Criptoanálisis de un criptosistema de dos canales basado en una función no lineal caótica

A.B. Orúe, M.J. García-Martínez, G. Pastor y F. Montoya
Instituto de Seguridad de la Información
Consejo Superior de Investigaciones Científicas
Serrano 144, 28006 Madrid
Email: gerardo@iec.csic.es

C. Sánchez Ávila
Dep. de Matemática Aplicada a las Tecnologías de la Información
E.T.S.I. de Telecomunicación, UPM
Email: carmen.sanchez.avila@upm.es

***Resumen*—En este artículo se realiza el criptoanálisis de un criptosistema caótico basado en el sistema de Lorenz, que utiliza dos canales de comunicación y una función no lineal caótica. Se demuestra que el sistema propuesto es inseguro ya que los valores de los parámetros del sistema pueden determinarse con gran precisión utilizando un receptor intruso.**

I. Introducción

El vínculo entre la criptografía y los sistemas caóticos continúa siendo objeto de un intenso estudio. Muchos investigadores están de acuerdo en que la interacción de estas áreas puede ser mutuamente beneficiosa. Diversas herramientas de análisis de los sistemas caóticos han servido igualmente como herramientas en el criptoanálisis de muchos sistemas y para el estudio y perfeccionamiento del diseño de otros ([2], [4], [7], [12], [13], [17], [23]). A partir de los primeros trabajos sobre la sincronización del caos ([21], [22]) comienza nuevamente el interés por los sistemas de comunicaciones seguros basados en sistemas caóticos. Los primeros sistemas no eran conscientes de los conceptos y estándares utilizados en criptografía, por lo que resultaron criptográficamente débiles e ineficientes. La mayoría de los criptosistemas caóticos propuestos en la actualidad comienzan a tener en cuenta muchos de los principios criptográficos básicos, aunque todavía no son suficientes y siguen resultando inseguros e ineficientes. Por tanto sigue existiendo una imperiosa necesidad de una mayor colaboración entre estas dos grandes áreas de investigación.

Observando las referencias puede constatarse que después de casi tres décadas la mayoría de las publicaciones que involucran a los criptosistemas caóticos sigue encontrándose en las áreas de física e ingeniería electrónica, fuera del área de la seguridad. La mayoría de estos trabajos están publicados en *Communications in Nonlinear Science and Numerical Simulation*, *Physics Letters A*, *Int. J. Bifurcation and Chaos*, *Chaos, Solitons & Fractals*, *Physical Review Letters*, *Physical Review E*, *IEEE Trans. on Circuits and System* y *IEEE Int. Symposium on Circuits and System*, *Chaos*, *Chinese Physics B*, *Eurasip Journal on Applied Signal Processing*. Esto explica en parte que actualmente la criptografía basada en el caos sea todavía considerada como un fenómeno marginal, a pesar de que los principios presentados por Shannon ([24]) acerca de la confusión y la difusión son inherentes a estos sistemas ([10], [5]).

La idea fundamental de los sistemas de comunicaciones seguros basados en caos, utiliza un sistema dinámico en regimen caótico para generar una secuencia de banda ancha pseudoaleatoria y la combina con el mensaje para producir una señal de aspecto ininteligible que se transmite sobre un canal inseguro. Luego, utilizando la sincronización de estos sistemas el receptor reproduce la señal pseudoaleatoria y la combina mediante la operación inversa con la señal recibida, recuperando así el mensaje original.

Un problema clave de la mayoría de este tipo de criptosistemas es la falta de seguridad ([1], [3], [14], [18]), en muchas ocasiones debido a que no se han tenido en cuenta los requerimientos necesarios desde el punto de vista de la criptología. El criptoanálisis y los sistemas de procesado de señales han desarrollado técnicas consolidadas de análisis de series numéricas y señales continuas, que permiten hallar las claves de un sistema, o al menos acotarlas, y a veces recuperar el texto claro sin conocer la clave. Cuando el diseñador del sistema desconoce la potencia de estas herramientas, el mismo sucumbe fácilmente al ataque de un criptoanalista.

A pesar de que se ha demostrado que muchos sistemas de cifrado caótico son inseguros e ineficientes, se siguen implementando nuevas modificaciones para resistir los ataques descubiertos ([6], [8], [11], [15], [16], [20], [25], [26]).

Recientemente se ha propuesto un nuevo criptosistema caótico [27] que utiliza el conocido sistema de Lorenz, en una estructura excitador-respuesta con dos canales de comunicación. Uno de estos canales de comunicación se utiliza para transmitir el mensaje cifrado y el otro canal se utiliza para transmitir la señal de sincronización necesaria para que en el extremo receptor, una vez sincronizado, se pueda obtener el mensaje. De este modo el proceso de sincronización queda completamente aislado del algoritmo de identificación de parámetros. El artículo explora la transmisión de señales

analógicas y digitales, investigando diversas técnicas para optimizar el rendimiento de los sistemas propuestos. Se asume que ambos extremos, transmisor y receptor, tienen la misma dinámica, en este caso el sistema caótico de Lorenz.

