4 Formulación matemática del criptosistema caótico de señales

En este capítulo se reportan las ecuaciones del criptosistema caótico que se diseñó, así como el desarrollo que se llevó a cabo para obtenerlas. El diseño de dichas ecuaciones toma en cuenta varias consideraciones para que el criptosistema sea fácil de implementar en un circuito analógico que sea robusto y fácilmente reconfigurable.

En la sección 4.1 se presenta de forma general la dinámica del criptosistema caótico y las condiciones que debe de cumplir para lograr sincronización entre el encriptor y el desencriptor. En la sección 4.2 se diseña el sistema caótico que es la base del criptosistema a partir de ciertos requerimientos de estructura y de funcionamiento. El diseño de la función de encripción y de desencripción se hace en la sección 4.3. Por último, en la sección 4.4 se juntan los resultados de las secciones previas y se desarrollan las ecuaciones del criptosistema caótico de señales.

4.1 Metodología de diseño de un criptosistema caótico

El esquema básico del criptosistema caótico a diseñar se muestra en la Figura 4-1.

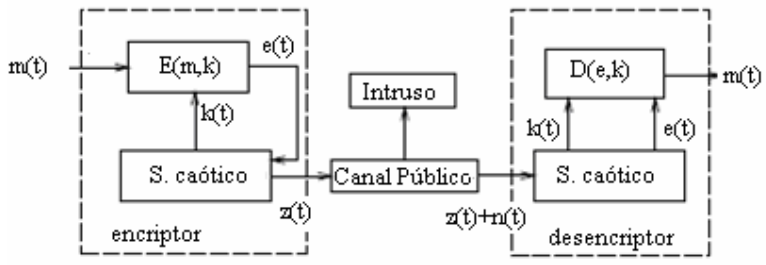

Figura 4-1 Esquema básico de un criptosistema caótico

Como se explicó en la sección 2.2.3, el funcionamiento de los criptosistemas caóticos, o sistemas de encripción caótica de tercera generación, se basa en la sincronización del desencriptor con el encriptor.

En [14] se presenta una metodología para diseñar un criptosistema a partir de un sistema caótico $\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{b}f(\mathbf{x})$, con $\mathbf{A} \in \mathbb{R}^{n\times n}$, $\mathbf{b} \in \mathbb{R}^{n}$ y una función no lineal $f : \mathbb{R}^{n} \mapsto \mathbb{R}$. El encriptor es un sistema caótico descrito por la ecuación:

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{b}f(\mathbf{x}) + \mathbf{b}e(t), \tag{4.1}$$

donde $\mathbf{x} \in \mathbb{R}^{n}$ es el vector de variables del encriptor. La señal $e(t)$ es la señal encriptada que resulta del proceso de encripción:

$$e(t) = E(m(t), \mathbf{L}\mathbf{x}), \tag{4.2}$$

donde $m(t)$ es la señal de información, $\mathbf{L} \in \mathbb{R}^{1\times n}$, la combinación lineal $\mathbf{L}\mathbf{x}$ es la llave de encripción, y E es la regla de encripción. La regla de encripción tiene como finalidad transformar la señal de información $m(t)$ en la señal encriptada $e(t)$, de forma que esta última no se parezca ni en magnitud ni en frecuencia a la señal de información. Por último, la señal que se transmite del sistema encriptor al desencriptor es:

$$z(t) = -e(t) - (f(\mathbf{x}) + \mathbf{k}\mathbf{x}), \tag{4.3}$$

donde $\mathbf{k} \in \mathbb{R}^{1\times n}$. La ecuación (4.3) muestra que la señal que se transmite está formada por dos partes: la señal encriptada $e(t)$ y la señal de sincronización $-(f(\mathbf{x}) + \mathbf{k}\mathbf{x})$, esta última es la que se encarga de lograr que el desencriptor se comporte igual al encriptor.

