Identificación, síntesis y análisis de Sistemas Criptográficos basados en caos

Por el Dr. Javier Areitio Bertolín y la Dra. Gloria Areitio Bertolín

Prof. Dr. Javier Areitio Bertolín – E.Mail: jareitio@eside.deusto.es
Catedrático de la Facultad de Ingeniería. ESIDE. Director del Grupo de Investigación Redes y Sistemas. Universidad de Deusto.
Prof. Dra. Gloria Areitio Bertolín – E. Mail: gloria.areitio@ehu.es
Laboratorio de Informática Aplicada. Universidad del País Vasco (UPV / EHU)

En el presente artículo se examinan los criptosistemas del tipo caótico. El caos es una de las áreas de las matemáticas que explora la dinámica no lineal. Tras definir los sistemas caóticos y vincularlos con la criptografía se sintetizan criptosistemas caóticos de diversos tipos: simétricos estilo OTP basados en RNGs/PRNGs y asimétricos o de clave pública estilo EG. Se identifican las principales propiedades y características de los criptosistemas caóticos. Se explora la criptografía caótica, sus ventajas, inconvenientes y criterios críticos. En criptosistemas caóticos, el cifrado se puede realizar directamente en hardware con señales de audio y video en tiempo real, sin necesidad de conversores A/D-D/A. El caos se puede utilizar para construir cifradores, generadores de números pseudoaleatorios, firma digital convencional y a ciegas, funciones unidireccionales hash, protocolos ZK, etc.

El caos puede definirse como la tendencia de los sistemas iterativos, simples, deterministicos a ser muy sensibles a las condiciones iniciales y a ser altamente no predecibles. El elemento central de todos los sistemas caóticos (o basados en caos) es el concepto de iteración. El estado actual del sistema es una función deterministica del estado o valor anterior. Formalmente una correspondencia caótica se especifica por medio de la expresión: $x_{n+1} = f(x_n)$, donde $f( )$ es una función no lineal. En general, la teoría del caos surge de las matemáticas de modelización de mecanismos físicos tales como la predicción del tiempo atmosférico, la evolución de la población, la dinámica de fluidos, la teoría de gases, etc. Todos los ejemplos anteriores son sistemas iterativos por naturaleza, por ejemplo la población de los próximos años es una función de la de este año. Se ha observado que los modelos más simples producen un comportamiento altamente no lineal de modo que variando las condiciones iniciales una cantidad pequeña puede tener unos efectos completamente impredecibles después de varias iteraciones.

Todo sistema caótico es muy sensible a las condiciones iniciales y genera un comportamiento aparentemente aleatorio pero a la vez completamente determinístico. Estas propiedades del caos proporcionan un potencial para aplicaciones en criptografía ya que las predicciones a largo plazo de los sistemas caóticos son muy difíciles. El hecho de que sea determinístico significa que se puede obtener el mismo conjunto de valores siempre que se disponga de la misma función de correspondencia caótica y de su valor inicial. El caos en generación de números aleatorios permite repetir la misma cadena de números siempre que se utilice la misma función de correspondencia caótica (o attractor) y valor inicial o semilla. La apariencia aleatoria del sistema hace prácticamente imposible los ataques del tipo codebook (un codebook contiene todas las posibles transformaciones entre texto en claro y texto cifrado bajo cada clave). Puesto que las funciones caóticas son muy sensibles a las condiciones iniciales, cualquier ligera diferencia en el valor inicial empleado, significará que el texto cifrado producido utilizando caos será muy diferente. Esto significa que el sistema será robusto contra ataques por fuerza bruta, ya que el número de posibles claves es impresionantemente grande, dependiendo de la precisión de los valores iniciales que estarán en función del hardware utilizado, y que puede ser más o menos elevado según el dominio sea analógico o digital.

La idea de utilizar el caos para construir sistemas de cifrado data de 1989. Últimamente los algoritmos de cifrado de imágenes basados en caos se construyen en base a tres grandes planteamientos: con permutación de posición, con sustitución de valor y una combinación de los casos anteriores. Existen dos clases de cifradores caóticos:

(1) Criptosistemas basados en técnicas de sincronización de caos de circuitos analógicos.