Las ecuaciones del sistema transmisor son:

$$\dot{x}_1 = -\sigma\, x_1 + \sigma\, x_2, \tag{1}$$
$$\dot{x}_2 = \rho\, x_1 - x_2 - x_1\, x_3, \tag{2}$$
$$\dot{x}_3 = x_1\, x_2 - \beta\, x_3. \tag{3}$$

El receptor diseñado utiliza un algoritmo recursivo, inspirado en la técnica de control denominada *backstepping*, según los autores, para obtener una sincronización rápida y estable. Actúa como un observador de estado que utiliza la señal x_1, para estimar los estados restantes del transmisor,

$$\dot{\widehat{f}}_2 = -(\sigma+1)\widehat{f}_2 - x_1\widehat{f}_3 + (\rho-1)x_1 \tag{4}$$
$$\dot{\widehat{f}}_3 = x_1\widehat{f}_2 - \beta\widehat{f}_3 + x_1^2, \tag{5}$$
$$\widehat{x}_2 = \widehat{f}_2 + x_1, \tag{6}$$
$$\widehat{x}_3 = \widehat{f}_3, \tag{7}$$

donde $X = [x_1\, x_2\, x_3]^t$ es el vector de estado del transmisor, $\widehat{X} = [\widehat{x}_2\, \widehat{x}_3]^t$ es el vector de estado del receptor, $\widehat{f}_1$ y $\widehat{f}_2$ son dos variables usadas implícitamente para observar las variables x_2 y x_3 del transmisor. Los parámetros del sistema tienen los valores: $8 < \sigma < 12$, $\rho = 28$, $\beta = 8/3$.

En el artículo se presentan tres casos de estudio afirmando que cada uno de ellos mejora la seguridad de los criptosistemas caóticos diseñados previamente. Primero se realiza un estudio de la sincronización de los sistemas caóticos. Después se diseña un receptor que consiste en un observador de estado que utiliza la señal de sincronización $x_1(t)$ del sistema de Lorenz para estimar los estados restantes del sistema transmisor $x_2(t)$, $x_3(t)$. Se realiza además un estudio de la estabilidad de la sincronización basado en funciones de Lyapunov. Luego se diseñan los sistemas transmisor y receptor, teniendo en cuenta su realización por hardware, mediante el uso de amplificaciones operacionales, resistencias y condensadores. Finalmente se realiza la simulación de la sincronización del sistema usando la herramienta Simulink del Matlab; comprobándose la sincronización entre ambos extremos.

II. Caso de estudio I

En este caso, los autores estudian el comportamiento del sistema descrito en [9], ahora desde la perspectiva de un método de sincronización basado en una técnica de control recursivo que incrementa la razón de convergencia de la sincronización utilizando determinadas funciones de Lyapunov. El sistema de comunicación seguro utiliza una función de cifrado que combina el mensaje claro $s(t)$ con una de las variables de estado del transmisor.

Se plantea la siguente ecuación de cifrado en el transmisor:

$$E(X, s, t) = x_2^2 + (1 + x_2^2)\, s(t). \tag{8}$$

En el extremo receptor, una vez lograda la sincronización de ambos extremos, transmisor y receptor, se recuperaría el mensaje claro por la ecuación inversa:

$$\widehat{s}(t) = D(\widehat{X}, s, t) = \frac{E(X, s, t) - \widehat{x}_2^2}{1 + \widehat{x}_2^2}, \tag{9}$$

donde $\widehat{s}(t)$ es el mensaje recuperado.

El criptosistema propuesto asume que son públicamente conocidos los parámetros ρ y β. El conocimiento del parámetro σ es intrascendente, pues no se requiere para descifrar el mensaje.

Los autores de [27] presentan este criptosistema como de seguridad reducida; sin embargo, los cambios introducidos solo modifican el método de sincronización empleado, de manera que el sistema sigue siendo inseguro, ya que sigue siendo vulnerable al criptoanálisis realizado en [19], donde se aplican las propiedades geométricas del sistema de Lorenz para reducir el espacio de búsqueda de los parámetros, y luego se determinan los parámetros de manera exacta a partir del texto cifrado.

III. Caso de estudio II

El segundo caso de estudio explora la utilización de una mejora con respecto al caso anterior, en la que el proceso de cifrado depende tanto de uno de los estados del sistema caótico como de alguno de sus parámetros. Se realiza el análisis de seguridad de este método, destacando sus ventajas y limitaciones, a través de la simulación de los ataques de intrusos en el canal de comunicación.