Por su parte, el desencriptor se modela como:

$$\mathbf{y} = \mathbf{A}\mathbf{y} + \mathbf{b}f(\mathbf{y}) + \mathbf{b}\tilde{e}(t), \tag{4.4}$$

donde $\mathbf{y} \in \mathbb{R}^{n}$ es el vector de variables del desencriptor. La señal $\tilde{e}(t)$ es la estimación de la señal encriptada y está dada por:

$$\tilde{e}(t) = -z(t) - (f(\mathbf{y}) + \mathbf{k}\mathbf{y}), \tag{4.5}$$

o equivalentemente:

$$\tilde{e}(t) = e(t) + \left(f(\mathbf{x}) - f(\mathbf{y}) \right) + \mathbf{k}(\mathbf{x} - \mathbf{y}), \tag{4.6}$$

En la ecuación (4.6) se puede ver que si $\mathbf{y} \to \mathbf{x}$, entonces $\tilde{e}(t) \to e(t)$.

La señal de información $\tilde{m}(t)$ se puede estimar pasando la estimación de la señal encriptada $\tilde{e}(t)$ por la regla de desencripción D, es decir:

$$\tilde{m}(t) = D\left(\tilde{e}(t), \mathbf{L}\mathbf{y}\right), \tag{4.7}$$

donde la combinación lineal $\mathbf{L}\mathbf{y}$ es la estimación de la llave de encripción y D cumple $\phi = D\left(E(\phi, \psi), \psi\right)$ para $\phi, \psi \in \square$.

Se puede afirmar que $\tilde{m}(t) \to m(t)$ conforme $\mathbf{y} \to \mathbf{x}$ y $\tilde{e}(t) \to e(t)$; por lo tanto, para que se pueda recobra la señal de información debe minimizarse el error de sincronización $\mathbf{e}$, el cual se define como la diferencia entre el estado del desencriptor y el encriptor; su dinámica se rige por:

$$\dot{\mathbf{e}} = \dot{\mathbf{y}} - \dot{\mathbf{x}}. \tag{4.8}$$

A partir de (4.1), (4.4) y (4.8) se tiene que:

$$\dot{\mathbf{e}} = \left(\mathbf{A}\mathbf{y} + \mathbf{b}f(\mathbf{y}) + \mathbf{b}\tilde{e}(t)\right) - \left(\mathbf{A}\mathbf{x} + \mathbf{b}f(\mathbf{x}) + \mathbf{b}e(t)\right). \tag{4.9}$$

Desarrollando (4.9) se obtiene:

$$\dot{\mathbf{e}} = \mathbf{A}(\mathbf{y} - \mathbf{x}) + \mathbf{b}\left(f(\mathbf{y}) + \tilde{e}(t) - f(\mathbf{x}) - e(t) \right). \tag{4.10}$$

Sustituyendo (4.6) en (4.10) se llega a la expresión:

$$\dot{\mathbf{e}} = \mathbf{A}(\mathbf{y} - \mathbf{x}) + \mathbf{b}\left(f(\mathbf{y}) + e(t) + \left(f(\mathbf{x}) - f(\mathbf{y}) \right) + \mathbf{k}(\mathbf{x} - \mathbf{y}) - f(\mathbf{x}) - e(t) \right). \tag{4.11}$$

Si se simplifica la ecuación (4.11) y se sustituye $\mathbf{e} = \mathbf{y} - \mathbf{x}$ en ella se obtiene que:

$$\dot{\mathbf{e}} = \mathbf{A}\mathbf{e} + \mathbf{b}(-\mathbf{k}\mathbf{e}). \tag{4.12}$$

En la ecuación (4.12), se puede ver que el sistema de error de sincronización se comporta como un sistema lineal donde $-\mathbf{k}\mathbf{e}$ hace el papel de retroalimentación.