(2) Cifradores basados en caos realizados sobre circuitos digitales, DSPs y computadores, en este último caso existe un efecto de precisión finita.

Síntesis y tipos de criptosistemas caóticos.

Describamos el funcionamiento de un posible sistema criptográfico digital basado en caos: supongamos que el texto en claro que se va a cifrar se encuentra en forma de números enteros. En primer lugar se define una función o mapa caótico discreto, por ejemplo se selecciona un logistic map. Seguidamente se define un número entero n como la clave que será el valor inicial de la función caótica. De esta forma para el primer carácter del texto cifrado se utilizará n como el valor inicial y el primer número entero del texto en claro como el número de iteraciones para obtener el carácter cifrado. El siguiente carácter de texto cifrado se obtendrá utilizando el carácter de texto cifrado previo como valor inicial mientras se itera el número de veces indicado por el carácter de texto en claro presente. En este desarrollo el cifrador es la función caótica, la clave es n (primer valor inicial), el número de iteraciones a realizar es el número entero del texto en claro correspondiente y el valor inicial utilizado es el número obtenido de la iteración anterior. En este criptosistema cualquier cambio en el texto en claro afectará a la parte restante del texto cifrado. Esto asegura un efecto de difusión en el criptosistema. Los caracteres del texto cifrado no sólo dependerán de la clave sino también del texto en claro. De este modo también existen elementos de confusión en el criptosistema desarrollado.

Por consiguiente los ataques estadísticos contra el criptosistema serían difíciles con tal que la función caótica del criptosistema no se revele.

En la actualidad, existen dos clases de criptosistemas caóticos:

(1) Analógicos o continuos. Se utilizan mapas caóticos continuos como el mapa de Lorenz. El proceso de cifrado se realiza sumando la señal del mensaje analógica a la salida del mapa caótico. El proceso de descifrado se realiza restando la señal cifrada de la salida de un mapa caótico sincronizado. La señal cifrada toma el aspecto de ruido ya que se ha mezclado con una señal caótica.
(2) Digitales o discretos. Se utilizan mapas caóticos discretos como el logistic map como función de mixing. La información puede considerarse una cadena de números enteros. El primer valor puede utilizarse como punto inicial del mapa. El proceso de cifrado iterara el punto inicial un número predeterminado de veces especificado por la clave y el punto obtenido será el texto cifrado. El proceso de descifrado consiste en realizar sobre el texto cifrado el mismo número de iteraciones inversas utilizando el mismo mapa caótico y el punto resultante es el texto en claro buscado.

Otra forma de clasificar a los criptosistemas caóticos es atendiendo a como se utiliza el mapa caótico:
(a) Se puede utilizar como ruido aleatorio que se envía a la salida, por ejemplo en sistemas simétricos estilo OTP.
(b) Se puede utilizar como función de mixing sobre el texto en claro, por ejemplo en sistemas asimétricos.

GENERACIÓN DE CLAVES DEL RECEPTOR:

- Cada usuario posee una clave pública formada por la tupla de elementos: (p, a_0, a_n, correspondencia caótica). Donde la correspondencia caótica puede ser muy variada, por ejemplo: $a_{n+1} = a^2_n \bmod p$, o bien, $a_{n+1} = (a^r_n + d) \bmod p$, donde r y d son conocidas.
- La clave privada es el valor n.

PROCESO DE CIFRADO EN EL EMISOR:

- El emisor genera de forma aleatoria un número entero k e itera el sistema caótico desde a_0 durante k veces hasta obtener a_k.
- Asi mismo itera a_n hasta obtener a_{n+k}.
- El texto cifrado se obtiene de las expresiones: $c_1 = a_k$; $c_2 = (m \cdot a_{n+k}) \bmod p$, donde m es el texto en claro a cifrar.

PROCESO DE DESCIFRADO EN EL RECEPTOR:

- El receptor descifra con su clave privada n. Para ello itera la función caótica desde $c_1 = a_k$ n-veces hasta obtener $s = a_{n+k}$.
- A continuación se obtiene el texto en claro m utilizando la expresión $m = (c_2 \cdot s^{-1}) \bmod p$.