La ecuación de cifrado en el extremo transmisor es:

$$E(X, \sigma, s, t) = x_2^2 + (\sigma^2 + x_2^2)\, s(t), \tag{10}$$

y la de descifrado en el receptor es:

$$\widehat{s}(t) = D(\widehat{X}, \sigma, s, t) = \frac{E(X, \sigma, s, t) - \widehat{x}_2^2}{\sigma + \widehat{x}_2^2}. \tag{11}$$

En este caso, el parámetro σ cumple con el papel de clave. El proceso de sincronización sigue siendo el mismo del caso anterior, es decir, se transmite por una parte la señal cifrada y por otra la señal de sincronización $x(t)$. Los autores ponen de manifiesto su falta de seguridad frente a ataques por estimación del valor de σ y filtrado. Sin embargo, la recuperación del valor de σ es un proceso sencillo que se puede conseguir a base del siguiente receptor intruso con tres ecuaciones:

$$\dot{\widehat{x}}_1 = -\widehat{\sigma}\, \widehat{x}_1 + \widehat{\sigma}\, \widehat{x}_2, \tag{12}$$
$$\dot{\widehat{x}}_2 = \rho\, x_1 - \widehat{x}_2 - x_1\, \widehat{x}_3, \tag{13}$$
$$\dot{\widehat{x}}_3 = x_1\, \widehat{x}_2 - \beta\, \widehat{x}_3. \tag{14}$$

Con este receptor, se genera una variable $\widehat{x}_1$ que intenta reproducir la variable de sincronización x_1. La Fig.1 representa el valor absoluto del error de sincronización $|x_1 - \widehat{x}_1|$ en función del valor estimado del parámetro $\widehat{\sigma}$ del receptor intruso, para un valor del parámetro $\sigma = 10$ del transmisor. Naturalmente, cuando el valor de ambos parámetros es diferente, el error de sincronización es notable; pero, cuando

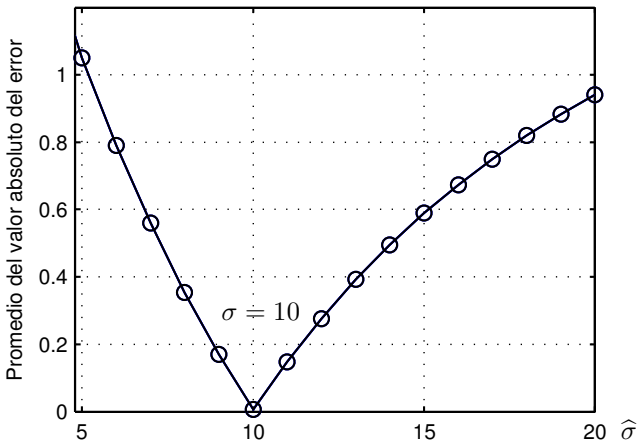

Fig. 1. Valor medio del error $|x_1 - \widehat{x}_1|$, en función de $\widehat{\sigma}$, para el caso 2 ($\sigma = 10$)

la diferencia entre parámetros disminuye progresivamente, el error de sincronización disminuye igualmente, para llegar a anularse cuando $\widehat{\sigma} = \sigma$. La Fig.1 se ha confeccionado con solo 16 valores de $\widehat{\sigma}$, simbolizados por los círculos, lo que pone de manifiesto la facilidad del ataque.

La recuperación del valor óptimo de $\widehat{\sigma}$ se puede llevar a cabo eficientemente, mediante un algoritmo de búsqueda adecuado.

Como demostración, se ha realizado un programa en Matlab 7, que busca maximizar la relación señal a ruido de la variable $\widehat{x}_1$; es decir, se minimiza el logaritmo del error cuadrático medio de $\widehat{x}_1$.

La medida se ha realizado una vez transcurrido el transitorio inicial (que se ocasiona debido a desconocer las condiciones iniciales del transmisor), entre $t = 5$ y $t = 10$ segundos.

Con el fin de simular un caso real se ha aleatorizado el valor de σ para que fuera menos convencional que en ejemplo de [27]; se ha elegido $\sigma = 10.5528$.

A continuación se describe el programa de búsqueda, en pseudocódigo:

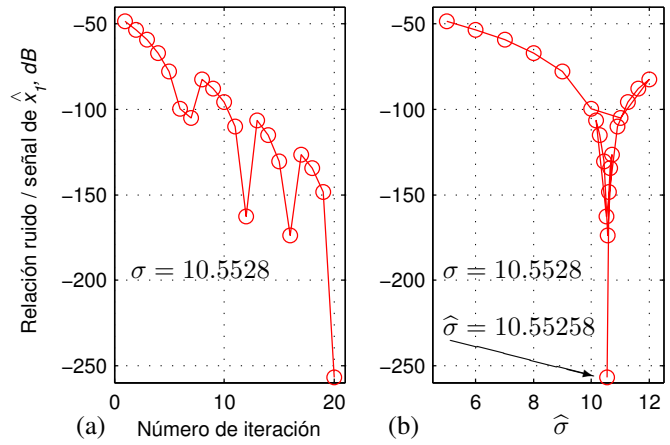

Fig. 2. Relación señal a ruido de $\widehat{x}_1$, en decibelios. (a) En función del número de iteración del algoritmo de recuperación. (b) En función de $\widehat{\sigma}$, para $\sigma = 10.5528$.