La ecuación (4.12) se puede expresar equivalentemente como:

$$\dot{\mathbf{e}} = (\mathbf{A} - \mathbf{bk})\mathbf{e}. \qquad (4.13)$$

Si los eigenvalores de la matriz $(\mathbf{A} - \mathbf{bk})$ se encuentran en el plano izquierdo abierto del plano complejo, el error de sincronización tiende a cero de forma exponencial, el desencriptor se vuelve un observador global del encriptor [14] y por lo tanto se puede recobrar la señal de información; es decir:

$$\mathrm{Re}\{eigs(\mathbf{A} - \mathbf{bk})\} < 0 \quad \Rightarrow \quad \mathbf{e} \to \mathbf{0} \quad \Rightarrow \quad \mathbf{y} \to \mathbf{x} \quad \Rightarrow \quad \tilde{m}(t) \to m(t). \qquad (4.14)$$

4.2 Formulación del sistema caótico

En esta sección se plantean las ecuaciones de variables de estado del sistema caótico que se va a utilizar en el criptosistema caótico. Existen diversos sistemas caóticos que podrían usarse para implementar este criptosistema; cada uno de ellos tiene diferente número de parámetros (variables de estado), diferente tipo y número de no linealidades, y diferente número de términos.

Se desea que el sistema caótico $\dot{\mathbf{x}} = \mathbf{Ax} + \mathbf{b}f(\mathbf{x})$ que se planteé cumpla con los siguientes requerimientos estructurales a modo de hacer sencilla y robusta la realización del sistema en circuito:

- Las ecuaciones del sistema podrán ser implementadas con un circuito de variables de estado que use integradores, sumadores y restadores analógicos. De cumplir con este requerimiento los estados del sistema son voltajes y se evita el uso de inductores los cuales tienen resistencias y capacitancias parásitas que pueden afectar el comportamiento del sistema como se reporta en [15].

- La matriz **A** será de preferencia una matriz de tipo companion, y el vector $\mathbf{b} = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}^T$ a modo de reducir el número de sumadores y restadores analógicos. El requerimiento anterior se debe a que los integradores quedan en cascada y todas las sumas y restas de los estados del sistema se hacen sólo a la entrada del primer integrador (en vez de realizar sumas y restas entre integrador e integrador).

- La no linealidad de preferencia debe ser una función lineal por partes que puede hacerse con amplificadores operacionales; con esto se evita el uso de multiplicadores y bloques no lineales más complejos. De preferencia la función lineal por partes será continua, para evitar los efectos de histéresis que se reportan en [15].

El sistema de tirón que se estudió en la sección 3.3.2.1, cumple con los requisitos; en dicha sección se encontró la expresión para escalar el sistema de tirón en magnitud y frecuencia:

$$\begin{bmatrix} \dot{u} \\ \dot{v} \\ \dot{w} \end{bmatrix} = \begin{bmatrix} 0 & \tau_1 \dfrac{\eta_1}{\eta_2} & 0 \\ 0 & 0 & \tau_2 \dfrac{\eta_2}{\eta_3} \\ 0 & -\tau_3 \dfrac{\eta_3}{\eta_2}\gamma & -\tau_3 \beta \end{bmatrix} \begin{bmatrix} u \\ v \\ w \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ \tau_3 \end{bmatrix} \left(\frac{\eta_3 \delta}{2\eta_1 \alpha} \left(\left| u + \eta_1 \alpha \right| - \left| u - \eta_1 \alpha \right| \right) - \frac{\eta_3}{\eta_1} \mu u \right), \quad (4.15)$$

presenta un comportamiento caótico con $\gamma = 1$, $\beta = 0.6$, $\delta = 1$, $\mu = 1$, $\alpha \in [0, 0.3]$, $\eta_1, \eta_2, \eta_3 \in \mathbb{R} \setminus \{0\}$ y $\tau_1, \tau_2, \tau_3 \in \mathbb{R}^+$.

