Criptoanálisis de sistema criptográfico

Basado en la sincronización de osciladores caóticos

TRATAMIENTO DE SEÑAL. En este artículo se demuestra la falta de seguridad de los criptosistemas basados en criptografía de señal. Se utilizan las aplicaciones de retorno para desenmascarar mensajes cifrados utilizando el oscilador de Chua, recuperándose las señales con una calidad muy aceptable.

G. Álvarez, F. Montoya, M. Romera y G. Pastor
Instituto de Física Aplicada, C.S.I.C. Serrano, 144. 28006 Madrid.
E-mail: gonzalo@iec.csic.es

Desde que en 1990, Pecora y Carrol [1] demostraron la viabilidad de la sincronización de dos sistemas caóticos, han surgido muchas realizaciones para aplicar esta posibilidad al mundo de las comunicaciones seguras. La idea fundamental en la que se basan estos criptosistemas consiste pues en utilizar un oscilador no lineal caótico como generador de una señal pseudoaleatoria de banda ancha. Esta señal se combina con el mensaje para producir una señal ininteligible que se transmite a través del canal de comunicaciones inseguro. En el sistema receptor se reproduce la señal pseudoaleatoria caótica, de manera que combinándola mediante la operación inversa con la señal recibida, se puede recuperar el mensaje original, de acuerdo con el diagrama de la figura 1.

Los requisitos que debe cumplir el generador pseudoaleatorio para producir la señal cifrante sin repetición ni predictabilidad son las siguientes:

*Sensibilidad de parámetros: basta con que uno de los parámetros del sistema varíe muy ligeramente para que dos trayectorias obtenidas a partir del mismo punto inicial se separen exponencialmente.

*Sensibilidad a las condiciones iniciales: dos trayectorias obtenidas a partir de dos puntos iniciales, x_o y x_o', arbitrariamente próximos, se separan una de otra exponencialmente.

*Ergodicidad: las trayectorias seguidas por puntos del espacio de fases recorren erráticamente todo el espacio con distribución uniforme.

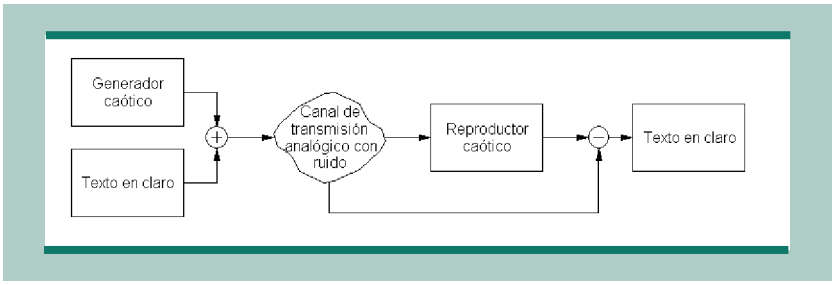


Figura 1. Esquema de bloques conceptual de un criptosistema caótico basado en el cifrado de Vernam.

En teoría, sólo se podrá reproducir en recepción el comportamiento del sistema caótico emisor si se conocen los valores exactos de las condiciones iniciales y de los parámetros, que pueden ser considerados como la clave del criptosistema caótico.

SISTEMA CRIPTOGRÁFICO BASADO EN LA SINCRONIZACIÓN DE OSCILADORES CAÓTICOS

El criptosistema presentado por R. González et al. [3] es otra implementación más basada en el circuito de Chua del ya clásico esquema de enmascaramiento caótico [4-6], en el que una señal analógica se suma aditivamente a la salida del oscilador caótico, que actúa como señal enmascaradora de banda ancha. En la medida en que la potencia de la señal de mensaje sea mucho menor que la de la señal caótica, y que su ancho de banda sea también menor, su espectro quedará "enterrado" en ella y resultará inaudible. En la figura 2 se muestra un esquema conceptual de este criptosistema.