Inicio
variables: $t,\ x_1,\ x_2,\ x_3,\ \widehat{x}_1,\ \widehat{x}_2,\ \widehat{x}_3,\ \widehat{\sigma},\ \Delta\widehat{\sigma}$;
variables auxiliares: $ruido,\ ruido\_dB,\ ruido\_previo$;
valores iniciales transmisor: $x_1(0) = x_2(0) = x_3(0) = 1$;
valores iniciales receptor: $\widehat{x}_1(0) = \widehat{x}_2(0) = \widehat{x}_3(0) = 0$;
parámetros: $\sigma = 10.5528;\ r = 28;\ b = 8/3$;

Algoritmo 1 recupera_sigma $(\widehat{\sigma})$

Entrada: $\widehat{\sigma} = 4;\ \Delta\widehat{\sigma} = 1;\ ruido\_previo = 1$;
  mientras $ruido\_previo > -250$ **hacer**
    $\widehat{\sigma} = \widehat{\sigma} + \Delta\widehat{\sigma}$;
    calcula: $x_1(t);\ \widehat{x}_1(t)$;
    $ruido = \left(\frac{(x_1(t) - \widehat{x}_1(t)}{x_1(t)}\right)^2$;
    $ruido\_dB = 10\ \log\left(\text{promedio}\left(ruido(t = 5\ a\ t = 10)\right)\right)$;
    si $(ruido\_previo < ruido\_dB)$; **entonces**
      $\Delta\widehat{\sigma} = -\Delta\widehat{\sigma}/e$;
    fin si
    $ruido\_previo = ruido\_dB$;
  fin mientras
Salida: $\widehat{\sigma}$;

El programa anterior, prueba valores de $\widehat{\sigma}$, empezando por un extremo, con incrementos $\Delta\widehat{\sigma}$ relativamente grandes, en este caso de una unidad. Según se aproximan los valores de $\widehat{\sigma}$ al valor de σ, el error va disminuyendo. Pero cuando el valor de $\widehat{\sigma}$ rebasa al valor de σ, en uno o dos saltos, se produce un aumento del error, en ese momento, el algoritmo invierte el sentido de búsqueda y reduce el valor del incremento en un factor e —se ha elegido el número e, porque sería la base de numeración óptima y, por tanto, reduce el número de escalones de búsqueda al máximo—. Después, se repite el procedimiento, hasta alcanzar una potencia de error ínfima, en este caso se ha fijado un límite de -250 dB.

La Fig.2 ilustra el proceso de recuperación de $\widehat{\sigma}$, para $\sigma = 10.5528$. La Fig.2(a) presenta los sucesivos valores de la relación ruido/señal de la variable $\widehat{x}_1$, en función del tiempo; alcanzándose un valor final de -257 dB, al cabo de 20 iteraciones.

La Fig.2(b) presenta los sucesivos valores de la relación ruido/señal de la variable $\widehat{x}_1$, en función de $\widehat{\sigma}$, cuyo valor final es $\widehat{\sigma} = 10.55258\ldots$.

Este ataque —que se puede considerar de fuerza bruta— es muy diferente a la prueba exhaustiva de claves contra un cifrador digital correcto, en el que el error de sincronización es máximo para todos los valores de la clave, excepto para aquel en que todos sus bits son exactos. En cambio, en este caso, bastan 20 intentos para determinar la clave con suficiente precisión.

El tiempo total requerido para la determinación final de $\widehat{\sigma}$, en un PC con 2.8 GHz de frecuencia de reloj, es de 5.26 segundos. Por tanto se puede concluir que el sistema es totalmente inseguro.

En la Fig.3 se ilustra el valor instantáneo de la relación ruido/señal del mensaje recuperado $\widehat{s}(t)$ en función del tiempo.

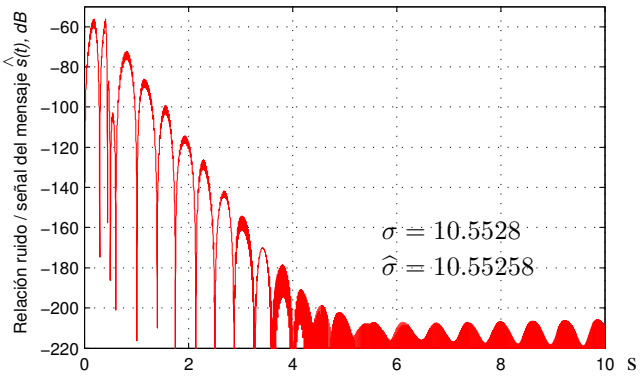

Fig. 3. Relación ruido/señal del mensaje en claro recuperado, en decibelios.

Puede observarse que, una vez transcurrido el transitorio inicial, que dura unos 5 segundos, la relación ruido/señal del mensaje claro recuperado $\widehat{s}(t)$ es aproximadamente de -205 dB.