Además de los requerimientos estructurales, el sistema caótico también debe de cumplir los siguientes requisitos de amplitud y frecuencia:

- El espectro en frecuencia de las variables de estado del sistema caótico debe ser fácilmente variable y mayor al de la señales a encriptar.

- La magnitud de las variables de estado deberá variar dentro de un rango menor a $[-3,3]$ unidades, para que al diseñar el circuito con amplificadores operacionales, éstos ocupen una buena parte de su rango de voltaje sin saturarse.

Para que el sistema (4.15) cumpla con las características de magnitud y frecuencia que requiere el criptosistema caótico se escoge $\tau_1 = \tau_2 = \tau_3 = 5\times10^4$, $\eta_1 = \eta_3 = 1.35$, y $\eta_2 = -1.35$. El sistema que queda como resultado de tal escalamiento es:

$$\frac{1}{\tau}\begin{bmatrix}\dot{x}_1\\ \dot{x}_2\\ \dot{x}_3\end{bmatrix} = \begin{bmatrix}0 & -1 & 0\\ 0 & 0 & -1\\ 0 & \gamma & -\beta\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix} + \begin{bmatrix}0\\ 0\\ 1\end{bmatrix}\left(\frac{\delta}{2\alpha}\left(|x_1+\alpha|-|x_1-\alpha|\right)-\mu x_1\right), \qquad (4.16)$$

donde $\gamma = 1$, $\beta = 0.6$, $\delta = 1.35$, $\mu = 1$, $\alpha = 0.3375$ y $\tau = 5\times10^4$.

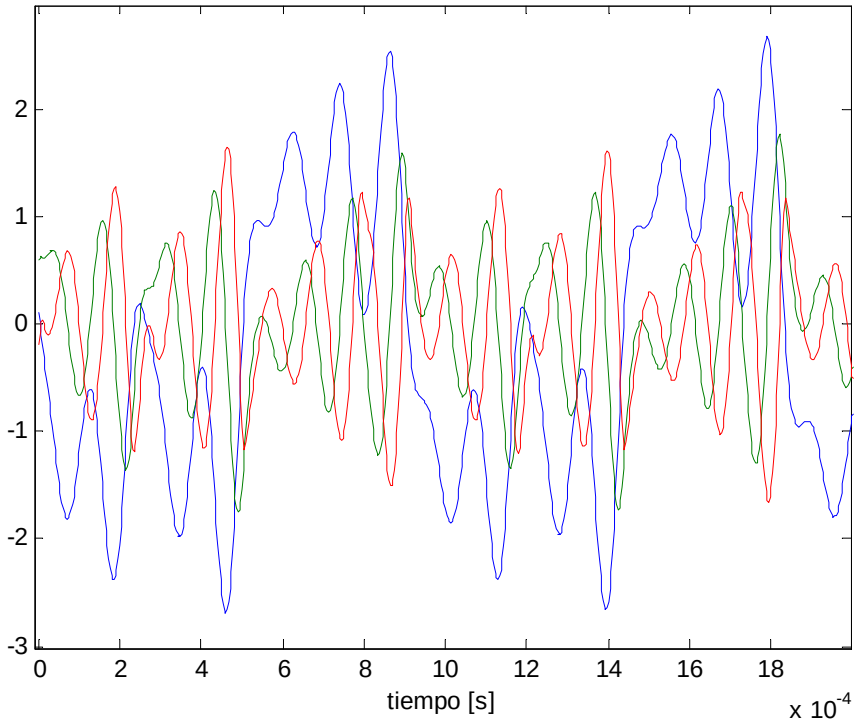

Figura 4-2 Series de tiempo de las variables del sistema: x1(azul), x2 (rojo), x3 (verde).

La Figura 4-2 muestra el comportamiento en el tiempo y la Figura 3-4 presenta el comportamiento en frecuencia de cada una de las variables de estado del sistema (4.16); se

puede ver que los rangos de amplitud son aceptables para trabajar con amplificadores operacionales y el rango de frecuencias cubre las frecuencias menores a 10kHz. Por lo tanto el sistema (4.16) cumple con los requerimientos de amplitud y frecuencia del criptosistema caótico.