El oscilador caótico del emisor posee tres variables de estado, x, y, z, utilizándose una de ellas para sumarla al mensaje a transmitir, s(t). Además, en condiciones reales el canal presentará ruido n(t), que se suma a la señal transmitida r(t). En el receptor se recibe r(t)+n(t), y se intenta sincronizar su oscilador caótico con el del emisor, del cual es una réplica exacta. La señal $x_1(t)$, en el caso de alcanzarse la sincronización, deberá seguir al valor de x(t), por lo que restándola de r(t)+n(t) se debería obtener una copia fiel $\hat{s}$ (t) del mensaje s(t). Los detalles de diseño del criptosistema se pueden encontrar en el artículo citado [3].

CRIPTOANÁLISIS

En los párrafos siguientes, se considerará, para facilitar la labor, un canal sin perturbaciones ni rui-

CRIPTOANÁLISIS

do. A decir verdad, en condiciones realistas, tales como transmisión a través de un canal físico con ruido y con ancho de banda limitado, se producirá la desincronización o la señal recuperada será irreconocible. Para que este esquema funcione, la potencia de la señal de mensaje debe ser muy inferior a la potencia de la portadora caótica, como mínimo 30 dB por debajo, para que quede efectivamente enmascarada. Si la señal de mensaje posee tan poca potencia y si el ruido es del mismo orden de magnitud, se verá enterrada y en recepción será imposible separarlos.

Básicamente, existen tres procedimientos de criptoanálisis para el criptosistema anterior:

*La extracción de la señal de información s(t) a partir de la señal transmitida r(t).

*La extracción de la señal $x_1(t)$ a partir de r(t).

*La estimación de los parámetros del oscilador caótico.

En este artículo vamos a demostrar la inutilidad de este criptosistema, utilizando el método de las aplicaciones de retorno [7] para extraer s(t) a partir del conocimiento de r(t) exclusivamente, es decir, según el procedimiento (1).

Dada la señal caótica x(t), puede construirse una aplicación de retorno de la siguiente forma: se define t_n como el instante en que x(t) alcanza su n-ésimo máximo local, y X_n, como el valor de x en ese momento. De forma análoga, se define otra aplicación de retorno estableciendo u_m como el instante en que x(t) alcanza su m-ésimo mínimo local, e Y_m, como el valor de x en ese instante. Usando estos valores, se pueden construir las aplicaciones de retorno X_{n+1} vs X_n e Y_{m+1} vs Y_m. Estas dos aplicaciones poseen atractores que parecen casi unidimensionales, como se muestra en los recuadros (1) y (2) de la figura 3 por la línea oscura. Si se añade la señal de mensaje s(t)

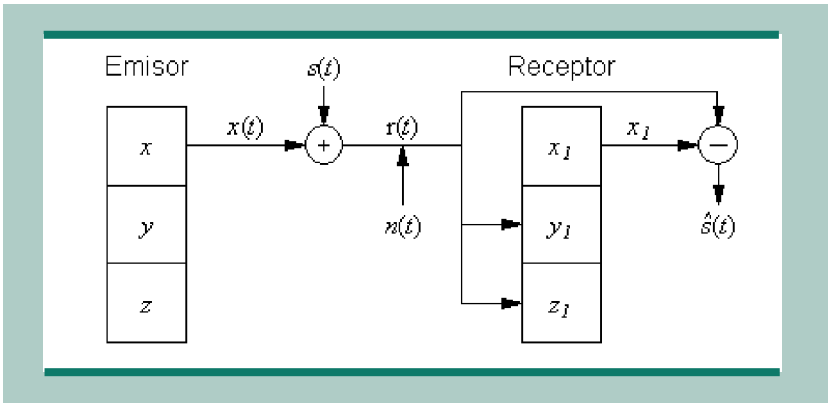


Figura 2. Sistemas emisor y receptor. El receptor obtiene el valor de x a partir de x(t), que le es transmitida desde el maestro. Gracias a las ecuaciones para y_1 y para z_1, es capaz de reproducir x_1, que una vez alcanzado el sincronismo seguirá con error mínimo al valor de x, lo que permite recuperar la señal del mensaje enmascarada.