IV. Caso de estudio III

Por último, en el tercer caso de estudio se propone un criptosistema que utiliza las mismas ecuaciones de cifrado (10) y descifrado (11) del caso II; pero en este caso el parámetro σ de la función de cifrado varía en función del tiempo. En el ejemplo presentado la ley de variación del parámetro σ oscila entre los valores 8, 9, 10, 11 y 12 en forma de escalera ascendente y descendente.

Los autores afirman que este método es mucho más seguro que los anteriores ya que,

- la variación temporal del parámetro, que hace el papel de clave, aumenta notablemente la robustez del procedimiento de cifrado,
- el atractor caótico del transmisor varía con el cambio del parámetro en el tiempo, dificultando los intentos de intrusión en el sistema.

El mensaje claro consiste en una secuencia binaria, en el que la duración de los bits es del mismo orden que la duración de los escalones del parámetro σ, para dificultar aún más el criptoanálisis. La amplitud de la secuencia se ha limitado al valor 0.01, con la intención de que no se pueda recuperar por filtrado.

V. Ataque al criptosistema: recuperación del mensaje claro

Para romper el criptosistema propuesto como caso III, se ha utilizado la siguiente ecuación:

$$\widehat{s}(t) = D(\widehat{X}, \widehat{\sigma}, s, t) = \frac{E(X, \sigma, s, t) - \widehat{x}_2^2}{\widehat{\sigma} + \widehat{x}_2^2}, \qquad (15)$$

que es similar a la que debe utilizar el receptor autorizado, con la única salvedad de que se desconocen los valores que adquiere en función del tiempo el parámetro σ. En su lugar, se utiliza un parámetro $\widehat{\sigma}$ de valor arbitrario constante.

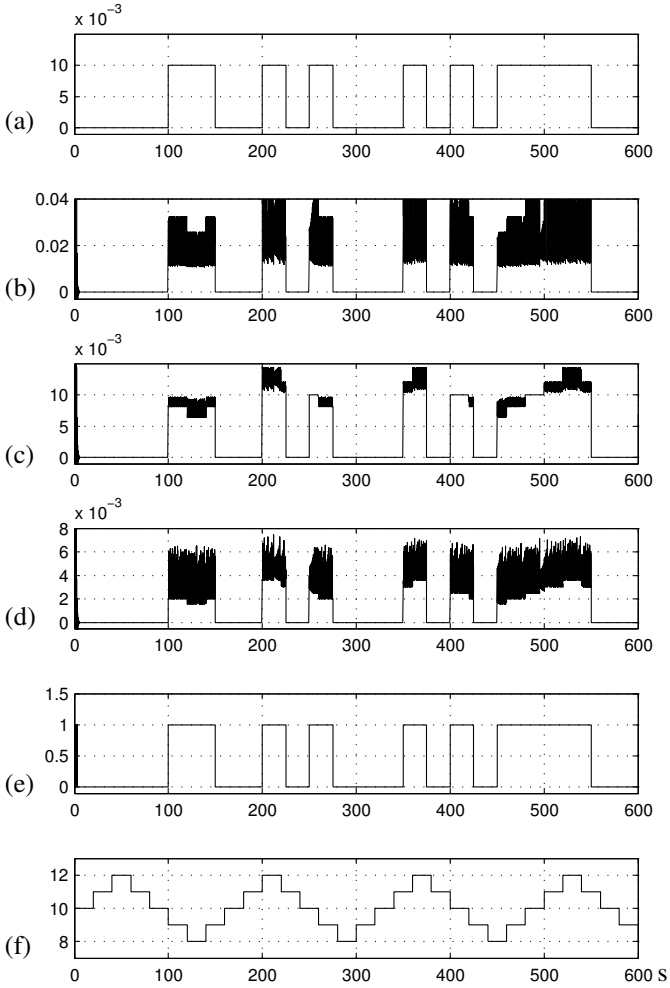

Fig. 4. Recuperación del mensaje para el caso III. (a) Mensaje claro. (b) Mensaje obtenido con $\widehat{\sigma} = 5$. (c) Mensaje obtenido con $\widehat{\sigma} = 10$. (d) Mensaje obtenido con $\widehat{\sigma} = 20$. (e) Mensaje recuperado a partir de cualquiera de los tres anteriores, mediante un comparador de nivel, con umbral 0.005. (f) Clave de cifrado σ.

El resultado se ilustra en la Fig. 4. Se han elegido tres valores diferentes para $\widehat{\sigma}$. Dos de ellos son el máximo y el mínimo para los cuales el sistema de Lorenz es caótico. Cuando $\rho = 28$ y $\beta = 8/3$, estos valores son $\widehat{\sigma} = 5$ y $\widehat{\sigma} = 20$. El tercer valor elegido es $\widehat{\sigma} = 10$, que coincide justamente con el valor central de los cinco que σ adquiere.

Se puede observar que, para los tres casos, el valor obtenido para $\widehat{s}(t)$ consiste en un impulso binario, igual al mensaje claro $s(t)$, sumado con unos paquetes de ruido de diversas amplitudes. Se puede comprobar que la amplitud de estos paquetes coincide con la diferencia de valores $|s(t) - \widehat{s}(t)|$. También se observa que en los momentos en que los valores de σ y $\widehat{\sigma}$ coinciden, el valor recuperado de $\widehat{s}(t)$ está limpio de ruido.