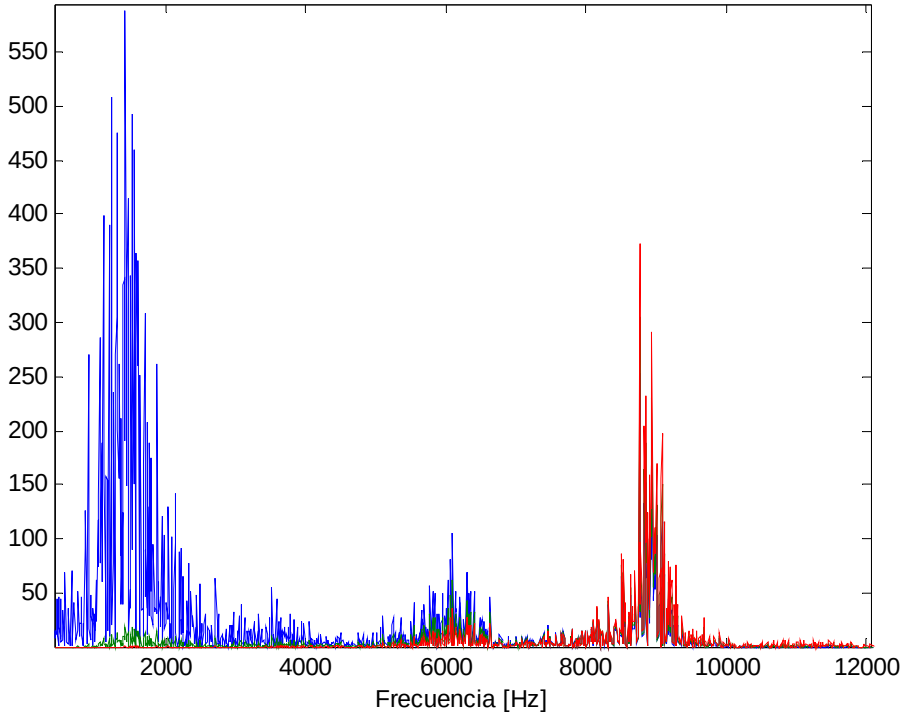

Figura 4-3 Espectro en frecuencia de las variables del sistema: x1(azul), x2 (rojo), x3 (verde).

4.3 Las funciones de encripción y desencripción

Como se vio en la sección 4.1, en [14] se menciona el uso de una función E la cual encripta la señal de información con una llave caótica, sin embargo, en dicho artículo no se comenta nada acerca de las características que la función de encripción debe de tener y los criterios que debe de cumplir.

No todas las funciones de encripción funcionan con cualquier sistema caótico ya que éstas realimentan al sistema caótico algunas de las variables de estado del sistema, y por lo tanto pueden sacar del régimen caótico al sistema. Además, no está claro que características

debe de cumplir la función de encripción para dar un buen nivel de seguridad en un criptosistema caótico.

Para superar estos problemas, en la sección 4.3.1 de esta tesis se plantean una serie de recomendaciones a tomar en cuenta en la formulación de la función de encripción E derivadas a partir de conceptos de Teoría de Información. Siguiendo dichas recomendaciones, en la sección 4.3.2 se desarrollarán las expresiones matemáticas de una función de encripción y una función de desencripción con las cuales se encontró un buen funcionamiento al aplicarlas a un sistema caótico de tirón.

