presente invención resuelve todos los problemas anteriormente planteados mediante un nuevo sistema de comunicaciones de alta seguridad que cifra el mensaje por bloques empleando un novedoso generador de señales pseudoaleatorias basado en la diferencia de fases entre dos osciladores caóticos.

En recientes estudios se ha detectado que la diferencia de fases entre dos osciladores caóticos en sincronización de fase tiene propiedades similares al ruido como se muestra en: A. N. Pisarchik, G. Huerta-Cuellar & C. W. Kulp, "Statistical Analysis of Symbolic Dynamics in Weakly Coupled Chaotic Oscillators", *Communications in Nonlinear Science and Numerical Simulation* vol. 62, 134 (2018). En este artículo se puede observar que resulta muy difícil realizar una reconstrucción de los atractores caóticos a partir de la diferencia de fases. Además, el grado de autocorrelación de la diferencia de fases en comparación con el de la señal caótica de uno de los osciladores, es menor, con lo que reúne unas características muy interesantes para utilizarse como señal pseudoaleatoria para sistemas de comunicaciones seguras.

Teniendo en cuenta lo anterior, en la presente invención, el emisor y el receptor cuentan con un generador de señales pseudoaleatorias cada uno. Son generadores gemelos y cada uno consta de dos osciladores caóticos acoplados de tal forma que pueden alcanzar la sincronización de fase, y cuyas señales de salida alimentan un detector de diferencia de fases. En el emisor, la señal de salida del detector de diferencia de fases se combina con la señal de información del mensaje en un codificador para obtener la señal cifrada que será enviada al receptor a través del canal de comunicación. En el receptor, esta señal del detector de diferencia de fases se combina con la señal cifrada recibida en un decodificador para extraer la señal de información del mensaje. Para que el receptor pueda descifrar correctamente el mensaje, debe generar la misma señal de salida que el emisor en el detector de diferencia de fases. Esto se logra mediante la implementación de dos canales de sincronización. A través de cada uno de ellos, el emisor envía una señal de cada oscilador caótico al receptor, que emplea estas señales para acoplar sus osciladores con los del emisor con el objetivo de alcanzar la sincronización completa. Cuando el receptor alcanza la sincronización, las señales de sus osciladores con las que alimentan el detector de diferencia de fases son las mismas que generan los osciladores del emisor. Por tanto, el receptor generará la misma señal de diferencia de fases que el emisor y el descifrado será correcto.

Para aumentar la seguridad, la presente invención proporciona un nuevo sistema mediante el cual el mensaje se cifra por bloques. Para ello, el mensaje se divide en bloques de información que se cifran en ciclos consecutivos. Cada ciclo consiste en que el emisor envía un par de señales de sincronización al receptor generadas a partir de unas nuevas condiciones iniciales aleatorias de los osciladores caóticos. A continuación, se deja de enviar estas señales de sincronización y se comienza a generar la señal de diferencia de fases para combinarla con el bloque correspondiente y enviarlo al receptor. De este modo, dado que a cada uno de los bloques le corresponde un par de señales de sincronización distinta, el receptor debe sincronizarse con el emisor para descifrar cada uno de los bloques. Estas señales de sincronización tienen la función de claves dinámicas, son únicas para cada bloque y son públicas.

Para evitar los ataques de sincronización, se implementa una función que emplea un mapa caótico para generar una secuencia ordenada de valores que toma un parámetro de los osciladores caóticos tanto en el emisor como en el receptor. Desde el inicio de la comunicación,

el parámetro de los ociladores cambia su valor en un tiempo menor que el tiempo de sincronización. De modo que las condiciones iniciales y el parámetro de la función forman una clave estática secreta que solo deben conocer emisor y receptor. Este sistema permite que las claves dinámicas sean públicas y que, en un ataque al sistema, no puedan ser utilizadas para desencriptar los bloques del mensaje. Además, la secuencia de valores del parámetro generada por el mapa caótico se repite para cada bloque del mensaje, lo que resuelve el problema de acceso aleatorio, es decir, si el receptor empieza a escuchar el canal de comunicaciones en un instante posterior al inicio de la transmisión por parte del emisor, el primero podrá descifrar los bloques posteriores al comienzo de la escucha. Otra característica importante del sistema debida a su especial diseño, es que permite su implementación en paralelo lo cual es importante a la hora de integrarlo en arquitecturas de computadores con varios núcleos de procesamiento.

Generador de señales pseudoaleatorias (figura 1)

La invención comprende un generador de señales pseudoaleatorias que está presente tanto en el transmisor como en el receptor. Este generador de señales es una de las reivindicaciones de la presente invención y comprende dos osciladores caóticos con un acoplamiento, que les permite alcanzar la sincronización de fase, y un detector de diferencia de fases.

En una realización preferente, el generador de señales pseudoaleatorias, (figura1), comprende un sistema de ecuaciones diferenciales que representan la dinámica de los osciladores caóticos a lo largo del tiempo:

$$\frac{\mathrm{d}\mathbf{u}_1}{\mathrm{d}t} = \mathbf{f}(\mathbf{u}_1),$$
$$\frac{\mathrm{d}\mathbf{u}_2}{\mathrm{d}t} = \mathbf{f}(\mathbf{u}_2) + \mathbf{g}(\mathbf{u}_1, \mathbf{u}_2),$$

donde los estados iniciales son diferentes, $\mathbf{u}_1(t_0) \neq \mathbf{u}_2(t_0)$. Para simplificar, consideramos que ambos osciladores son idénticos en configuración maestro-esclavo, de tal forma que $\mathbf{f} : \mathbb{R}^d \to \mathbb{R}^d$ describe las derivadas temporales de las variables de estado de cada uno de los osciladores aislados y $\mathbf{g} : \mathbb{R}^{2d} \to \mathbb{R}^d$ representa la función de acoplamiento que permite a los osciladores alcanzar la sincronización de fase, siendo d el grado de libertad del sistema. En una realización particular, para el caso $d = 3$, las variables de estado del oscilador maestro pueden ser representadas por el vector de estado $\mathbf{u}_1(t) = [x_1(t), y_1(t), z_1(t)]^\intercal$, y las del oscilador esclavo por $\mathbf{u}_2(t) = [x_2(t), y_2(t), z_2(t)]^\intercal$. Las variables de estado representan las señales que generan los osciladores. La diferencia de fases entre ambos osciladores $\theta(t) = \phi_2(t) - \phi_1(t)$ es una señal pseudoaleatoria, siendo $\phi_1(t)$ y $\phi_2(t)$ las fases absolutas del oscilador maestro y del esclavo respecto a un instante de referencia t_{ref} las cuales pueden ser obtenidas a partir de los vectores de estado $\mathbf{u}_1(t)$ y $\mathbf{u}_2(t)$ mediante una transformación convencional realizada en el detector de diferencia de fases. Además, si se elige que los estados iniciales sean aleatorios, entonces, la diferencia de fases representa una señal

aleatoria.

Sistema de cifrado en bloques (figura 2)

La finalidad del sistema de comunicaciones seguras es poder enviar un mensaje cifrado desde el emisor (10) al receptor (20) mediante el enmascaramiento del mensaje o texto plano $m(\tau)$ en una señal aleatoria $r_{\mathrm{E}}(t)$ generada en el emisor. Solo el receptor tienen la capacidad de reproducir esta señal y, por tanto, de separar el texto plano del mensaje cifrado debido a que puede sincronizarse con el emisor. El mensaje (o texto plano) consiste una señal que podemos dividir en M bloques contiguos $m_i(\tau)$ para $\tau_{i-1} < \tau \leq \tau_i$ e $i = 1, \ldots, M$, siendo $m(\tau) = \bigcup_i m_i(\tau)$ el mensaje completo que se desea transmitir y $\Delta\tau_{\mathrm{info}} = \tau_i - \tau_{i-1}$ la duración del los bloques.

Definimos i-ésimo ciclo como el intervalo temporal durante el cual se envían las claves dinámicas y el bloque $m_i(\tau)$ cifrado. Un ciclo comienza en t_0^i, termina en t_{fin}^i y se divide en dos intervalos:

- El intervalo asíncrono cuya duración es $\Delta t_{\mathrm{asinc}} = t_{\mathrm{ref}}^i - t_0^i$ y es lo suficientemente amplio como para que los osciladores del emisor se sincronicen completamente con los del receptor. En t_0^i se generan nuevos estados iniciales aleatorios para el emisor mediante una fuente de entropía (9) y, a continuación, comienza el envío de las claves dinámicas hasta alcanzar instante t_{ref}^i.
- El intervalo sincronizado cuya duración es $\Delta t_{\mathrm{sinc}} = t_{\mathrm{fin}}^i - t_{\mathrm{ref}}^i$ y, durante el cual, se cifra, se envía y se descifra el bloque $m_i(\tau)$, por lo que se hace necesario que se cumpla que $\Delta t_{\mathrm{sinc}} \geq \Delta\tau_{\mathrm{info}}$. El intervalo comienza en t_{ref}^i que es el instante de referencia para la diferencia de fases tanto en el emisor como en el receptor.