Para recuperar el mensaje claro, para cualquiera de los tres casos anteriores, basta con utilizar un comparador de nivel, regulado al valor 0.005. El mensaje finalmente recuperado aparece en la Fig. 4(e).

Hay que destacar, que el tiempo requerido para el ataque

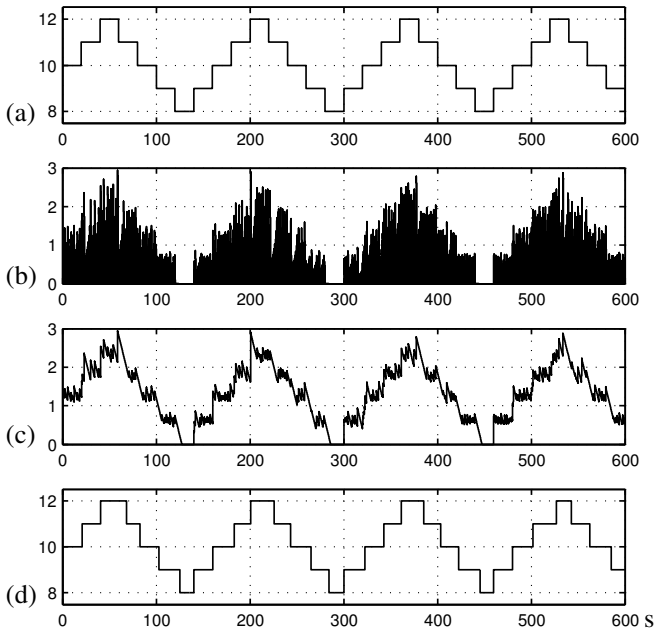

Fig. 5. Recuperación de la clave. (a) Clave de transmisión σ; (b) valor absoluto del error de sincronización $|x_1 - \widehat{x}_1|$, para $\widehat{\sigma} = 8$; (c) detección de envolvente de $|x_1 - \widehat{x}_1|$; (d) clave recuperada $\widehat{\sigma}$.

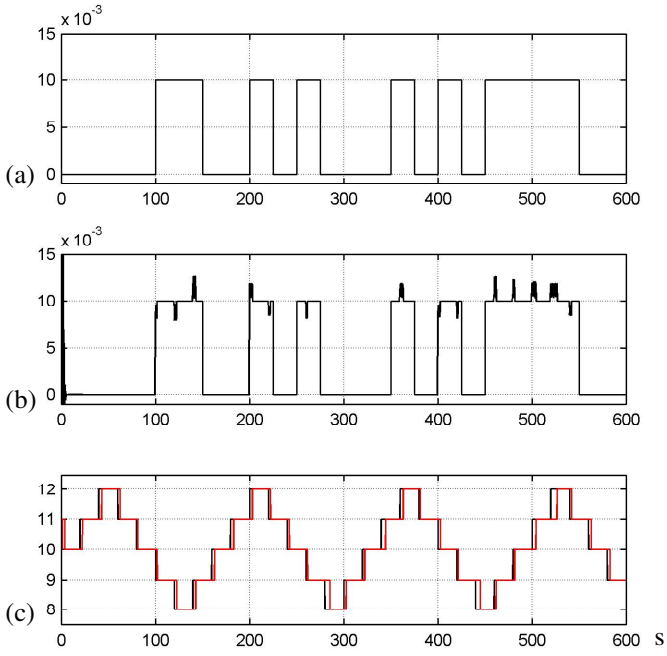

Fig. 6. Recuperación exacta del mensaje claro. (a) mensaje claro original; (b) mensaje recuperado; (c) clave de transmisión σ y clave recuperada $\widehat{\sigma}$, superpuestas.

es nulo, puesto que no es preciso probar varios valores de la clave $\widehat{\sigma}$, sino que basta utilizar cualquier valor comprendido dentro del rango admisible para que el sistema sea caótico.

A parte del transitorio inicial, debido a la diferencia de valores iniciales entre los integradores del emisor y el receptor, puede observarse que el mensaje recuperado coincide exactamente en tiempo con el mensaje original. Esto no ocurría en la figura 13 de [27], debido a que el sistema observador utilizado para recuperar el mensaje utilizaba un filtrado, con el consiguiente retardo.

VI. Determinación de la clave

También es posible determinar la clave de cifrado utilizada σ, con su variación temporal, utilizando el mismo receptor definido por las Eqs. (12), (13), (14), donde el parámetro $\widehat{\sigma}$ del receptor se elige inicialmente como una constante arbitraria en la zona central de los valores admisibles para σ.