4.3.1 Generalidades de la función de encripción

La función de encripción E tiene como meta transformar la señal de información a una señal encriptada. En la sección 2.1 se definió el criptosistema seguro de Shannon. Dicho concepto puede ser aplicado también en el esquema de criptosistema caótico, sólo que en este caso las variables son continuas; por lo tanto un criptosistema caótico seguro de Shannon como aquel que cumple que la información mutua del mensaje y el criptograma es nula, es decir:

$$I(C,M)=0. \tag{4.17}$$

La ecuación (4.17) puede expresarse en términos de entropías diferenciales como:

$$h(M)-h(M\mid C)=0, \tag{4.18}$$

lo que significa que el criptosistema será seguro si el mensaje y el criptograma son estadísticamente independientes o poco dependientes [2].

La señal encriptada (criptograma) se obtiene al pasar por la función de encripción a la señal sin encriptar (mensaje), otra forma de interpretarlo es decir que la señal encriptada es una transformación del proceso aleatorio que representa la señal de información. Por lo

tanto, para hacer que la señal de información y la señal encriptada sean poco dependientes estadísticamente se debe de tener una función de encripción que afecte la distribución de la señal de información y su autocorrelación; es decir que afecte a la señal de información en magnitud y en frecuencia. Consecuentemente la función de encripción debe ser no lineal, para que así la señal encriptada sea diferente en forma en tiempo y en frecuencia en relación a la señal de información. Si la función de encripción fuera lineal, el esquema de encripción sería equivalente a un esquema de modulación caótica de segunda generación, y si la señal de información fuera lo suficientemente grande podría ser fácil localizarla en el dominio de la frecuencia ya que sólo se tendría una sobreposición del espectro de ella y del de la llave caótica.

Por otro lado, para evitar la posibilidad de que la función de encripción saque del régimen caótico al criptosistema se puede analizar la dinámica del sistema caótico junto con la función de encripción: encontrar atractores, checar condiciones de estabilidad, etc. Éste tipo de análisis si bien es correcto y recomendable, puede resultar complejo. La recomendación que se hace en este trabajo sobre la función de encripción consiste en hacer que en promedio la señal encriptada no contenga variables de estado del sistema y por lo tanto, en promedio no afecte a la dinámica del sistema más que como perturbaciones aleatorias. Para lograr lo anterior se requiere que la señal de información $m(t)$ sea un proceso aleatorio con valor esperado igual a cero y siga una distribución aleatoria par, la llave $k(t)$ sea caótica y que se tenga una función $g:\square \mapsto \square$ no lineal, biyectiva e impar; si la función de encripción es de la forma:

$$e(t) = E\left(m(t), k(t)\right) = g\left(m(t) + k(t)\right) - g\left(k(t)\right), \qquad (4.19)$$

entonces el valor esperado de la señal encriptada $e(t)$ en un instante de tiempo t_0 cualquiera será:

$$\bar{\varepsilon}\left(t_0\right)=\int_{-\infty}^{\infty} g\left(m\left(t_0\right)+k\left(t_0\right)\right)d\phi-g\left(k\left(t_0\right)\right). \qquad (4.20)$$

Se dijo que la función g es biyectiva e impar, por lo tanto la transformación que le hace a la señal de información no cambia el valor esperado de ésta, por lo tanto la expresión (4.20) se reduce a:

$$\bar{\varepsilon}\left(t_0\right)=g\left(\int_{-\infty}^{\infty} m\left(t_0\right)+k\left(t_0\right)d\phi\right)-g\left(k\left(t_0\right)\right)=g\left(k\left(t_0\right)\right)-g\left(k\left(t_0\right)\right)=0, \qquad (4.21)$$

lo que significa que en promedio la función de encripción planteada en la ecuación (4.19) no altera la dinámica (atractores, estabilidad, etc.) del sistema caótico sobre el cual se aplique.

Por último, la función de desencripción correspondiente a la función de encripción de la ecuación (4.19) es:

$$m\left(t\right)=D\left(e\left(t\right),k\left(t\right)\right)=g^{-1}\left(e\left(t\right)+g\left(k\left(t\right)\right)\right)-k\left(t\right), \qquad (4.22)$$

donde la función g^{-1} es la función inversa de la función g, y como consecuencia es biyectiva, no lineal e impar.