La duración total de un ciclo es la suma de las duraciones de los intervalos anteriores, esto es, $\Delta t_{\mathrm{ciclo}} = \Delta t_{\mathrm{asinc}} + \Delta t_{\mathrm{sinc}}$. Entonces, para el envío del mensaje completo se emplean M ciclos consecutivos y se necesita un tiempo total de $M\Delta t_{\mathrm{ciclo}}$ (en la figura 3 muestra las señales del sistema en dos ciclos consecutivos).

Llamamos cifrado al procedimiento que consiste en enmascarar cada uno de los bloques $m_i(\tau)$ en la diferencia de fases $\theta_{\mathrm{E}}^i(t)$ producida en el emisor, y que da lugar a la señal cifrada $s(t) = m_{\mathrm{E}}(t) + r_{\mathrm{E}}(t)$ que se envía al receptor a través del canal de comunicación (22), donde

$$m_{\mathrm{E}}(t) = \begin{cases} m_i(\tau) & \text{si } t_{\mathrm{ref}}^i < t \leq t_{\mathrm{fin}}^i \\ \emptyset & \text{en otro caso,} \end{cases} \quad \text{y} \quad r_{\mathrm{E}}(t) = \begin{cases} \theta_{\mathrm{E}}^i(t) & \text{si } t_{\mathrm{ref}}^i < t \leq t_{\mathrm{fin}}^i \\ \emptyset & \text{en otro caso,} \end{cases}$$

siendo $m_{\mathrm{E}}(t)$ la señal de información, que es generada por un búfer de entrada (6), y $r_{\mathrm{E}}(t)$ la señal aleatoria generada en el emisor, según fue comentado.

En una realización preferente, el generador de señales pseudoaleatorias del emisor (5) com-

prende el sistema ecuaciones diferenciales que representan la dinámica de los osciladores caóticos a lo largo del tiempo $t \in \left[t_0^i, t_{\text{fin}}^i\right]$

$$\frac{\mathrm{d}\mathbf{u}_{\mathrm{E1}}^i}{\mathrm{d}t} = \mathbf{f}(\mathbf{u}_{\mathrm{E1}}^i; c), \quad [1]$$

$$\frac{\mathrm{d}\mathbf{u}_{\mathrm{E2}}^i}{\mathrm{d}t} = \mathbf{f}(\mathbf{u}_{\mathrm{E2}}^i; c) + \mathbf{g}(y_{\mathrm{E1}}^i, y_{\mathrm{E2}}^i), \quad [2]$$

los estados iniciales $\mathbf{u}_{\mathrm{E1}}^i(t_0^i) \neq \mathbf{u}_{\mathrm{E2}}^i(t_0^i)$ y un detector de diferencia de fases (14), donde c es un parámetro de los osciladores caóticos que puede ser ajustado, según se comenta más adelante. En esta realización, se acoplan los osciladores empelando únicamente la variable de estado y_{E1}^i.

Sistema de descifrado

Llamamos descifrado al procedimiento que ocurre en el receptor (20) y que consiste en sustraer cada uno de los bloques $m_i(\tau)$ de la señal cifrada $s(t)$. Este proceso solo es posible si, durante el intervalo sincronizado, el receptor es capaz de generar una diferencia de fases $\theta_{\mathrm{R}}^i(t)$ que sea la misma diferencia $\theta_{\mathrm{E}}^i(t)$ que se genera en el emisor (10), y que de lugar a la señal de información recuperada en el receptor $m_{\mathrm{R}}(t) = s(t) - r_{\mathrm{R}}(t)$. En consecuencia, se tiene que cumplir que $r_{\mathrm{R}}(t) = r_{\mathrm{E}}(t)$, donde

$$r_{\mathrm{R}}(t) = \begin{cases} \theta_{\mathrm{R}}^i(t) & \text{si } t_{\text{ref}}^i < t \leq t_{\text{fin}}^i \\ \emptyset & \text{en otro caso} \end{cases}$$

es la señal aleatoria reproducida en el receptor gracias a la sincronización entre emisor y receptor.

Con el objetivo de evitar distintos ataques basados en criptoanálisis, se impone que los estados iniciales $\mathbf{u}_{\mathrm{E1}}^i(t_0^i)$ y $\mathbf{u}_{\mathrm{E2}}^i(t_0^i)$ en el emisor sean aleatorios. Por tanto, para que se cumpla la condición $r_{\mathrm{R}}(t) = r_{\mathrm{E}}(t)$, el emisor envía, además de la señal cifrada, dos señales de sincronización, $s_1(t)$ y $s_2(t)$, que contienen las claves dinámicas. Este procedimiento consiste en enviar dos variables de estado del emisor, una de las variables del oscilador maestro y otra del oscilador esclavo, a través de dos canales de sincronización (23, 24). Una vez en el receptor, estas señales se emplean para acoplar los osciladores maestros y los osciladores esclavos durante el intervalo asíncrono, cuya duración debe ser suficiente para que alcancen la sincronización completa.

En la realización anterior, en la que los osciladores del emisor (1, 2) están representados por las ecuaciones [1] y [2], el generador de señales pseudoaleatorias del receptor (15) comprende el sistema ecuaciones diferenciales que representan la dinámica de los osciladores

caóticos a lo largo del tiempo $t \in [t'_0, t'_{\text{fin}}]$

$$\frac{\mathrm{d}\mathbf{u}_{\mathrm{R1}}}{\mathrm{d}t} = \mathbf{f}(\mathbf{u}_{\mathrm{R1}}; c) + \mathbf{h}(s_1, x_{\mathrm{R1}}; \kappa),$$
$$\frac{\mathrm{d}\mathbf{u}_{\mathrm{R2}}}{\mathrm{d}t} = \mathbf{f}(\mathbf{u}_{\mathrm{R2}}; c) + \mathbf{g}(y_{\mathrm{R1}}, y_{\mathrm{R2}}) + \mathbf{h}(s_2, x_{\mathrm{R2}}; \kappa),$$

siendo los estados iniciales $\mathbf{u}_{\mathrm{R1}}(t'_0)$ y $\mathbf{u}_{\mathrm{R2}}(t'_0)$ arbitrarios. Además, el receptor (15) comprende un detector de diferencia de fases. La función $\mathbf{h} : \mathbb{R}^{2d} \to \mathbb{R}^d$ representa el acoplamiento (19, 21) entre los osciladores del emisor y el receptor, y κ es el parámetro de fuerza de acoplamiento que toma el valor necesario para que se produzca la sincronización completa durante el intervalo asíncrono, es decir, cuando $s_1(t) \neq \emptyset$ y $s_2(t) \neq \emptyset$, siendo nulo en cualquier otro caso.

Entonces, en la misma realización preferente, las señales de sincronización consiste en

$$s_1(t) = \begin{cases} x^i_{\mathrm{E1}}(t) & \text{si } t^i_0 < t \leq t^i_{\mathrm{ref}} \\ \emptyset & \text{en otro caso,} \end{cases} \quad \text{y} \quad s_2(t) = \begin{cases} x^i_{\mathrm{E2}}(t) & \text{si } t^i_0 < t \leq t^i_{\mathrm{ref}} \\ \emptyset & \text{en otro caso,} \end{cases}$$

En ambos casos, por seguridad, se evita enviar las condiciones iniciales $x^i_{\mathrm{E1}}(t^i_0)$ y $x^i_{\mathrm{E2}}(t^i_0)$.

El sistema permite el acceso aleatorio a los canales (22, 23, 24) de manera que si $t'_0 \leq t^1_0$ y $t'_{\text{fin}} \geq t^M_{\text{fin}}$, el receptor puede acceder al mensaje completo $m(\tau)$. Si por el contrario, $t'_0 > t^1_0$ y/o $t'_{\text{fin}} < t^M_{\text{fin}}$, el receptor aún puede descifrar algunos bloques y, por tanto, acceder a una parte del mensaje dependiendo del tiempo durante el cual accede a los canales. En cualquier caso, si $r_{\mathrm{R}}(t) = r_{\mathrm{E}}(t)$, la señal de información recuperada en el decodificador es

$$m_{\mathrm{R}}(t) = s(t) - r_{\mathrm{R}}(t) = \begin{cases} m_i(\tau) & \text{si } t^i_{\mathrm{ref}} < t \leq t^i_{\text{fin}} \\ \emptyset & \text{en otro caso.} \end{cases}$$

El búfer de salida (16) se en carga de concatenar los bloques $m_i(\tau)$ que forman el mensaje descifrado.