CRIPTOANÁLISIS

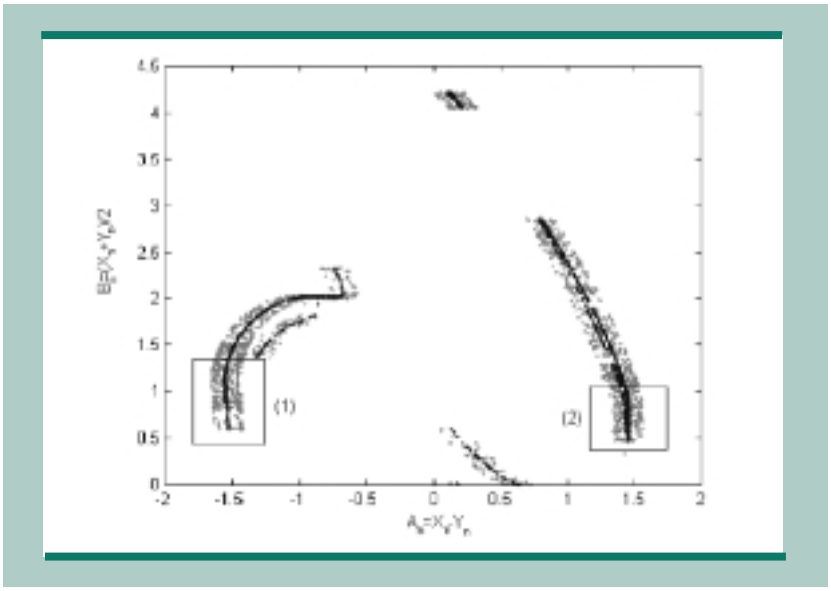
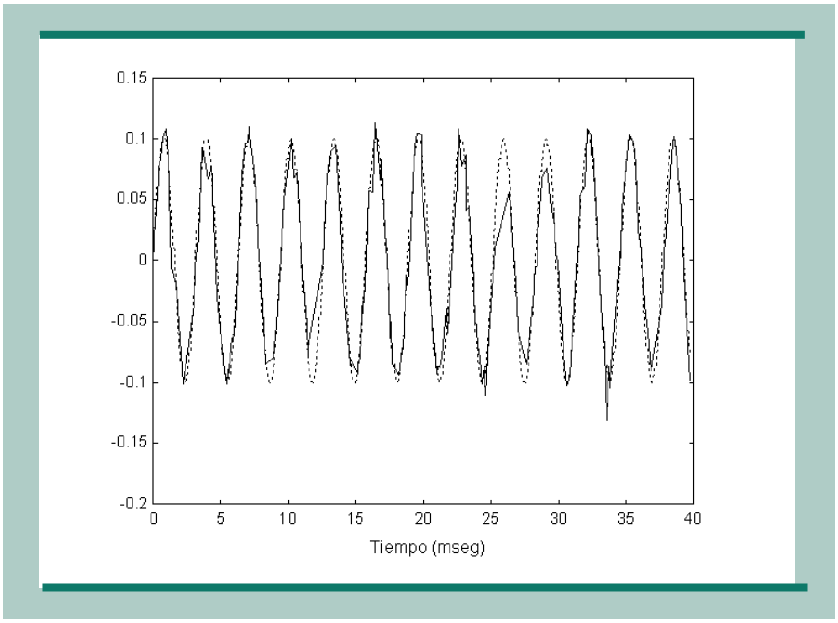