4.3.2 Formulación de las funciones de encripción y desencripción.

Siguiendo los principios presentados en el apartado anterior se diseñó una función de encripción. Para empezar se seleccionó la llave caótica de la función de encripción $k\left(t\right)$; de las tres variables de estado del sistema la que abarca mayor amplitud y un mayor rango de frecuencias es x_1; por simplicidad ésta se usará como llave caótica en el encriptor (y_1 en el desencriptor).

La función no lineal, biyectiva e impar que se escogió como g es:

$$g(x) = -\rho x + \frac{\rho - 1}{2}\left(|x+\eta| - |x-\eta|\right) = \begin{cases} -\rho x + \eta(1-\rho) & x < -\eta \\ -x & |x| < \eta \\ -\rho x - \eta(1-\rho) & x > \eta \end{cases}, \qquad (4.23)$$

donde $0 < \rho < 1$, y $\eta > 0$, y su gráfica se muestra en la Figura 4-4.

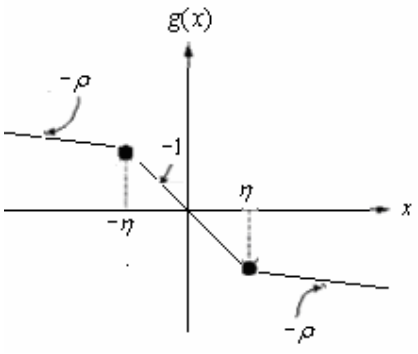

Figura 4-4 Función g(x)

La función inversa de (4.23) queda definida como:

$$g^{-1}(x) = -\rho^{-1}x + \frac{\rho^{-1} - 1}{2}\left(|x+\eta| - |x-\eta|\right) = \begin{cases} -\rho^{-1}x + \eta(1-\rho^{-1}) & x < -\eta \\ -x & |x| < \eta \\ -\rho^{-1} - \eta(1-\rho^{-1}) & x > \eta \end{cases}. \qquad (4.24)$$

La muestra la gráfica de la función inversa $g^{-1}(x)$.

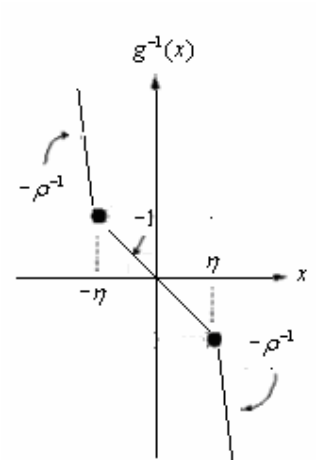

Figura 4-5 Función $g^{-1}(x)$

Se concluye que las funciones de encripción y de desencripción a usar en el criptosistema caótico son:

$$\begin{cases} E\left(m(t),x_1\right)=g\left(m(t)+x_1\right)-g\left(x_1\right) \\ g\left(m(t)+x_1\right)=-\rho\left(m(t)+x_1\right)+\dfrac{\rho-1}{2}\left(\left|m(t)+x_1+\eta\right|-\left|m(t)+x_1-\eta\right|\right), \\ g\left(x_1\right)=-\rho x_1+\dfrac{\rho-1}{2}\left(\left|x_1+\eta\right|-\left|x_1-\eta\right|\right) \end{cases} \quad (4.25)$$

$$\begin{cases} D\left(e(t),y_1\right)=g^{-1}\left(e(t)+g\left(y_1\right)\right)-y_1 \\ g^{-1}\left(e(t)+g\left(y_1\right)\right)=-\rho^{-1}\left(e(t)+g\left(y_1\right)\right) \\ \qquad\qquad +\dfrac{\rho^{-1}-1}{2}\left(\left|e(t)+g\left(y_1\right)+\eta\right|-\left|e(t)+g\left(y_1\right)-\eta\right|\right), \\ g\left(y_1\right)=-\rho\left(y_1\right)+\dfrac{\rho-1}{2}\left(\left|y_1+\eta\right|-\left|y_1-\eta\right|\right) \end{cases} \quad (4.26)$$

y los valores de los parámetros que se escogen son $\rho=1/10$, y $\eta=0.7$.