Protección contra ataques de sincronización

Para evitar el ataque de sincronización, tanto el emisor (10) como el receptor (20) cuentan con un generador del parámetro c (8, 18) basado en un mapa caótico discreto. Este dispositivo cambia el valor del parámetro de los osciladores caóticos en intervalos de tiempo fijos Δt_c mucho menores que el tiempo que necesitaría un atacante para la sincronización completa si tuviese acceso a los canales de sincronización, es decir, $\Delta t_c \ll \Delta t_{\mathrm{asinc}}$. De modo que, si dividimos el intervalo de tiempo para el i-ésimo ciclo en N subintervalos, tal que $\Delta t_{\mathrm{ciclo}} = N\Delta t_c$, a cada subintervalo, desde $n = 0$ hasta $n = N - 1$, le corresponde un valor de c que se obtiene mediante la función $c_{n+1} = \varphi(c_n, v_{n+1}; \rho)$, donde v_n es el n-ésimo valor de un

mapa caótico y ρ un parámetro del mismo que forma parte de la clave estática del sistema. Así mismo, los valores iniciales c_0 y v_0, también son parte de la clave estática. La función φ produce una secuencia de N valores de c acotados de manera que los osciladores conservan siempre su comportamiento caótico.

BREVE DESCRIPCIÓN DE LAS FIGURAS

Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión de las características de la invención, de acuerdo con un ejemplo preferente de realización práctica de la misma, se acompaña como parte integrante de dicha descripción, un juego de figuras en donde con carácter ilustrativo y no limitativo, se ha representado lo siguiente:

Figura 1: Diagrama del generador de señales pseudoaleatorias en el que los osciladores caóticos son idénticos y están acoplados en configuración maestro-esclavo.

Figura 2: Diagrama del sistema de comunicaciones seguras basado en enmascaramiento mediante el desfase entre osciladores caóticos.

Figura 3: Representa las series temporales para los dos primeros ciclos de cifrado del la imagen de la figura 4: (a) y (b) señales de sincronización, (c) señal aleatoria generada en el emisor y el receptor, (d) señal cifrada y (e) señal de información recuperada en el receptor.

Figura 4: Imagen de una persona que es empleada como mensaje en la realización preferente para una demostración del cifrado.

Figura 5: Resultado del cifrado de la imagen de la figura 4 en la realización preferente.

Figura 6: Desviación típica de los bits que componen los números de coma flotante de una secuencia de números aleatorios obtenida del generador de señales pseudoaleatorias del emisor. El bit menos significativo se corresponde con la posición 1.

REALIZACIÓN PREFERENTE DE LA INVENCIÓN

La implementación de la presente invención está directamente relacionada con el campo de los sistemas de comunicación segura, dispositivos electrónicos analógicos y digitales y programas de computador, más específicamente se refiere a un sistema de comunicación altamente segura basada en sistemas caóticos. Adicionalmente, la presente invención puede ser implementada en circuitos electrónicos como en sistemas de comunicación inalámbricas.

La presente invención se ilustra adicionalmente mediante el siguiente ejemplo de aplicación, el cual no pretenden ser limitativo de su alcance. En este ejemplo de aplicación se desarrolla un método computacional para la implementación de la invención mediante software, hardwa-

re o una mezcla de ambos. Para ello, se establece un discretización del dominio del tiempo t de tal forma que $t_j = t_0 + jh$ con $j = 0, 1, \ldots$ y $t_0 = 0$ son los instantes de una discretización equiespaciada con paso de tiempo $h = 0.1$.

Esta realización implementa la invención empleando osciladores de Rössler idénticos como osciladores caóticos en los generadores de señales pseudoaleatorias. Además, se emplea el mapa logístico como mapa caótico para su implementación en los generadores (8, 18) del parámetro c.

Osciladores caóticos del emisor

En esta realización preferente, la pareja de osciladores caóticos (1, 2) del generador de señales pseudoaleatorias del emisor (5) consiste en los osciladores de Rössler idénticos con acoplamiento (3) difusivo representados por las ecuaciones diferenciales que describen su dinámica a lo largo del tiempo $t \in \left[t_0^i, t_{\text{fin}}^i\right]$

$$\begin{aligned} \frac{\mathrm{d}x_{\mathrm{E1}}^i}{\mathrm{d}t} &= -y_{\mathrm{E1}}^i - z_{\mathrm{E1}}^i, \\ \frac{\mathrm{d}y_{\mathrm{E1}}^i}{\mathrm{d}t} &= x_{\mathrm{E1}}^i + a\, y_{\mathrm{E1}}^i, \\ \frac{\mathrm{d}z_{\mathrm{E1}}^i}{\mathrm{d}t} &= b + z_{\mathrm{E1}}^i (x_{\mathrm{E1}}^i - c), \end{aligned} \qquad [3]$$

$$\begin{aligned} \frac{\mathrm{d}x_{\mathrm{E2}}^i}{\mathrm{d}t} &= -y_{\mathrm{E2}}^i - z_{\mathrm{E2}}^i, \\ \frac{\mathrm{d}y_{\mathrm{E2}}^i}{\mathrm{d}t} &= x_{\mathrm{E2}}^i + a\, y_{\mathrm{E2}}^i + \kappa' \left(y_{\mathrm{E1}}^i - y_{\mathrm{E2}}^i\right), \\ \frac{\mathrm{d}z_{\mathrm{E2}}^i}{\mathrm{d}t} &= b + z_{\mathrm{E2}}^i (x_{\mathrm{E2}}^i - c), \end{aligned} \qquad [4]$$

donde $a = 1.65$ y $b = 0.2$ son parámetros fijos de los osciladores, mientras que c es un parámetro ajustable que mantiene el comportamiento caótico de los osciladores si toma valores en el intervalo $[8.5, 12]$. El sistema de ecuaciones [3] corresponde al oscilador maestro (1) y el sistema [4] al esclavo (2). Para que los osciladores alcancen la sincronización de fase de forma intermitente, se fija el parámetro de fuerza de acoplamiento $\kappa' = 0.001$. Los estados iniciales $\mathbf{u}_{\mathrm{E1}}^i(t_0^i) \neq \mathbf{u}_{\mathrm{E2}}^i(t_0^i)$ son aleatorios, de forma que cada una de las condiciones iniciales se obtiene a partir de una distribución uniforme $\mathcal{U}(0, 1)$ que emplea la fuente de entropía (9).

Llamamos serie temporal a los valores que toma una variable del sistema en los instantes de una discretización del dominio del tiempo como la anteriormente descrita. Con el objetivo de obtener las series temporales de las variables de estado de los osciladores de Rössler, se emplea un esquema de integración numérica para problemas de valor inicial. En esta realización se emplea un esquema Runge-Kutta de cuarto orden. Estos esquemas proporcionan una aproximación de la variable en el instante calculado, de modo que $\mathbf{u}_{\mathrm{E1}}^i(t_j) \approx {\mathbf{u}_{\mathrm{E1}}^i}^{(j)}$ y $\mathbf{u}_{\mathrm{E2}}^i(t_j) \approx {\mathbf{u}_{\mathrm{E2}}^i}^{(j)}$, donde

$${\mathbf{u}_{\mathrm{E1}}^i}^{(j)} = \begin{pmatrix} {x_{\mathrm{E1}}^i}^{(j)} \\ {y_{\mathrm{E1}}^i}^{(j)} \\ {z_{\mathrm{E1}}^i}^{(j)} \end{pmatrix} \quad \text{y} \quad {\mathbf{u}_{\mathrm{E2}}^i}^{(j)} = \begin{pmatrix} {x_{\mathrm{E2}}^i}^{(j)} \\ {y_{\mathrm{E2}}^i}^{(j)} \\ {z_{\mathrm{E2}}^i}^{(j)} \end{pmatrix}$$

son una aproximación de los vectores de estado de los osciladores maestro y esclavo res-

pectivamente en el instante t_j, obtenidos a partir del esquema de integración numérica.

Osciladores caóticos del receptor

En esta realización preferente, la pareja osciladores de Rössler idénticos del receptor con acoplamiento (13) difusivo viene representada por las ecuaciones diferenciales que describen su dinámica a lo largo del tiempo $t \in [t'_0, t'_{\text{fin}}]$

$$\begin{aligned} \frac{\mathrm{d}x_{\mathrm{R1}}}{\mathrm{d}t} &= -y_{\mathrm{R1}} - z_{\mathrm{R1}} + \kappa\,(s_1 - x_{\mathrm{R1}}), \\ \frac{\mathrm{d}y_{\mathrm{R1}}}{\mathrm{d}t} &= x_{\mathrm{R1}} + a\,y_{\mathrm{R1}}, \\ \frac{\mathrm{d}z_{\mathrm{R1}}}{\mathrm{d}t} &= b + z_{\mathrm{R1}}(x_{\mathrm{R1}} - c), \end{aligned} \qquad [5]$$

$$\begin{aligned} \frac{\mathrm{d}x_{\mathrm{R2}}}{\mathrm{d}t} &= -y_{\mathrm{R2}} - z_{\mathrm{R2}} + \kappa\,(s_2 - x_{\mathrm{R2}}), \\ \frac{\mathrm{d}y_{\mathrm{R2}}}{\mathrm{d}t} &= x_{\mathrm{R2}} + a\,y_{\mathrm{R2}} + \kappa'(y_{\mathrm{R1}} - y_{\mathrm{R2}}), \\ \frac{\mathrm{d}z_{\mathrm{R2}}}{\mathrm{d}t} &= b + z_{\mathrm{R2}}(x_{\mathrm{R2}} - c), \end{aligned} \qquad [6]$$