La Fig. 5 ilustra el proceso de recuperación de la clave. En la Fig. 5(b) se representa la diferencia $|x_1 - \widehat{x}_1|$, que proporciona el valor absoluto de la señal de error de recuperación de la variable x_1. En los momentos en que coinciden los valores de los parámetros σ y $\widehat{\sigma}$ el error es nulo; mientras que cuando no coinciden, se produce un ruido de magnitud proporcional a la diferencia de valores $|\sigma - \widehat{\sigma}|$. En la Fig. 5(c) se presenta el resultado de aplicar un detector de envolvente al error absoluto $|x_1 - \widehat{x}_1|$. La recuperación de la clave se efectúa mediante cuatro comparadores de nivel (disparador de Schmitt) que detectan los saltos de los escalones.

En el ejemplo de la figura se ha elegido un valor de parámetro de recepción $\widehat{\sigma} = 8$ coincidente con el escalón inferior de σ, aunque también se podría haber elegido el valor del escalón superior $\widehat{\sigma} = 12$. La selección del parámetro $\widehat{\sigma}$ se hace por prueba y error, ajustándolo hasta que se encuentra que el escalón inferior de la Fig. 5(b) es idéntico a cero y libre de ruido. La reconstrucción de la clave $\widehat{\sigma}$ se ha hecho sumando los escalones detectados, mediante el comparador de nivel, con el valor de $\widehat{\sigma} = 8$ utilizado. La amplitud de los escalones se ha ajustado para conseguir un mensaje claro $\widehat{s}(t)$ con el menor ruido posible.

En la Fig. 6 se presenta el mensaje recuperado cuando en la Eq. (15) se utiliza la clave recuperada $\widehat{\sigma}$. Puede observarse en la Fig. 6(b) que hay unos pequeños picos de ruido superpuestos al mensaje recuperado, debidos al desfase entre la clave de transmisión σ y clave recuperada $\widehat{\sigma}$; tal desfase se debe al retraso ocasionado por el detector de envolvente; la Fig. 6(c) presenta las dos claves pudiendo observarse el ligero desfase.

Naturalmente, los picos de ruido desaparecerán en el momento que el tren de impulsos se descreste, igualmente a como se hizo para recuperar el mensaje en la Fig. 4(e).

VII. Implementación del sistema

En el artículo [27] se describe una forma de realizar este criptosistema caótico mediante circuitos analógicos, tanto en transmisión como en recepción, empleando resistencias y condensadores. Los valores de estos componentes determinan los valores de los parámetros y, por tanto, de la clave; pero, lamentablemente, es imposible conseguir componentes con una exactitud mejor que el 0.1 %. Lo que ocasiona un ligero desajuste entre los valores de los parámetros del transmisor y el receptor.

Para que el sistema legítimo pueda sincronizarse, los receptores autorizados deben de tener forzosamente un amplio

margen de enganche frente a los desajustes de los parámetros, lo que se consigue gracias a que el coeficiente de Liapunov condicional del sistema formado por las Eqs. (1), (2), (3) y las Eq. (4) a (7) es negativo, por tanto convergente frente a ligeros desajustes. Esto permite atacar el sistema con receptores intrusos, cuyos parámetros —es decir la clave— se pueden ir reajustando experimentalmente, mientras se observa el ruido de recepción hasta lograr eliminarlo, lo que supone haber determinado la clave.

VIII. Conclusión

El criptosistema caótico continuo de dos canales basado en una función no lineal es inseguro en sus tres versiones posibles, pudiéndose determinar fácilmente el mensaje cifrado y la clave utilizada. Una vez más, se demuestra que los denominados *sistemas de comunicaciones seguros basados en caos continuo*, dependientes de la sincronización de los sistemas transmisor y receptor, son inseguros.

Su principal defecto es la baja sensibilidad a la clave secreta, lo que en realidad es un requisito indispensable para el funcionamiento de las realizaciones reales de cualquier criptosistema caótico analógico ya que como se ha explicado anteriormente, es prácticamente imposible garantizar el ajuste exacto entre los sistemas emisor y receptor.

Agradecimientos

Los autores agradecen su ayuda al Plan Nacional de I+D+i, Tecnologías Informáticas, proyecto TIN2011-22668: Secure Identification and Authentication In Electronic Communications (IDEASEC).

Referencias

[1] G. Alvarez, L. Hernandez, J. Muñoz, F. Montoya, and S. Li, "Security analysis of a communication system based on the synchronization of different order chaotic systems," *Phys. Lett. A*, vol. 345, no. 4–6, pp. 245–250, 2005.

[2] G. Alvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalysis of a chaotic encryption system," *Phys. Lett. A*, vol. 276, no. 1–4, pp. 191–196, 2000.

[3] ——, "Cryptanalyzing an improved security modulated chaotic encryption scheme using ciphertext absolute value," *Chaos Soliton. Fract.*, vol. 23, no. 5, pp. 1749–1756, 2005.

[4] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129–2151, August 2006.

[5] J. Amigó, "Chaos-based cryptography," in *Intelligent Computing Based on Chaos*, ser. Studies in Computational Intelligence, L. Kocarev, Z. Galias, and S. Lian, Eds. Springer Berlin-Heidelberg, 2009, vol. 184, pp. 291–313.