EJEMPLO:

- Claves del receptor:
  - Clave pública: ($p = 7919$, $a_0 = 2$, $a_n = 256$, $a_{n+1} = a^2_n \bmod p$)
  - Clave privada: $n = 3$
- Cifrar el mensaje $m = 3$: Sea $k = 2$. Itera a_0 hasta $a_k = a_2 = 16$. Itera a_n hasta obtener $a_{n+k} = a_5 = 2618$ donde $a_4 = 2184$. $c_1 = a_k = 16$; $c_2 = (m \cdot a_{n+k}) \bmod p = (3 \cdot 2618) \bmod 7919 = 7854$
- El descifrado es: desde $c_1 = a_k = 16$, $n = 3$ veces hasta obtener $s = a_{n+k} = a_5 = 2618$. Luego $m = (c_2 \cdot s^{-1}) \bmod p = (7854 \cdot 2618^{-1}) \bmod 7919 = 3$.

Fig. 1.- Síntesis de un criptosistema caótico asimétrico, discreto, estilo E-G.

Propiedades de los sistemas caóticos y su relación con las de los sistemas criptográficos.

Un sistema caótico es un sistema dinámico, no lineal, determinístico que muestra una dependencia muy sensible a las condiciones iniciales y presenta una evolución a través de un espacio de fase que parece ser aleatorio. Las principales propiedades de un sistema caótico son:
(1) Es topológicamente transitivo.
(2) Presenta una densa colección de puntos con órbitas periódicas.
(3) Es sensible a la condición inicial del sistema. Inicialmente los puntos cercanos del sistema pueden evolucionar muy rápidamente en grandes trayectorias diferentes. Esta propiedad se denomina efecto mariposa. Como resultado de la sensibilidad, el comportamiento de los sistemas caóticos parece ser aleatorio, exhibiendo una dispersión de error exponencial. Presenta una elevada dependencia de las condiciones iniciales, pequeños cambios pueden conducir a un comportamiento totalmente diferente en

un corto intervalo de tiempo. Por tanto la predicción a largo plazo es prácticamente imposible debido a la sensibilidad a las condiciones iniciales, esta característica es interesante en criptografía en donde se utilizan señales muy complejas y difíciles de predecir.

(4) El caos es un comportamiento que se sitúa entre la rígida regularidad y la aleatoriedad.

(5) La dinámica de señales caóticas son similares al ruido pero deterministicas, con naturaleza compleja, elevado ancho de banda y aperiódicas.

DCS (DISCRETE CHAOTIC SEQUENCE):

- $x_{n+1} = (1 - u \cdot x_n^{\,2})$
  donde el parámetro u pertenece al intervalo [0, 2],
  x_n pertenece al intervalo [-1, 1],
  x_0 es la condición inicial de computación o semilla.
  Cuando u se encuentra entre 1,41 y 2 la correspondencia presenta comportamiento caótico. Esta DCS es no periódica y diferentes DCSs no están correlacionadas. En base al par (u, x_0) se generan las claves pública y privada.

AUTOMORFISMO TOROIDAL:

- $\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = A \cdot \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod K$

  la matriz del automorfismo es $A = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix}$ y el tamaño del reticulo es de K puntos (x_i, y_i). Es periódico y se utiliza en sistemas caóticos. Clave K y subclave k.

LOGISTIC MAP:

- $x_{n+1} = A \cdot x_n \cdot (1 - x_n)$
  donde $x_n \in [0, 1]$; la condición de estado caótico es: $3{,}99465 < A \leq 4$, x_0 es la semilla inicial, por ejemplo 0,83.

TENT MAP:

- $x_{n+1} = (k \cdot x_n)$ para $x_n < 1/2$ $x_{n+1} = k.(1 - x_n)$ para $x_n \geq 1/2$
  donde k número real positivo y $x_n \in [0, 1]$;

CHEBYSHEV MAP DE GRADO k:

- $x_{n+1} = \cos(2^k \cdot \cos^{-1} x_n)$ donde $x_n \in [-1, 1]$; $k \geq 2$.

BERNOULLI MAP:

- $x_{n+1} = (2 \cdot x_n) \bmod 1$ donde $x_n \in [0, 1]$; ( ) mod 1 significa descartar la parte entera del número real.

Fig. 2.- Diferentes mapas o funciones caóticas (*atractores*) para desarrollar sistemas criptográficos caóticos.