donde los parámetros a, b, c y κ' toman los mismos valores que en las ecuaciones del emisor. El sistema de ecuaciones [5] corresponde al oscilador maestro (11) y el sistema [6] al esclavo (12). Los estados iniciales toman los valores arbitrarios $\mathbf{u}_{\mathrm{R1}}(t'_0) = \mathbf{u}_{\mathrm{R2}}(t'_0) = [0,0,0]^{\mathsf{T}}$. El parámetro de fuerza de acoplamiento κ toma los siguientes valores

$$\kappa = \begin{cases} 1.75 & \text{si } s_1(t_j) \neq \emptyset \text{ y } s_2(t_j) \neq \emptyset \\ 0 & \text{en otro caso,} \end{cases}$$

de tal forma que 1.75 es el valor con el que emisor y receptor alcanzan la sincronización completa durante el intervalo asíncrono, esto es, al integrar los sistemas [5] y [6] producirán las mismas series temporales durante el intervalo sincronizado que los sistemas de ecuaciones del emisor [3] y [4] respectivamente. El esquema de integración numérica que se emplea para obtener las series temporales es el mismo que se utiliza para integrar las ecuaciones del emisor, de modo que $\mathbf{u}_{\mathrm{R1}}(t_j) \approx \mathbf{u}_{\mathrm{R1}}{}^{(j)}$ y $\mathbf{u}_{\mathrm{R2}}(t_j) \approx \mathbf{u}_{\mathrm{R2}}{}^{(j)}$, donde

$$\mathbf{u}_{\mathrm{R1}}{}^{(j)} = \begin{pmatrix} x_{\mathrm{R1}}{}^{(j)} \\ y_{\mathrm{R1}}{}^{(j)} \\ z_{\mathrm{R1}}{}^{(j)} \end{pmatrix} \quad \text{y} \quad \mathbf{u}_{\mathrm{R2}}{}^{(j)} = \begin{pmatrix} x_{\mathrm{R2}}{}^{(j)} \\ y_{\mathrm{R2}}{}^{(j)} \\ z_{\mathrm{R2}}{}^{(j)} \end{pmatrix}$$

son una aproximación de los vectores de estado de los osciladores maestro y esclavo respectivamente en el instante t_j, obtenidos a partir del esquema.

Detector de diferencia de fases

Tanto emisor como receptor poseen un detector de diferencia de fases (4, 14) que forma parte de sus generadores de señales pseudoaleatorias. A continuación, se detalla la implementación de estos detectores empleando las series temporales generadas al integrar numéricamente las ecuaciones de los osciladores caóticos.

La representación de un oscilador de Rössler en el espacio de estados es un atractor caótico de tipo espiral. El cálculo de la fase relativa en un instante t_j se puede realizar midiendo la fase de un vector que sigue la trayectoria proyectada del atractor en el plano XY. De modo que las fases relativas de cada oscilador en el instante t_j se pueden aproximar por

$$\alpha_{\mathrm{E1}}^{i}{}^{(j)} = \operatorname{atan}\frac{y_{\mathrm{E1}}^{i}{}^{(j)} - y^*}{x_{\mathrm{E1}}^{i}{}^{(j)} - x^*}, \qquad \alpha_{\mathrm{E2}}^{i}{}^{(j)} = \operatorname{atan}\frac{y_{\mathrm{E2}}^{i}{}^{(j)} - y^*}{x_{\mathrm{E2}}^{i}{}^{(j)} - x^*},$$
$$\alpha_{\mathrm{R1}}{}^{(j)} = \operatorname{atan}\frac{y_{\mathrm{R1}}{}^{(j)} - y^*}{x_{\mathrm{R1}}{}^{(j)} - x^*}, \qquad \alpha_{\mathrm{R2}}{}^{(j)} = \operatorname{atan}\frac{y_{\mathrm{R2}}{}^{(j)} - y^*}{x_{\mathrm{R2}}{}^{(j)} - x^*},$$

donde $x^* = \frac{1}{2}\left(c - \sqrt{c^2 - 4ab}\right)$ e $y^* = -c + \frac{1}{2a}\sqrt{c^2 - 4ab}$ son las coordenadas de los centros de los atractores que depende de c.

Entonces, la diferencia de fases absolutas se pueden aproximar en el instante t_j mediante las expresiones

$$\theta_{\mathrm{E}}^{i}{}^{(j)} = \phi_{\mathrm{E2}}^{i}{}^{(j)} - \phi_{\mathrm{E1}}^{i}{}^{(j)} = 2\pi\left(k_{\mathrm{E2}}^{i}{}^{(j)} - k_{\mathrm{E1}}^{i}{}^{(j)}\right) + \alpha_{\mathrm{E2}}^{i}{}^{(j)} - \alpha_{\mathrm{E1}}^{i}{}^{(j)},$$
$$\theta_{\mathrm{R}}^{i}{}^{(j)} = \phi_{\mathrm{R2}}^{i}{}^{(j)} - \phi_{\mathrm{R1}}^{i}{}^{(j)} = 2\pi\left(k_{\mathrm{R2}}^{i}{}^{(j)} - k_{\mathrm{R1}}^{i}{}^{(j)}\right) + \alpha_{\mathrm{R2}}{}^{(j)} - \alpha_{\mathrm{R1}}{}^{(j)},$$

siendo $k_{\mathrm{E1}}^{i}{}^{(j)}$, $k_{\mathrm{E2}}^{i}{}^{(j)}$, $k_{\mathrm{R1}}^{i}{}^{(j)}$ y $k_{\mathrm{R2}}^{i}{}^{(j)}$ el número entero de ciclos de cada oscilador desde el instante de referencia t_{ref}^{i} hasta el instante t_j. De manera que, la diferencia de vueltas entre la pareja de osciladores del emisor, puede contabilizarse como

$$\Delta k_{\mathrm{E}}^{i}{}^{(j)} = k_{\mathrm{E2}}^{i}{}^{(j)} - k_{\mathrm{E1}}^{i}{}^{(j)} = \begin{cases} 0 & \text{si } t_j = t_{\mathrm{ref}}^{i}, \\ \Delta k_{\mathrm{E}}^{i}{}^{(j-1)} + 1 & \text{si } \alpha_{\mathrm{E2}}^{i}{}^{(j)} < 0 \ \wedge \ \alpha_{\mathrm{E2}}^{i}{}^{(j-1)} > 0, \\ \Delta k_{\mathrm{E}}^{i}{}^{(j-1)} - 1 & \text{si } \alpha_{\mathrm{E1}}^{i}{}^{(j)} < 0 \ \wedge \ \alpha_{\mathrm{E1}}^{i}{}^{(j-1)} > 0, \\ \Delta k_{\mathrm{E}}^{i}{}^{(j-1)} & \text{en otro caso.} \end{cases}$$

Del mismo modo, para el receptor se tiene que

$$\Delta k_{\mathrm{R}}^{i}{}^{(j)} = k_{\mathrm{R2}}^{i}{}^{(j)} - k_{\mathrm{R1}}^{i}{}^{(j)} = \begin{cases} 0 & \text{si } t_j = t_{\mathrm{ref}}^{i}, \\ \Delta k_{\mathrm{R}}^{i}{}^{(j-1)} + 1 & \text{si } \alpha_{\mathrm{R2}}{}^{(j)} < 0 \ \wedge \ \alpha_{\mathrm{R2}}{}^{(j-1)} > 0, \\ \Delta k_{\mathrm{R}}^{i}{}^{(j-1)} - 1 & \text{si } \alpha_{\mathrm{R1}}{}^{(j)} < 0 \ \wedge \ \alpha_{\mathrm{R1}}{}^{(j-1)} > 0, \\ \Delta k_{\mathrm{R}}^{i}{}^{(j-1)} & \text{en otro caso.} \end{cases}$$

Sincronización emisor-receptor

Teniendo en cuenta todo lo anterior, las señales de sincronización consisten en

$$s_1(t_j) = \begin{cases} x_{\mathrm{E1}}^{i\ (j)} & \text{si } t_0^i < t_j \leq t_{\mathrm{ref}}^i \\ \emptyset & \text{en otro caso,} \end{cases} \quad \text{y} \quad s_2(t_j) = \begin{cases} x_{\mathrm{E2}}^{i\ (j)} & \text{si } t_0^i < t_j \leq t_{\mathrm{ref}}^i \\ \emptyset & \text{en otro caso.} \end{cases}$$

En ambas señales se evita enviar el valor de las condiciones iniciales aleatorias $x_{\mathrm{E1}}^i(t_0^i)$ y $x_{\mathrm{E2}}^i(t_0^i)$. Esta situación permite que los ciclos de cifrado se puedan concatenar de forma que el instante final de cada uno de ellos coincida con el instante inicial del siguiente, es decir, $t_{\mathrm{fin}}^i = t_0^{i+1}$. En la figura 3 se muestran las dos señales de sincronización para los dos primeros ciclos del cifrado de la imagen de la figura 4.