Figura 3. Atractores de las aplicaciones de retorno obtenidos para los máximos y mínimos de x(t) en el oscilador caótico de Chua. En línea oscura se muestra el oscilador sin señal de mensaje. La banda difusa alrededor de los segmentos anteriores representan la señal caótica más el mensaje.

a la señal caótica x(t), entonces el efecto que se produce sobre el atractor cuasi unidimensional de las aplicaciones de retorno es una difusión alrededor de los segmentos del atractor cuando sólo existía la señal caótica. El ensanchamiento es simétrico a ambos lados, lo que permite recobrar el mensaje transmitido sin más que medir la distancia que ocupan los puntos respecto de la posición que ocuparían en ausencia de mensaje. Esta distancia se puede aproximar con muy buenos resultados como la distancia del punto a la media de los valores de los puntos encerrados en uno u otro recuadro en la figura 3. Los resultados de este examen, realizado únicamente a partir del conocimiento de r(t), y por tanto sin conocimiento ni de los valores del circuito caótico, ni de la señal x(t), ni por supuesto de la señal a transmitir, se muestran en la figura 4. Como se ve, se ha obtenido la señal de mensaje con una calidad muy aceptable, que permite conocer con gran exactitud la frecuencia del tono original, 318,31 Hz, que a partir de la señal obtenida puede estimarse en 318,75 Hz; es decir, con un error del 0,004%. Es importante recalcar que este resultado tan sorprendente se ha obtenido sin filtrado ni amplificación ni posterior procesamiento de la señal recuperada, los cuales por supuesto mejorarían notablemente la señal recuperada.

Figura 4. Desenmascaramiento de la señal de mensaje utilizando aplicaciones de retorno. La línea de puntos representa el mensaje original s (t)= 0,1 sin($2\pi ft$), con f = 318.31 Hz, mientras que la línea continua representa el mensaje reconstruido.



En [8] puede encontrarse una explicación detallada de cómo obtener x(t) a partir de r(t), así como la manera de estimar los parámetros del oscilador caótico; es decir, de los procedimientos (2) y (3).

CONCLUSIONES

Por lo tanto, en vista de lo que ha quedado demostrado en este artículo y lo que puede comprobarse en [8], los mensajes cifrados mediante este criptosistema pueden recuperarse mediante los tres procedimientos de criptoanálisis mencionados, por lo que no supone la más mínima seguridad a la hora de proteger la confidencialidad de un mensaje. Este criptosistema, por tanto, no puede considerarse como un mecanismo de cifrado serio, sino más bien como un medio para frustrar los intentos por entender una comunicación durante una escucha casual, ya que no sirve para evitar que el atacante determinado descifre fácilmente los mensajes.

REFERENCIAS

[1] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems", Phys. Rev. Lett. 64, 821-824 (1990).

[2] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps", Int. J. Bifurc. Chaos 8(6), 1259-1284 (1998).

[3] R. González, M. Prian, E. A. Romero, V. Sánchez, J. L. Rojas y M. Sánchez, "Criptografía de Señal", Mundo Electrónico, 303, 58-60 (1999).

[4] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, "Experimental demonstration of secure communications via chaotic synchronization", Int. J. Bifurc. Chaos 2, 709-713 (1992).

[5] K. M. Cuomo and A. V. Oppenheim, "Circuit Implementation of Synchronized Chaos with Application to Communications", Phys. Rev. Lett. 7(1), 65-68 (1993).

[6] G. Álvarez Marañón y Miguel A. F. Sanjuán, "Comunicaciones Seguras utilizando Señales Caóticas", Revista Española de Física 13(5), 23-27 (1999).

[7] G. Pérez y H.A. Cerdeira, "Extracting Messages Masked by Chaos", Phys. Rev. Lett. 74(11), 1970-1973 (1995).

[8] Th. Beth, D. E. Lazic, A. Mathias, "Cryptanalysis of Cryptosystems based on Remote Chaos Replication", in Advances in Cryptology •CRYPTO •94, 318-331 (1994). ME