(6) En el dominio analógico, poseen propiedades no periódicas, no convergentes y ergódicas.

(7) Los criptosistemas basados en sistemas caóticos cumplen las propiedades de Shannon de difusión y confusión. Claude Shannon enunció dos propiedades que debería tener todo sistema criptográfico para impedir el análisis estadístico:

(a) Confusión. Significa que la clave no se relaciona de una forma simple con el texto cifrado. En concreto, cada carácter del texto cifrado debería depender de varias partes de la clave. El uso de transformaciones debería complicar la dependencia de las estadísticas del texto cifrado con las estadísticas del texto en claro.

(b) Difusión. Significa que el cambio de un carácter en el texto en claro debería afectar a varios caracteres del texto cifrado, y recíprocamente el cambio de un carácter del texto cifrado debería afectar a varios caracteres del texto en claro.

Existe una cierta relación entre las propiedades de los sistemas caóticos y la de los sistemas criptográficos tradicionales:

1) La propiedad que señala que un proceso deterministico puede causar comportamiento aleatorio/pseudoaleatorio, en los sistemas caóticos hace referencia a la propiedad denominada dinámica determinista y en los sistemas criptográficos se corresponde con la propiedad denominada pseudoaleatoriedad determinista.

2) La propiedad que indica que la salida tiene la misma distribución para cualquier entrada, en los sistemas caóticos hace referencia a la propiedad denominada ergodicidad (es la convergencia del valor medio sobre la trayectoria al valor medio del conjunto) y en los sistemas criptográficos se corresponde con la propiedad denominada confusión (acuñada por Shannon).

3) La propiedad que señala que una pequeña desviación en la entrada puede causar un gran cambio en la salida, en los sistemas caóticos hace referencia a la propiedad denominada sensibilidad

a las condiciones iniciales / parámetro de control y en los sistemas criptográficos se corresponde con la propiedad denominada difusión con un pequeño cambio en el texto en claro / clave secreta.
4) La propiedad que indica que una pequeña desviación en el área local puede causar un gran cambio en todo el espacio, en los sistemas caóticos hace referencia a la propiedad denominada mixing (garantiza la convergencia desde el estado local de no equilibrio, al estado de equilibrio, es decir para cualquier texto cifrado todos los posibles textos en claro de un ataque por fuerza bruta son equiprobables) y en los sistemas criptográficos se corresponde con la propiedad denominada difusión con un pequeño cambio en un bloque en claro de todo el texto en claro.
5) La propiedad que señala que un proceso simple posee una complejidad muy elevada en los sistemas caóticos hace referencia a la propiedad denominada complejidad de estructura y en los sistemas criptográficos se corresponde con la propiedad denominada complejidad del algoritmo.

Mapas-funciones caóticas discretas. Propiedades estadísticas de sistemas caóticos digitales.

Se define un sistema dinámico no lineal de tiempo discreto, de una dimensión por medio del par (I, f) donde I representa un intervalo real y f una transformación escalar iterativa, no lineal de I a I:

$$x_{i+1} = f(x_i)$$

donde $\{x_i\}$ es la secuencia caótica generada por f. Así mismo x_i con i mayor o igual a cero determina los estados del sistema dinámico y x_0 representa la condición inicial o semilla. Uno de los sistemas caóticos más conocidos y utilizados es la secuencia denominada mapa logístico o logístic map:

$$f(x) = A.x.(1 - x)$$

donde x pertenece al intervalo entre cero y uno. Se ha demostrado que el sistema esta en estado caótico si el valor de A es mayor que 3,99465 y menor o igual que 4.

Cuando un sistema caótico se realiza sobre computadores digitales con precisión de computación finita, sus propiedades dinámicas serán diferentes de las que presentan los sistemas de valores continuos en el dominio analógico. Los problemas típicos son:
(1) Longitud del ciclo más corto.
(2) Degradación en la distribución y correlación. Aunque se ha identificado el problema no existe aún una teoría establecida para medir la degradación dinámica de los sistemas caóticos digitales que da lugar a defectos potenciales, para ello se utilizan tests experimentales al no existir una herramienta teórica.

Ventajas de los criptosistemas caóticos.