La sincronización entre emisor y receptor se alcanza cuando $\left|\theta_{\mathrm{E}}^{i\ (j)} - \theta_{\mathrm{R}}^{i\ (j)}\right| < \epsilon$ para todo $t_j \in \left(t_{\mathrm{ref}}^i, t_{\mathrm{fin}}^i\right]$, donde ϵ representa el error de máquina que depende de la arquitectura de computación.

Generador del parámetro c de los osciladores caóticos

Tanto emisor como receptor poseen un generador del parámetro c (8, 18). En esta realización, se emplea el mapa logístico $v_{n+1} = \rho\, v_n(1 - v_n)$ con parámetro ρ y condición inicial v_0 de manera que ambos parte de la clave estática. En esta realización del sistema, el parámetro c cambia en cada paso de integración, luego $\Delta t_c = h = 0.1$ y $c = c^{(j)}$ para $t_{j-1} < t \leq t_j$ y $t_j > t_0^1$. Para que los osciladores del emisor y el receptor conserven su comportamiento caótico, c debe estar contenido en el intervalo $[8.5, 12]$. Entonces, en esta realización preferente, la secuencia de valores del parámetro c que conforma la salida del generador viene descrita por

$$c_{n+1} = \begin{cases} c_n + v_{n+1} & \text{si } c_n + v_{n+1} \leq 12 \\ 8.5 + \mathrm{mód}(c_n + v_{n+1}, 12) & \text{en otro caso.} \end{cases}$$

donde $n = 0, 1, \ldots$ y $c_0 \in [8.5, 12]$ es la condición inicial del generador que también forma parte de la clave estática. Para que el sistema conserve la propiedad de acceso aleatorio, este procedimiento se reinicia para cada ciclo de cifrado/descifrado, esto es, $c^{(j)} = c_1$ si $t_j = t_0^i + h$ y, en consecuencia, $c^{(j+n)} = c_{n+1}$ para los sucesivos pasos de integración del i-ésimo ciclo.

Cifrado y descifrado de una imagen

Como ejemplo, se utiliza una imagen de una persona (figura 4) de 512×512 pixeles como mensaje o texto plano. Cada pixel está representado por 24 bits, 8 bits para representar la intensidad de cada uno de los tres colores: rojo (R), verde (G) y azul (B). Para enviar el

mensaje, se reordenan los bits de cada pixel de la imagen en un vector de la siguiente forma:

$$m = [R_{1,1}, G_{1,1}, B_{1,1}, \ldots, R_{1,512}, G_{1,512}, B_{1,512}, \ldots, R_{512,512}, G_{512,512}, B_{512,512}],$$

donde los subíndices de cada color indican la posición del pixel al que corresponden en unos ejes cartesianos. Por tanto, el mensaje m contiene un total de $512 \times 512 \times 24 = 6291456$ bits.

La señal aleatoria en el emisor es la secuencia de bits aleatorios

$$r_{\mathrm{E}}(t_j) = \begin{cases} {\theta_{\mathrm{E}}^{i}}^{(j)} & \text{si } t_{\mathrm{ref}}^{i} < t_j \leq t_{\mathrm{fin}}^{i} \\ \emptyset & \text{en otro caso,} \end{cases}$$

y, del mismo modo, el receptor reproduce la señal aleatoria

$$r_{\mathrm{R}}(t_j) = \begin{cases} {\theta_{\mathrm{R}}^{i}}^{(j)} & \text{si } t_{\mathrm{ref}}^{i} < t_j \leq t_{\mathrm{fin}}^{i} \\ \emptyset & \text{en otro caso.} \end{cases}$$

En la figura 3 se puede observar que las señales $r_{\mathrm{E}}(t_j)$ y $r_{\mathrm{R}}(t_j)$ coinciden. Esto es debido a que emisor y receptor emplean los mismos valores de clave estática que se muestran en la tabla 1, lo que provoca que puedan sincronizar sus osciladores.

Como se desea descifrar el mensaje completo, se supone que el receptor comienza a escuchar los canales en el mismo instante que el emisor comienza a generar las claves dinámicas del primer bloque. Entonces, por convenio se establece que $t'_0 = t_0^1 = t_0 = 0$.

Una cota superior del tiempo necesario para la sincronización completa entre los osciladores de Rössler del emisor y el receptor es $\Delta t_{\mathrm{asinc}} = 100$ unidades de tiempo, o lo que es lo mismo, se necesitan 10^3 iteraciones del esquema de integración en el emisor y el receptor. Luego, el tiempo de referencia para el cálculo de ${\theta_{\mathrm{E}}^{i}}^{(j)}$ y ${\theta_{\mathrm{R}}^{i}}^{(j)}$ es $t_{\mathrm{ref}}^{i} = t_0^i + 100$.

Para una arquitectura de 64 bits y aritmética de coma flotante, se puede analizar que bits sufren cambios con mas frecuencia en una secuencia de números aleatorios correspondiente a ${\theta_{\mathrm{E}}^{i}}^{(j)}$ midiendo la desviación típica de la representación de los números en código binario. En la figura 6 se puede observar la desviación típica de cada uno de los 64 bits de una secuencia aleatoria generada en el emisor. En esta realización, se evita emplear para codificar la información los bits mas significativos que corresponden a los situados en las últimas posiciones, de forma que se elige la banda de bits comprendida entre las posiciones 6 y 45 ambas incluidas, lo cual permite utilizar 40 bits por cada valor de la diferencia de fases generada en el emisor para enmascarar el mensaje.

Para obtener la duración del intervalo sincronizado, se establece de forma arbitraria que en un ciclo se realicen 10^4 iteraciones de los esquemas de integración numérica. Luego, $\Delta t_{\mathrm{ciclo}} = \Delta t_{\mathrm{asinc}} + \Delta t_{\mathrm{sinc}} = 100 + 900 = 1000$ unidades de tiempo y, por tanto, $t_{\mathrm{fin}}^{i} = t_0^i + 1000 = t_{\mathrm{ref}}^{i} + 900$. Entonces, si se dispone de 9×10^3 valores de ${\theta_{\mathrm{E}}^{i}}^{(j)}$ por cada ciclo y de 40 bits por

cada uno de esos valores, entonces se debe dividir el mensaje m en $M = 18$ bloques ${m_i}^{(j)}$ de 36×10^4 bits cada uno, de forma que a cada valor de $t_j \in \left(t^i_{\text{ref}}, t^i_{\text{fin}}\right]$ le corresponde una secuencia de 40 bits del mensaje. Entonces, la señal de información generada en el emisor corresponde con

$$m_{\text{E}}(t_j) = \begin{cases} {m_i}^{(j)} & \text{si } t^i_{\text{ref}} < t_j \leq t^i_{\text{fin}} \\ \emptyset & \text{en otro caso,} \end{cases}$$

donde $i = 1, 2, \ldots, 18$. Para enmascarar la señal de información en la señal aleatoria, el emisor aplica el operador lógico XOR, representado en esta realización por el símbolo $\oplus$, entre los valores de la secuencia $m_{\text{E}}(t_j)$ y los 40 bits útiles de cada valor de la secuencia $r_{\text{E}}(t_j)$. De modo que la señal cifrada que se envía al receptor por el canal de comunicación es $s(t_j) = m_{\text{E}}(t_j) \oplus r_{\text{E}}(t_j)$.

Dado que cada ciclo requiere de 10^4 iteraciones de los esquemas de integración numérica, los generadores del parámetro c del emisor y el receptor deben calcular 10^4 valores de c a partir de los valores de c_0, v_0 y ρ contenidos en la clave estática. Los valores incluidos en la clave estática se muestran en la tabla 1. Si emisor y receptor emplean la misma clave estática, entonces pueden sincronizarse a través de las claves dinámicas. En tal caso, la señal de información recuperada en el receptor es

$$m_{\text{R}}(t_j) = s(t_j) \oplus r_{\text{R}}(t_j) = \begin{cases} 0 \ldots 0 \; {m_i}^{(j)} \; 0 \ldots 0 & \text{si } t^i_{\text{ref}} < t_j \leq t^i_{\text{fin}} \\ \emptyset & \text{en otro caso,} \end{cases}$$

donde, de nuevo, el símbolo $\oplus$ representa al operador lógico XOR y ${m_i}^{(j)}$ es la secuencia de 40 bits del mensaje enviada en el instante t_j que va precedida y seguida de los ceros que completan los 64 bits del número de coma flotante. La figura 3 muestra la señal $m_{\text{R}}(t)$ para los dos primeros ciclos de cifrado de la imagen.

Finalmente, el receptor puede recomponer el mensaje sabiendo que $m = \bigcup_i {m_i}^{(j)}$, es decir, concatenando los sucesivos bloques. La figura 5 muestra el resultado de cifrar la imagen de la figura 4. El resultado de descifrar la imagen empleando las claves de la tabla 1 es exactamente el mostrado en la figura 4.