[6] X.-L. An, J.-N. Yu, Y.-Z. Li, Y.-D. Chu, J.-G. Zhang, and X.-F. Li, "Design of a new multistage chaos synchronized system for secure communications and study on noise perturbation," *Mathematical and Computer Modelling*, vol. 54, no. 1–2, pp. 7–18, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0895717711000355

[7] F. Dachselt and W. Schwarz, "Chaos and cryptography," *IEEE Trans. Circuits Syst. I-Fundam. Theor. Appl.*, vol. 48, no. 12, pp. 1498–1509, 2001.

[8] H. Dimassi, A. Loría, and S. Belghith, "A new secured transmission scheme based on chaotic synchronization via smooth adaptive unknown-input observers," *Communications in Nonlinear Science and Numerical Simulation*, no. 0, 2012.

[9] Z.-P. Jiang, "A note on chaotic secure communication systems," *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on*, vol. 49, no. 1, pp. 92–96, 2002. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=974882

[10] L. Kocarev, "Chaos-based cryptography: a brief overview," *IEEE Circuits and Sistems Magazine*, vol. 1, no. 3, pp. 6–21, 2001.

[11] G. Kun, "A synchronization controller for the unified chaotic system and its application in secure communication," in *Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference on*, april 2011, pp. 4700 –4703.

[12] Q. Lawande, B. Ivan, and S. Dhodapkar, "Chaos based cryptography: a new approach to secure communications," *BARC Newsletter*, vol. 258, no. 258, 2005.

[13] S. Li, "Analyses and new designs of digital chaotic ciphers," Ph.D. dissertation, Xi'an Jiaotong University, 2003.

[14] S. Li, G. Chen, and G. Alvarez, "Return map cryptanalysis revisited," *I. J. Bifurcation and Chaos*, vol. 16, no. 5, pp. 1557–1568, 2006. [Online]. Available: http://dx.doi.org/10.1142/S0218127406015507

[15] J. L. Mata-Machuca, R. Martínez-Guerra, R. Aguilar-López, and C. Aguilar-Ibañez, "A chaotic system in synchronization and secure communications," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 4, pp. 1706 – 1713, 2012.

[16] W. Mu, B. Cui, X. Lou, and H. Zhu, "Adaptive synchronization of time-delayed chaotic systems and its application to secure communication," in *Information Sciences and Systems (CISS), 2011 45th Annual Conference on*, march 2011, pp. 1 –5.

[17] A. Orúe, V. Fernández, G. Pastor, M. Romera, G. Alvarez, and F. Montoya, "Criptoanálisis de un cifrador caótico realizado con redes neuronales celulares," in *RECSI*, A. M. L. Hernandez, Ed., 2008, pp. 163–171.

[18] A. Orue, G. Alvarez, G. Pastor, M. Romera, F. Montoya, and S. Li, "A new parameter determination method for some double-scroll chaotic systems and its applications to chaotic cryptanalysis," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 11, pp. 3471–3483, 2010. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1007570409006534

[19] A. Orue, V. Fernandez, G. Alvarez, G. Pastor, M. Romera, S. Li, and F. Montoya, "Determination of the parameters for a Lorenz system and application to break the security of two-channel chaotic cryptosystems," *Physics Letters A*, vol. 372, no. 34, pp. 5588–5592, 2008. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S0375960108009663

[20] J. Pan, Q. Ding, and B. Du, "The optimization scheme of chaotic masking secure communication based on lorenz system," in *Chaos-Fractals Theories and Applications (IWCFTA), 2010 International Workshop on*, oct. 2010, pp. 154 –158.

[21] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–824, 1990.

[22] L. Pecora and T. Carroll, "Driving systems with chaotic signals," *Physical Review A*, vol. 44, no. 4, p. 2374, 1991.

[23] C. Rîncu and A. Serbanescu, "Chaos-based cryptography. a possible solution for information security," *Bulletin of the Transilvania University of Brasovia*, vol. 2, no. 51, p. 51, 2009. [Online]. Available: http://but.unitbv.ro/BU2009/BULETIN2009/Series III/BULETIN III PDF/rincu.pdf

[24] C. Shannon, *Communication theory of secrecy systems*. AT and T, 1949, no. 1. [Online]. Available: http://202.38.64.11/ whli/lecture-crypto-pb/materials/Communication Theory of Secrecy Systems.pdf

[25] N. Smaoui, A. Karouma, and M. Zribi, "Secure communications based on the synchronization of the hyperchaotic chen and the unified chaotic systems," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 8, pp. 3279–3293, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1007570410005538

[26] H. Wang, X.-J. Zhu, S.-W. Gao, and Z.-Y. Chen, "Singular observer approach for chaotic synchronization and private communication," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 3, pp. 1517–1523, 2011. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1007570410003497

[27] A. Zaher and A. Abu-Rezq, "On the design of chaos-based secure communication systems," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 9, pp. 3721–3737, 2011. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1007570411000037