Las principales ventajas de los criptosistemas caóticos son:
(1) Resistencia a las formas tradicionales de ataques. Debido a la naturaleza de las funciones caóticas o attractors, los métodos ordinarios de criptoanálisis no tienen aplicación aquí. El criptoanálisis normal utiliza diferentes métodos como análisis estadístico, búsqueda exhaustiva por fuerza bruta y se aprovecha de las debilidades del algoritmo criptográfico. Sin embargo, los métodos establecidos realmente no pueden aplicarse a la criptografía caótica debido al hecho de que el caos es inmune a los ataques estadísticos debido a su naturaleza aleatoria. De hecho la fuerza bruta no es adecuada ya que el posible intervalo de valores de la clave se define sobre un campo de números continuo, comparado con los métodos que seleccionan una clave de un gran campo de números enteros discreto pero finito. La debilidad en el algoritmo puede contrarrestarse utilizando formas más ingeniosas de cifrar el mensaje.
(2) Facilidad a la hora de incrementar la variedad de algoritmos. Debido a la posibilidad de un gran número de parámetros, la criptografía caótica puede proporcionar una estructura de la que pueden ser utilizadas miles de funciones o mapas caóticos, de este modo se diversifica el número de formas que puede codificarse el mensaje. Los criptosistemas tradicionales emplean algoritmos que sólo incrementan la difusión y confusión de la linealidad del criptosistema con un incremento lineal de iteraciones o longitud de clave, en cambio la crip-

Criptografía clásica	Criptografía caótica
Utiliza métodos algebraicos, valores discretos sobre campos finitos modulares	Utiliza métodos analíticos y valores continuos. Puede utilizar valores discretos.
Realización digital por medio de aritmética de números enteros.	Realización digital por medios tanto de aritmética no entera (números reales en coma flotante) como por medio de aritmética de números enteros.

Fig. 3.- Comparativa entre la criptografía clásica y la basada en caos.

tografía caótica presenta mejores propiedades en esta área. Por tanto, simplemente buscando cualquier función con términos de realimentación y propiedades caóticas se puede llegar a obtener muchas más formas de cifrar.

(3) Dificultad para detectar picos espectrales. Las funciones caóticas tienen apariencia aleatoria pero determinísticas. Intentando el análisis estadístico sobre la señal cifrada se debería comparar para tratar de analizar su representación en el dominio frecuencial para encontrar picos en el espectro que permitan obtener de alguna forma las características de las propiedades de la función de cifrado.

(4) Adecuado para su implementación en sistemas analógicos con máxima precisión. La ventaja más clara de la criptografía caótica frente a los criptosistemas tradicionales es el hecho de que puede implementarse directamente en hardware (circuitos específicos, computadores analógicos de propósito general) sin tener que recurrir a utilizar conversión digital a analógica. Como cualquier forma de conversión implica pérdida de precisión es deseable tener mucha mayor precisión como sea posible cuando se representa el texto del mensaje en forma cifrada. Una implementación física de una función caótica puede construirse en forma de un circuito hardware denominado oscilador Van der Pol u oscilador Chua. De esta forma es posible tener un algoritmo de cifrado que no se encuentre limitado por la tecnología o velocidad de los computadores actuales y poder operar sobre señales analógicas continuas, sin problemas a elevada velocidad.