Claves estáticas					
Emisor			Receptor		
c_0	v_0	ρ	c_0	v_0	ρ
10	0.4	3.95	10	0.4	3.95

Tabla 1: Tabla de claves estáticas para el emisor y el receptor que producen un descifrado correcto del mensaje.

REIVINDICACIONES

1. Sistema de comunicaciones seguras que envía una información cifrada de un mensaje desde un emisor (10) a un receptor (20) con el que comparte previamente una clave estática secreta formada por unas condiciones iniciales y un parámetro de los osciladores, donde el emisor está configurado para dividir dicha información del mensaje $m(\tau)$ en *M* bloques contiguos, donde cada bloque $m_i(\tau)$ es cifrado durante un *i*-ésimo ciclo que se divide en dos intervalos de tiempo: un intervalo asíncrono, que abarca desde el instante inicial t_0^i hasta el instante de referencia t_{ref}^i; y un intervalo sincronizado, que abarca desde t_{ref}^i hasta el instante final t_{fin}^i; comprendiendo además el sistema:

   - - un generador de señales pseudoaleatorias (5) contenido en el emisor, caracterizado por que comprende dos osciladores caóticos (1, 2) configurados con vectores de estado iniciales distintos y aleatorios, en el instante inicial en el que comienzan a oscilar, y con un acoplamiento (3) configurado para alcanzar la sincronización de fase de los osciladores, estando la salida de los osciladores conectada a un detector de diferencia de fases (4), configurado para calcular la diferencia de fases absolutas $\theta(t)$ durante el intervalo sincronizado, tomando como diferencia de fases inicial la diferencia de fases relativas en el instante de referencia t_{ref}^i,

   - un generador de señales pseudoaleatorias (15) contenido en el receptor e idéntico al contenido en el emisor, caracterizado por ser capaz de reproducir la misma diferencia de fases absolutas que el generador de señales pseudoaleatorias del emisor durante el intervalo sincronizado porque está configurado para que sus osciladores (11, 12) alcancen la sincronización de fase completa con los osciladores del emisor durante el intervalo asíncrono, empleando una pareja de claves dinámicas públicas,

   - dos canales de sincronización (23, 24), a través de los cuales el emisor envía al receptor dos señales de sincronización $s_1(t)$ y $s_2(t)$, que contienen las claves dinámicas públicas, formada cada una por una de las señales generadas por cada oscilador del emisor durante el intervalo asíncrono excluyendo los estados iniciales, y que solo pueden ser empleadas para el

descifrado del mensaje si el receptor está configurado con la misma clave estática secreta que el emisor emplea para el cifrado,

- dos acopladores (19, 21) incluidos en el receptor, cada uno de los cuales recibe una de las señales de sincronización, para sincronizar cada oscilador del receptor con su gemelo correspondiente en el emisor,

- un codificador (7), contenido en el emisor, configurado para combinar la señal pseudoaleatoria $r_E(t)$ de la salida de su detector de diferencia de fases (4) con la señal de información $m_E(t)$ que contiene el mensaje $m(\tau)$ dividido en bloques por un búfer de entrada (6), y generar en su salida la señal cifrada $s(t)$,

- un canal de comunicaciones (22), a través del cual se envía al receptor la señal cifrada $s(t)$, compuesta por los bloques $m_i(\tau)$ que son generados y enviados por el emisor durante el intervalo de sincronizado

- un decodificador (17), contenido en el receptor, configurado para combinar la señal pseudoaleatoria $r_R(t)$ de la salida de su detector de diferencia de fases (14) con la señal cifrada recibida $s(t)$ y generar en su salida la señal de información recuperada $m_R(t)$ durante el intervalo sincronizado, que contiene la secuencia de bloques $m_i(\tau)$ que son concatenados por un búfer de salida (16) del receptor para conformar el mensaje $m(\tau)$ descifrado,

- dos generadores de un parámetro (8, 18), uno contenido en el emisor y el otro en el receptor, que contienen un mapa caótico que son gemelos en el emisor y receptor para generar, a partir de la clave estática secreta, una misma secuencia de valores de un parámetro de cada oscilador del emisor y receptor, que se repite en cada ciclo de cifrado de los bloques del mensaje.

2. Sistema, según reivindicación 1, donde el generador de señales pseudoaleatorias (5) del emisor comprende una fuente de entropía (9), configurada para generar los distintos estados aleatorios iniciales $u_{E1}^i(t_0^i)$ y $u_{E2}^i(t_0^i)$ de los osciladores al inicio del ciclo de cifrado de cada bloque $m_i(\tau)$ del mensaje, estando el generador de un parámetro (8) del emisor, configurado para variar un parámetro c de los osciladores (1, 2) durante el ciclo de cifrado, y donde cada uno de los osciladores del emisor está configurado para

generar una de las señales de sincronización, cada una de las cuales conforma una clave dinámica pública y única para cada bloque del mensaje, que se envían durante el intervalo asíncrono al receptor (20) por los canales de sincronización (23, 24), donde el detector de diferencia de fase (4) del emisor está configurado para comenzar a calcular la diferencia de fases $\theta_E^i(t)$ a partir del instante de referencia t_{ref}^i tomando como fase de referencia la fase relativa de cada oscilador en ese instante, conformando la salida del detector de diferencia de fases (4) del emisor la señal aleatoria definida por

$$r_E(t) = \begin{cases} \theta_E^i(t) & si\ t_{ref}^i < t \leq\ t_{fin}^i \\ \emptyset & en\ otro\ caso. \end{cases}$$

3. Sistema de comunicaciones, según la reivindicación 2, donde cada clave dinámica de cada bloque del mensaje comprende una señal de cada oscilador del emisor excluyendo las condiciones iniciales aleatorias, y estando el receptor configurado para sincronizar sus osciladores con los del emisor a partir de dichas claves dinámicas de las señales de sincronización, y generar las mismas señales que el emisor durante el intervalo sincronizado.

4. Sistema de comunicaciones, según la reivindicación 1, donde los ociladores caóticos (11, 12) del generador de señales pseudoaleatorias (15) del receptor, tienen estados iniciales $u_{R1}(t_0')$ y $u_{R2}(t_0')$ arbitrarios en el instante inicial t_0' en el que el receptor comienza la escucha de los canales de comunicación (22) y de sincronización (23, 24), estando el generador de un parámetro (18) del receptor configurado para variar un parámetro c de los osciladores durante el proceso de descifrado, y donde el detector de diferencia de fase del receptor está configurado para comenzar a calcular la diferencia de fases $\theta_R^i(t)$ a partir del instante de referencia $t_{\mathrm{ref}}^{\mathrm{i}}$ tomando como fase de referencia la fase relativa de cada oscilador en ese instante, conformando la salida del detector de diferencia de fases (14) del receptor una réplica de la señal aleatoria que se genera en el emisor definida por

$$r_R(t) = \begin{cases} \theta_R^i(t) & si\ t_{ref}^i < t \leq\ t_{fin}^i \\ \emptyset & en\ otro\ caso. \end{cases}$$

5. Sistema de comunicaciones, según la reivindicación 1, donde la señal de información generada por el búfer de entrada (6) del emisor comprende la secuencia de bloques en los que se divide el mensaje para ser enviados durante el intervalo sincronizado, quedando definida por

$$m_E(t) = \begin{cases} m_i(\tau) & si\ t_{ref}^i < t \leq\ t_{fin}^i \\ \emptyset & en\ otro\ caso, \end{cases}$$

donde el bloque $m_i(\tau)$ definido en el intervalo $\tau_{i-1} < \tau \leq \tau_i$ tiene una duración $\Delta\tau_{info} = \tau_i - \tau_{i-1}$ que debe ser menor o igual a la duración del intervalo sincronizado $\Delta t_{sinc} = t_{fin}^i - t_{\mathrm{ref}}^{\mathrm{i}}$, siendo el mensaje completo $m(\tau) = \cup_i m_i(\tau)$ con $i = 1, \ldots, M$.

