Resumen "Cryptography with Chaos".

Marcos Daniel Calderón Calderón
Maestría en Ciencias de la Computación
Centro de Investigación en Matemáticas (CIMAT)
Guanajuato , Gto.
marcos.calderon@cimat.mx

***Resumen*—Es posible cifrar un mensage (un texto compuesto por algún alfabeto) usando la propiedad ergódica de la ecuación logística. La idea básica es cifrar cada carácter del mensage como el número entero de iteraciones realizadas en la ecuación logística, con el fin de transferir la trayectoria desde una condición inicial hacia un E-intervalo dentro del atractor caótico logístico.**

Las oscilaciones deterministas ocurridas en fenómenos caóticos tienen un comportamiento estocástico e impredecible.

Actualmente, el comportamiento estocástico que presentan los osciladores caóticos que se caracteriza por un gran amplio espectro de frecuencia, se ha utilizado para ocultar informaciónmación, con el fin de transmitir de manera segura mensajes secretos.

Una primera aplicación para la transmisión de señales con el uso de caos fué propuesto por Pecora y Carroll. Ellos mostraron que dos circuitos caóticos similares pueden sincronizar sus trayectorias. Entonces, el mensaje a ser enviado está enmascarado en una de las señales caóticas. Durante la transmisión, el mensaje es extraído cuando el receptor utiliz un circuíto síncrono.

Otra idea para la transmisión de mensajes con el uso de caos surge del hecho de que el caos puede ser controlado mediante el uso de pequeñas perturbaciones. El emisor envía una señal controlada que codifica el mensaje binario. Dependiendo sobre cuáles dos medios planos en una sección de Poincaré la trayectoria cruza, el receptor considera qe un dígito binario 0 ó 1 está siendo transmitido. El emisor envía un pequeño parámetro de perturbación que el receptor debe aplicar en el sistema caótico, con el fin de orientar la trayectoria en alguna región en el espacio de fase. El mensaje es recuperado asumiento que esta reción es asociada con algún alfabeto unitario. También usando técnicas de orientación, el emisor envía una retroalimentación de corrección de la órbita que el receptor debe aplicar a la trayectoria del sistema caótico, con el fin de hacer este alcance en la trayectoria, alguna $\epsilon-$vecindad de un punto en un intervalo prestablecido de tiempo. La información es entonces recuperada por el receptor, asumiento que elgún símbolo unitario del alfabeto es asiciado con el tiempo de llegada y el alcande de la $\epsilon-$vecindad.

En este trabajo, el mensaje a transmitir es un texto compuesto por algún alfabeto. También se asocia un $\epsilon-$invervalo del atractor con el símbolo del alfabeto. Sin embargo, del mensaje cifrado que es transmitido se obtiene un texto original, sin el uso de sistemas caóticos sincronizados o por técnicas de control y destino, pero, ahora se aprovecha una propidad de cualquier sistema caótico: ergodicidad.

Se utiliza el mapa logístico:

$$X_{n+1} = bX_n(1 - X_n), \tag{1}$$

donde $X_n \in [0, 1]$, se tiene unas comportamiento caótico, se puede cifrar de una manera rápida y segura.

Se propone que el cifrado de algún carácter es el número de iteraciones aplicadas en la ecuación anterior y que forman una trayectoria que comienza en una condición inicial X_0 y donde se tine un $\epsilon-$invervalo con el carácter.

En este caso, el alfabeto está compuesto de S elementos con sus respectivos $\epsilon-$invervalos. Cada intervalo, está en el rango $[X_{min} + (S-1)\epsilon, X_{min} + S\epsilon)$, donde, $S = 256$, $\epsilon = (X_{max} - X_{min})/S$ y $[X_{min}, X_{max}]$ es una porción del atractor, o puede ser el atractor mismo.

El número de iteraciones **(el texto cifrado)** es usado junto con las llaves secretas: las S asociaciones entre los S $\epsilon-$intervalos y las S unidades de algún alfabeto, la primera condición inicial X_0, y el parámetro de control b, así, se trabaja con $S + 2$, llaves secretas, permitiendo al receptor descifrar el texto cifrado al iterar la ecuación logística las veces indicadas por el texto cifrado. La posición del punto final con respecto a los S $\epsilon-$intervalos, apunta al carácter original que envió el receptor.

En el parrafo anterior, se hace referencia a X_0 como la primer condición inicial, porque siempre que se cifre una unidad de un texto plano (por ejemplo, la palabra "hi" es un texto plano con dos unidades), una nueva condición inicial es considerada. Si $C1$ es el texto cifrado de la primera unidad en un texto plano, para cifrar la segunda unidad en este texto plano se usa como condición ini izl $X_0^{'} = F^{C1}X_0$, donde F^{C1} es la $C1$ iteración de la ecuación del mapa logístico. Si $C2$ es el texto cifrado de la segunda unidad del texto plano, la condición inicial utilizada para cifrar la tercera unidad en el mismo texto plano es $X_0^{''} = f^{C2}(x_0^{'})$. Esta regla es fácil de aplicar al resto de las unidades que falten en el texto plano.

La condición inicial es cambiada ara permitir que diferentes unidades en el texto plano tengan la misma unidad del texto cifrado. Debido a este truco, el método criptográfica no es de la clase de transformaciónes uno a uno, algo que es muy común en métodos usuales de criptografía.

Se debe de notar qu $X_0^{''}$ también es dado por $F^{C1+C2}(X_0)$. Sin embargo, es preferible no utilizar esta notación, ya que se quiere enfatizar que, independientemente de la condición inicial, la unidad de texto cifrado C_n es un número que no excede el valor 65 532. Además de esta condición, las unidades del texto cifrado también dependen de dos parámetros, un

tiempo transistorio N_0 y un coeficiente η que serán definidos después.

De acuerdo al tamaño de las trayectorias utilizadas en este trabajo, tenemos que revisar algunos puntos sobre ergodicidad. Debido a la ergodicidad, un número infinito de trayectorias (que comienzan en cualquier X_0) con tamaños diferentes llegan al mismo $epsilon$-intervalo. Como resultado, una simple unidad en un texto plano podría ser cifrado en un número infinito de maneras. De cualquier manera, trabajar con un número muy grande de posibilidades es impráctico y de hecho, no es necesario.

La razón por la cual podemos considerar una trayectoria de un tamaño pequeño cuyo tamaño representa una unidad del texto plano cifrado, depende de la existencia de una densidad invariante natural de los atractores caóticos. Esta densidad invarianta, es la distribución del espacio de las trayectorias de tamaño infinito, puede ser bien descritas por una trayectoria de tamaño finito. En suma, debido a la ergodicidad, casi cualquier condición inicial, después de que es iterada, genera un atractor con la misma densidad natural invariante. Como un sistema caótico es ergódico, casi cualquier condición inicial, cuando es iterada por algún sistema, se llega a un ϵ-invervalo muchas veces, a condición de que este intervalo pertenece al atractor. Y la frecuencia con que cada porción del atractor es visitado depende de su densidad.

Para calcular la densidad natural invariante, pero no en su forma analítica, uno debe considerar una trayectoria de N iteraciones, comenzando desde algún punto X_0, y revisar su distribución en mu8chos ϵ-intervalos que dividen al atractor. Nosotros elegimos trabajar con trayectorias que no exceden las 65532 iteraciones, tal que el número C_n, una unidad del texto cifrado, es rápidamente calculada y envidad por el receptor para usar únicamente una transmisión de un entero de un byte.

I. Referencias.