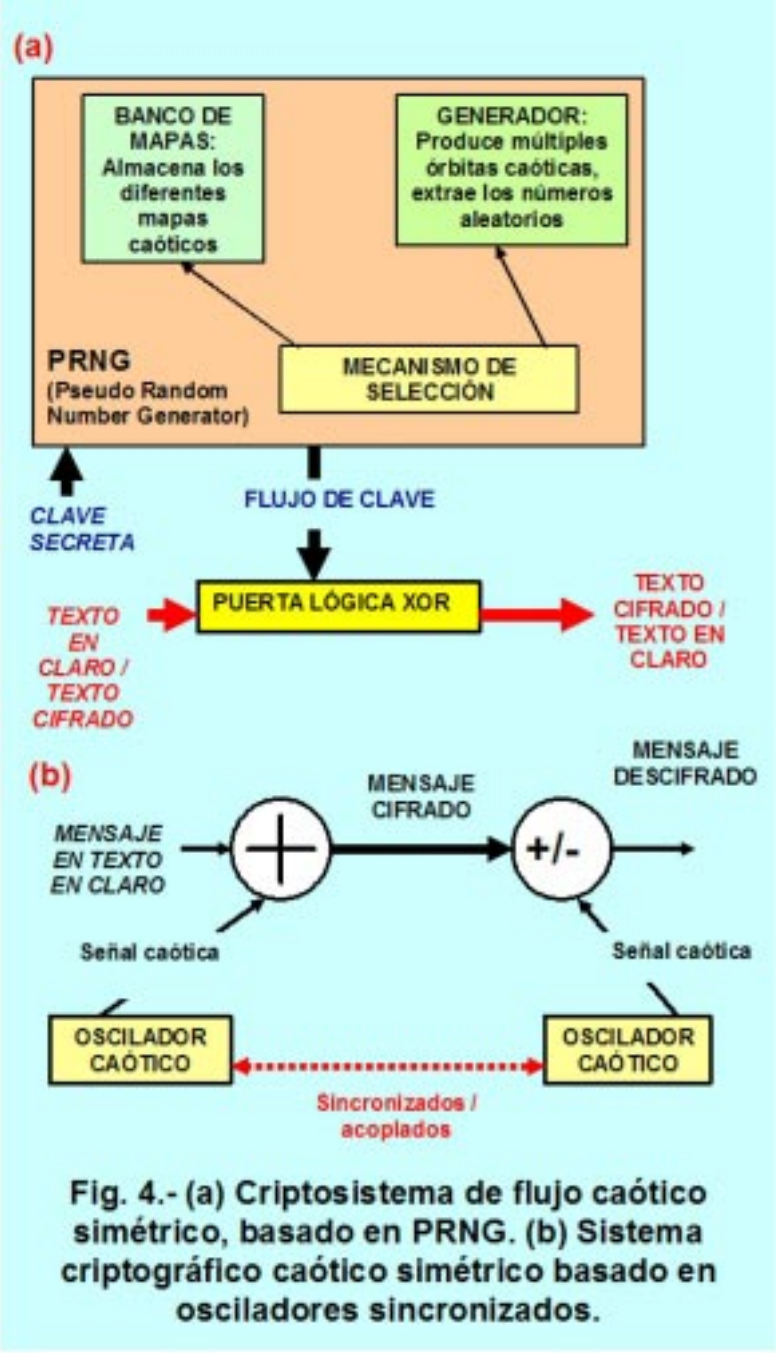

Fig. 4.- (a) Criptosistema de flujo caótico simétrico, basado en PRNG. (b) Sistema criptográfico caótico simétrico basado en osciladores sincronizados.

Inconvenientes de los criptosistemas caóticos.

Las principales inconvenientes de los criptosistemas caóticos son:

(1) La dificultad del criptoanálisis es una debilidad. La criptografía caótica es resistente al criptoanálisis convencional, debido a esta dificultad la seguridad del criptosistema caótico no puede ser cuantificada fácilmente y por tanto el nivel de seguridad no está aún muy bien caracterizado. En cambio en los criptosistemas tradicionales, como por ejemplo en RSA, la seguridad esta basada en la dificultad de factorizar números muy grandes en sus dos factores primos p y q.

(2) Los mensajes muy largos pueden hacer inseguro al sistema. El sistema puede ser inseguro para cifrar mensajes muy largos. Esta debilidad se debe

al hecho de que la función caótica puede repetirse o ir en órbita para varias condiciones iniciales. Si se observa la salida del algoritmo de cifrado que opera con los mismos parámetros para muchos mensajes diferentes, puede ser posible reconstruir parte o toda la correspondencia caótica utilizada para combinar todas las órbitas posibles observadas a partir de la salida cifrada. La forma práctica de hacer es intentar recuperar el gráfico del espacio de fase del sistema, creando un gráfico de la n-ésima muestra contra la n+1-ésima muestra del mensaje cifrado. Se han desarrollado diversas técnicas con cierto éxito para encubrir esta debilidad.