6. Sistema de comunicaciones, según la reivindicación 1, donde el decodificador (17) del receptor está configurado para generar la señal de información recuperada y recuperar el mensaje completo, únicamente cuando se inicia la escucha de los canales de sincronización y de comunicación al inicio de la transmisión, $t_0' \leq t_0^1$, y de forma continuada hasta, al menos, el instante t_{fin}^M, y cuando el tiempo de escucha es menor al tiempo de transmisión del mensaje, realiza una recuperación parcial del mensaje, quedando la señal definida por

$$m_R(t) = \begin{cases} m_i(\tau) & si\ t_{ref}^i < t \leq\ t_{fin}^i \\ \emptyset & en\ otro\ caso. \end{cases}$$

7. Sistema de comunicaciones seguras, según la reivindicación 1, donde el mapa caótico de los generadores del parámetro *c* 8, 18) de los osciladores del emisor (10) y receptor (20), están configurados para cambiar el valor del parámetro c en intervalos de tiempo fijos Δt_c menores que el intervalo asíncrono, donde el intervalo de tiempo de cada *i*-ésimo ciclo se divide en *N* subintervalos, tal que la duración total de un ciclo es $\Delta t_{ciclo} = N\Delta t_c$, en el que a cada subintervalo desde $n = 0$ hasta $n = N - 1$, le corresponde un valor de c que se obtiene mediante la función $c_{n+1} = \varphi(c_n, v_n; \rho)$ siendo v_n el *n*-ésimo valor del mapa caótico y ρ un parámetro del mismo que forma parte de una clave estática secreta almacenada en el emisor y receptor y de la que también forman parte los valores iniciales c_0 y v_0, y siendo la función φ una secuencia de *N* valores del parámetro c para que los osciladores conserven siempre su comportamiento caótico, estando el receptor configurado para sincronizar sus osciladores completamente con los del emisor únicamente cuando su clave estática secreta coincide con la del emisor, permitiendo descifrar los bloques del mensaje.

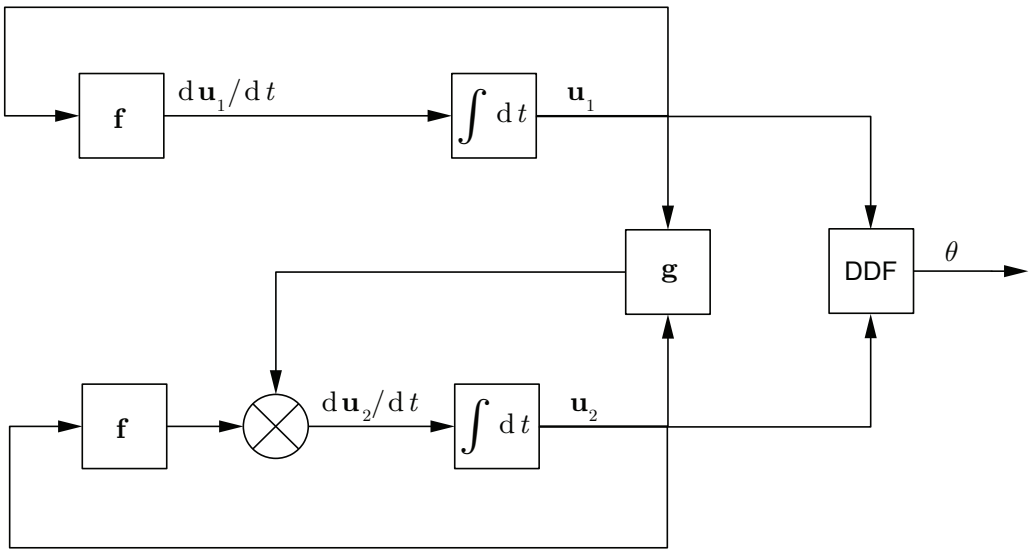
f
$d\mathbf{u}_1/dt$
$\int dt$
$\mathbf{u}_1$
g
DDF
θ
f
$d\mathbf{u}_2/dt$
$\int dt$
$\mathbf{u}_2$

Figura 1

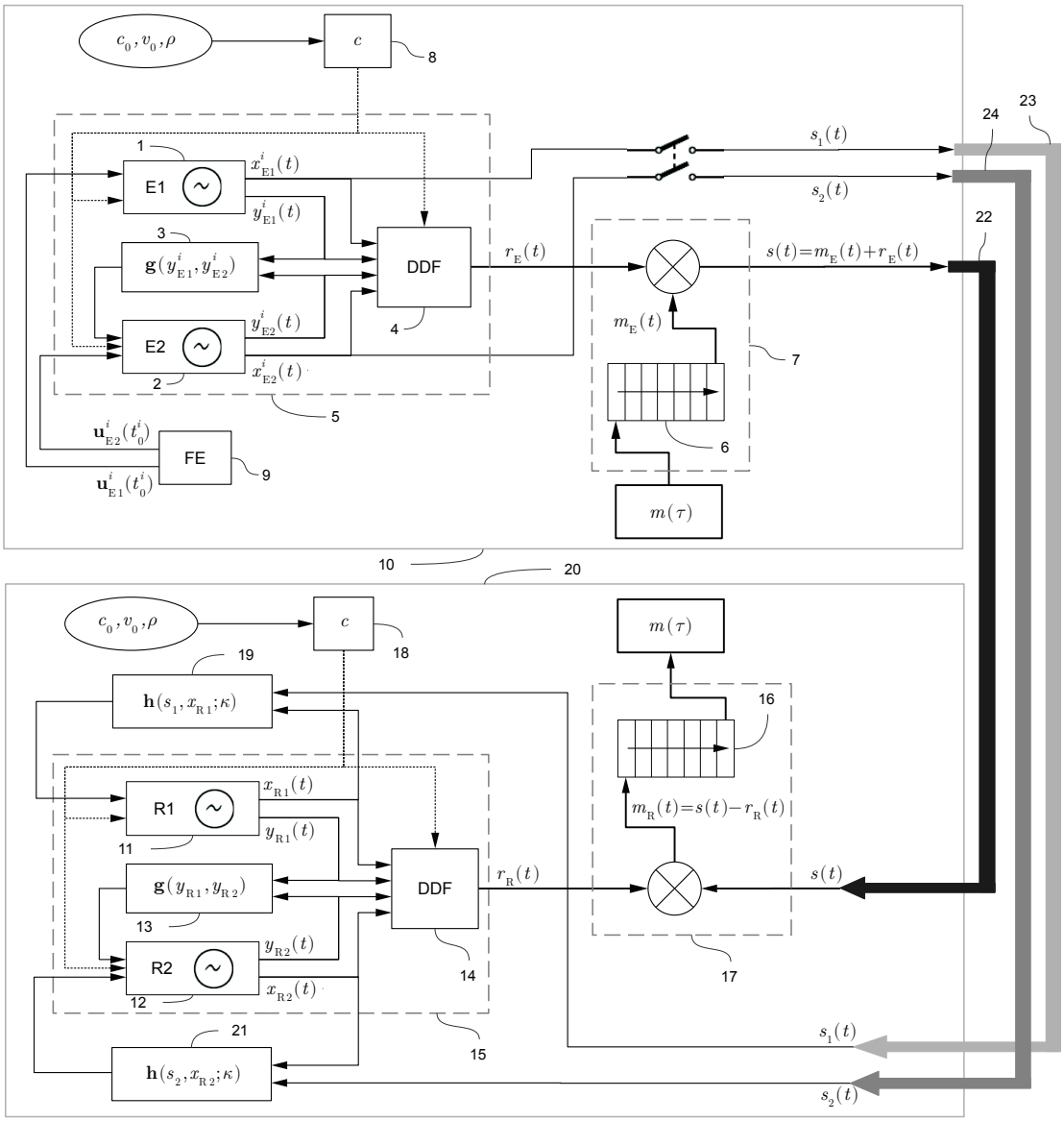
c_0, v_0, ρ
c
8
1
E1
$x^i_{E1}(t)$
$y^i_{E1}(t)$
3
$\mathbf{g}(y^i_{E1}, y^i_{E2})$
DDF
4
$r_E(t)$
$s_1(t)$
$s_2(t)$
24
23
22
$s(t)=m_E(t)+r_E(t)$
$m_E(t)$
7
E2
$y^i_{E2}(t)$
$x^i_{E2}(t)$
2
5
6
$m(\tau)$
$\mathbf{u}^i_{E2}(t^i_0)$
FE
9
$\mathbf{u}^i_{E1}(t^i_0)$
10
20
c_0, v_0, ρ
c
18
$m(\tau)$
19
$\mathbf{h}(s_1, x_{R1}; \kappa)$
16
$m_R(t)=s(t)-r_R(t)$
R1
$x_{R1}(t)$
$y_{R1}(t)$
11
$\mathbf{g}(y_{R1}, y_{R2})$
DDF
$r_R(t)$
$s(t)$
13
14
17
R2
$y_{R2}(t)$
$x_{R2}(t)$
12
15
21
$\mathbf{h}(s_2, x_{R2}; \kappa)$
$s_1(t)$
$s_2(t)$

Figura 2

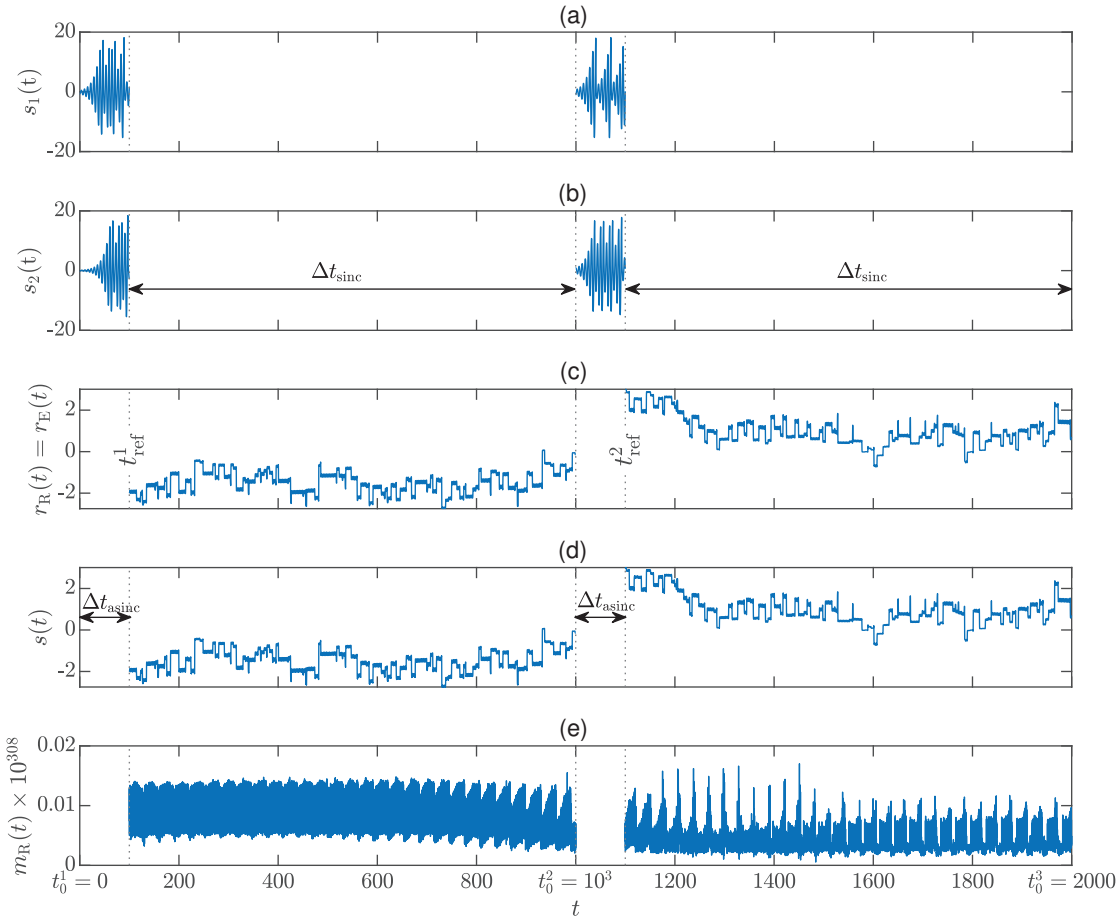
(a)
$s_1(t)$
20
0
-20
(b)
$s_2(t)$
Δt_{sinc}
Δt_{sinc}
(c)
$r_{\text{R}}(t) = r_{\text{E}}(t)$
t^1_{ref}
t^2_{ref}
(d)
$s(t)$
Δt_{asinc}
Δt_{asinc}
(e)
$m_{\text{R}}(t) \times 10^{308}$
0.02
0.01
$t^1_0 = 0$
200
400
600
800
$t^2_0 = 10^3$
1200
1400
1600
1800
$t^3_0 = 2000$
t

Figura 3

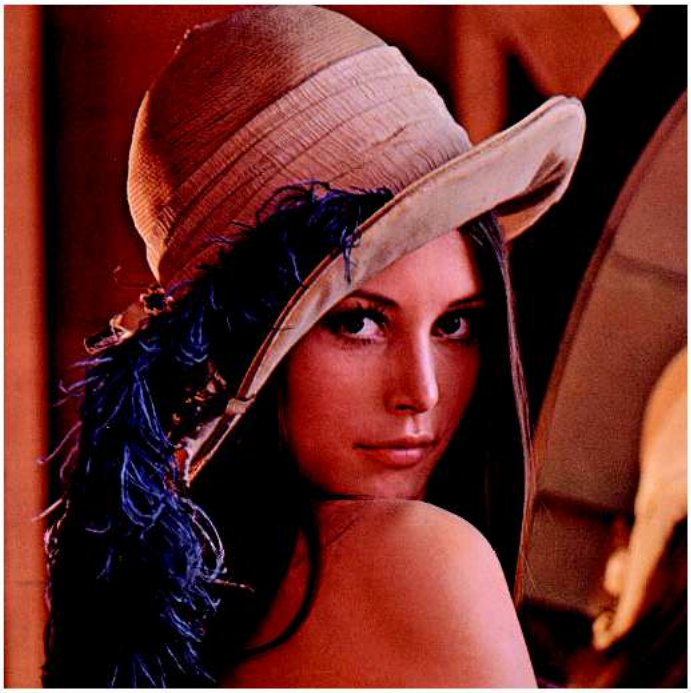

Figura 4

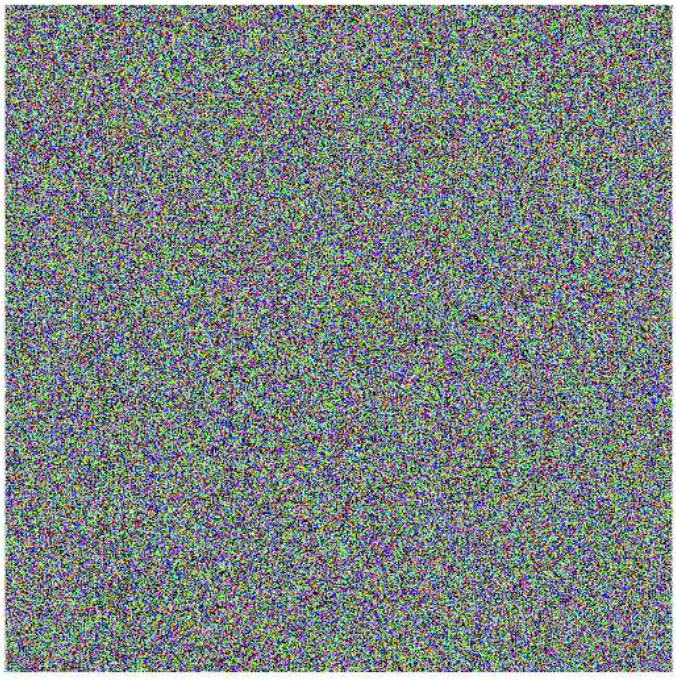

Figura 5

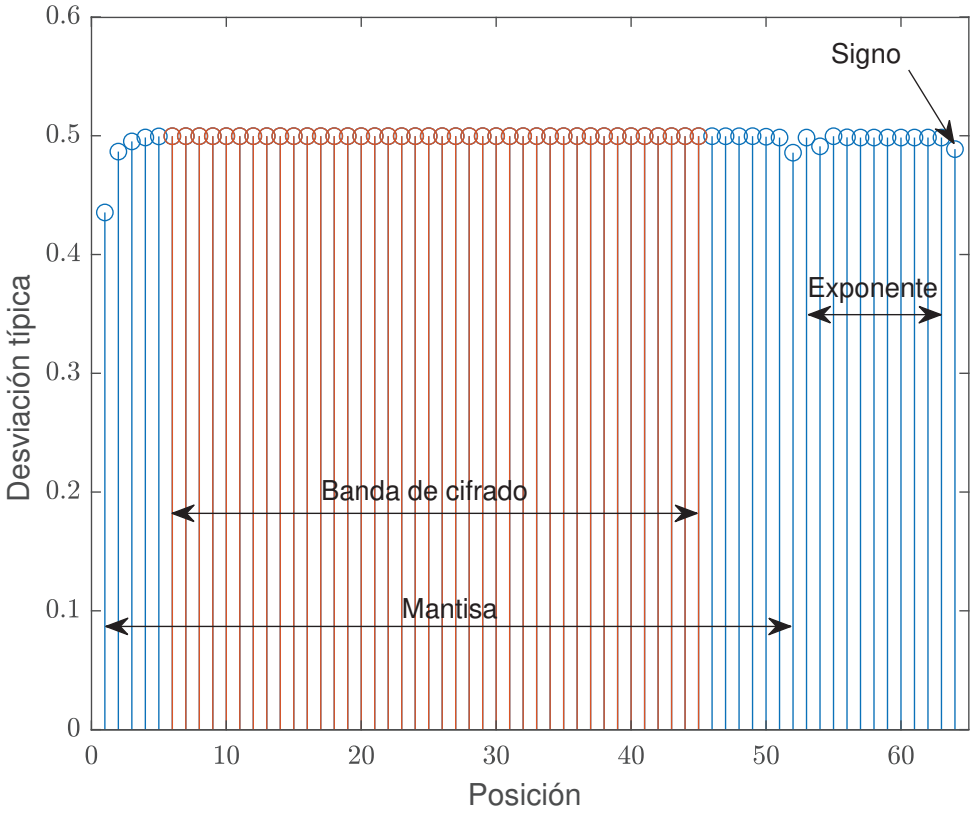
Signo
Exponente
Banda de cifrado
Mantisa
Desviación típica
Posición
0.6
0.5
0.4
0.3
0.2
0.1
0
0
10
20
30
40
50
60

Figura 6