(3) Presenta algunos problemas de implementación práctica. Incluso aunque se consiga un criptosistema caótico perfecto en teoría, la implementación práctica puede ser fuente de problemas tanto en los dominios analógico como digital:

(a) En el dominio analógico, se presenta el problema del ruido. El ruido es una anomalía inherente en todos los sistemas cuya temperatura ambiente se encuentre por encima del cero absoluto (-273ºC = 0ºK) lo cual es inevitable. Dado que las funciones caóticas son muy sensibles a las condiciones iniciales, es difícil de hecho poder construir dos generadores caóticos basados en hardware idénticos y sincronizados ya que el ruido tenderá a des-sincronizarlos. La re-sincronización regular de los dos generadores es necesaria pero puede llegar a convertirse en un punto débil del sistema.

(b) Para sistemas digitales. Cuando se selecciona una clave para cifrar o codificar los bits del mensaje sólo se puede cuantificar los datos en un campo de números finitos. Esto significa que en vez de tener un campo de números continuo (como el conjunto de los números reales R) para operar, se esta limitado a un subconjunto del infinito (campo de números continuo), que simplemente fuerza a la función caótica a una órbita periódica lo cual no ocurre con las órbitas caóticas del dominio analógico.

(4) La diferente representación de los números en diferentes plataformas hardware que tiene que ver con los números en coma flotante. Los números en coma flotante son números reales con un número fijo de dígitos que representan el número, un exponente (normalmente en base diez) y una coma decimal flotante. Aunque existen estándares del IEEE que tratan de la representación de números en coma flotante en binario, se presentan problemas de implementación cuando los microprocesadores tienen tamaños de datos diferentes desde 4 bits a 128 bits, lo que hace imposible estandarizar las formas de calcular los números. Aunque hay algunas formas de solucionarlo se requiere un cierto esfuerzo.

Sistemas dinámicos continuos	Sistemas dinámicos discretos
Cifrado de mensajes con modulación de trayectorias	Cifrado de texto en claro con n-ésima inversa iteración de una correspondencia caótica.
Descifrado de un texto cifrado por sincronización de dos sistemas o filtrado de trayectorias moduladas	Descifrado de un texto cifrado con la n-ésima iteración de una correspondencia caótica.
Herramientas aplicadas: sincronización de dos sistemas caóticos y control del caos.	Herramientas aplicadas: caos y teoria ergódica. Dos enfoques: • Incluir la clave secreta en el parámetro interno de la correspondencia caótica. • Incluir la clave secreta en las condiciones iniciales.

Fig. 5.- Métodos para construir criptosistemas caóticos.

Estrategias de implementación. Criterios de las funciones caóticas en criptografía.

La aplicación de las funciones caóticas y de la teoría del caos a entornos criptográficos puede dividirse en dos grandes categorías o tipos de aplicaciones:

(1) Utilizar alguna función caótica como un RNG (Random Number Generador) o más bien PRNG (Pseudo RNG), bien para la generación de la clave aleatoria, o para utilizarla como fuente de números aleatorios para un criptosistema simétrico de flujo OTP (One Time Pad). En estas aplicaciones, la clave es el estado inicial del sistema. Un ejemplo de este tipo de aplicación RNG es un sistema que utiliza información de estado parcial de estados sucesivos como números aleatorios que se suman al texto en claro módulo el tamaño del alfabeto.

(2) Hacer corresponder el texto en claro al estado inicial del sistema caótico, y a continuación hacer pasar por un ciclo al sistema a través de algún número de iteraciones dando lugar el estado resultante al texto cifrado. En estas aplicaciones, la clave es:

(a) El algoritmo de correspondencia.

(b) Los detalles de la función que representan el sistema.

(c) El número de iteraciones.

(d) Cualquier combinación de las tres anteriores.

Un ejemplo de este tipo de aplicación de correspondencia es un sistema que segmenta números reales en un número de divisiones igual al tamaño del alfabeto, e itera estos valores, utilizando la función caótica durante muchos ciclos, para obtener el texto cifrado.

Los siguientes criterios corresponden a los de las funciones caóticas ideales y debe cumplir cualquier sistema caótico que pretenda utilizarse en criptografía:

1) Semillas o condiciones iniciales muy similares deben producir secuencias muy diferentes de valores. Para las aplicaciones de correspondencia, claves similares deberían cifrar el texto en claro dando lugar a texto cifrado muy diferente.

2) Cada secuencia debería ser aleatoria y sin ciclos para cualquier longitud de mensaje concebible. Las aplicaciones RNG deberían no tener ciclos y patrones para prevenir coincidencia y ataques de inferencia. Las aplicaciones de correspondencia deberían no tener patrones para ocultar cualquier similitud entre texto en claro y cifrado, y no tener ciclos, para asegurar que cada texto cifrado se descifra a un único texto en claro. La ausencia de ciclos es crítica, si un texto en claro se itera a cualquier valor que es un elemento de un ciclo, entonces puede ser indistinguible de otros elementos.

3) Para aplicaciones RNG el conocimiento de una sucesión de elementos de la secuencia no debería permitir predecir los elementos anteriores o posteriores. Para aplicaciones de correspondencias, la función no debería ser fácilmente reversible sin la clave.

4) Debería haber un número de valores de claves viable mayor que el número más grande concebible de sesiones de comunicaciones que tengan lugar durante el ciclo de vida de la función caótica.

5) La progresión del sistema de un estado al siguiente debería ser determinístico y reproducible.

El grado de cumplimiento de cada criterio anterior varía, por ello debe realizarse un análisis de cada implementación. Se deben tener en cuenta aspectos como:

(a) Las funciones caóticas son muy sensibles a las condiciones iniciales, con un pequeño cambio en las condiciones iniciales se produce cambios importantes en la secuencia de valores generada.

(b) Una función caótica, por definición, presenta un comportamiento no lineal que puede mejorarse. Es posible optimizar la no linealidad de una función dada y controlar la aleatoriedad.

(c) Si se revela toda la información sobre el estado del sistema todos los estados siguientes se podrán calcular. Es importante construir RNG/PRNG que sólo utilicen información de estado parcial como salida.

(d) Debe examinarse el sistema respecto al número de claves posibles y si existen claves débiles.

(e) Cuando se utilice matemática de coma flotante es crítico que todas las partes tengan igual precisión ya que cualquier redondeo inconsistente puede dar lugar a texto cifrado no reconocible.

Consideraciones finales.

Existe un gran futuro para la criptografía caótica encontrando aplicaciones en diversas áreas militar, industrial e incluso comercial, donde se puede utilizar para proteger datos y comunicaciones electrónicas. Una característica destacable es la posibilidad de cifrar en hardware en tiempo real a elevada velocidad (más de 50 Gbps). Permite implementaciones muy eficientes en computadores analógicos y sobre circuitos de propósito especial. Con DSPs (Procesadores Digitales de Señal) en el dominio digital también permite soluciones interesantes. Nuestro grupo de investigación lleva trabajando en esta área de los criptosistemas caóticos más de doce años con resultados tanto en la síntesis de criptosistemas analógicos y digitales como en el criptoanálisis para la valoración de niveles de seguridad para cifradores comerciales en el dominio de imágenes, video y audio con implementaciones en los dominios continuo y discreto.

Este artículo se enmarca en las actividades desarrolladas dentro del proyecto LEFIS-APTICE (financiado por Socrates 2005. European Commission).

Bibliografia.

-Areitio, J. y Areitio, G. “Desarrollo y Análisis de Criptosistemas Asimétricos estilo Paillier”. REE Nº 602. Enero 2005.
-Areitio, J. y Areitio, G. “Identificación y análisis en torno a la PKI y su relación con los Certificados Digitales y la Firma Electrónica Avanzada”. REE. Nº 596/597.
-Areitio, J. “Análisis de Esquemas para el Intercambio de Secretos”. REE. Nº 601.
-Areitio, J. “Síntesis de Mecanismos Criptográficos de Clave Pública no Convencionales”. REE Nº 599.
-Bossert, M. “Channel Coding for Telecommunications”. John Wiley and Sons, Ltd. Chichester. UK. 1999.
-Gutmann, P. “Design and Verification of a Cryptographic Security Architecture”. Springer Verlag. 2003.
-Mao, W. “Modern Cryptography: Theory and Practice“. Prentice-Hall. PTR. 2003.
-Oppliger, R. “Contemporary Cryptography”. Artech House Publishers. 2005.
-Schneier, B. “Applied Cryptography, Practical Algorithms and Source Codes in C”. John Wiley and Sons. NY. 1996.
-Konheim, A.G. “Computer Security and Cryptography”. J. Wiley & Sons. 2006.