4.4 El criptosistema caótico

En esta sección se juntan los resultados obtenidos en las secciones previas para formular las ecuaciones dinámicas del criptosistema caótico. El criptosistema caótico se hará usando el sistema caótico (4.16) que se formuló en la sección 4.2. Este sistema se puede expresar equivalentemente como:

$$\dot{\mathbf{x}}=\mathbf{A}\mathbf{x}+\mathbf{b}f\left(\mathbf{x}\right), \quad (4.27)$$

donde $\mathbf{x}=\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$, $\mathbf{A}=\begin{bmatrix} 0 & -\tau & 0 \\ 0 & 0 & -\tau \\ 0 & \tau\gamma & -\tau\beta \end{bmatrix}$, $\mathbf{b}=\begin{bmatrix} 0 \\ 0 \\ \tau \end{bmatrix}$, $f\left(\mathbf{x}\right)=\dfrac{\delta}{2\alpha}\left(\left|x_1+\alpha\right|-\left|x_1-\alpha\right|\right)-\mu x_1$,

$\tau=5\times10^4$, $\gamma=1$, $\beta=0.6$, $\delta=1.35$, $\mu=1$ y $\alpha=0.3375$.

En la sección 4.1 se concluyó que para lograr la sincronización en el criptosistema hay que escoger valores de $\mathbf{k}$ tales que los eigenvalores de la matriz $\mathbf{A}-\mathbf{bk}$ se encuentren en el semiplano izquierdo del plano complejo.

Si los tres eigenvalores de $\mathbf{A}-\mathbf{bk}$ se colocan en $\lambda=-\tau$, el polinomio característico debe ser de la forma:

$$\left(\lambda+\tau\right)^3=\lambda^3+3\tau\lambda^2+3\tau^2\lambda+\tau^3=0. \tag{4.28}$$

El polinomio característico de la matriz:

$$\mathbf{A}-\mathbf{bk}=-\tau\begin{bmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ k_1 & -\gamma+k_2 & \beta+k_3\end{bmatrix}, \tag{4.29}$$

es:

$$\lambda^3+\left(\beta+k_3\right)\tau\lambda^2+\left(\gamma-k_2\right)\tau^2\lambda+k_1\tau^3=0, \tag{4.30}$$

con $\tau=5\times10^4$, $\gamma=1$, $\beta=0.6$. Si se iguala (4.30) con (4.28), se tiene que:

$$\begin{array}{lcl} k_1=1 & & k_1=1\\ k_2=\gamma-3 & \Rightarrow & k_2=-2\\ k_3=3-\beta & & k_3=2.4\end{array}. \tag{4.31}$$

Por otro lado, en la sección 4.3.2 se desarrollaron las funciones de encripción y de desencripción.

A partir de los resultados obtenidos, se concluye que el encriptor del criptosistema caótico está descrito por las ecuaciones:

$$\frac{1}{\tau}\begin{bmatrix}\dot{x}_1\\ \dot{x}_2\\ \dot{x}_3\end{bmatrix}=\begin{bmatrix}0 & -1 & 0\\ 0 & 0 & -1\\ 0 & \gamma & -\beta\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix}+\begin{bmatrix}0\\ 0\\ 1\end{bmatrix}\left(f\left(x_1\right)+e(t)\right), \tag{4.32}$$

$$f\left(x_1\right)=\begin{cases}-\mu x_1-\delta & x_1<-\alpha\\ \left(\dfrac{\delta}{\alpha}-\mu\right)x_1 & -\alpha\le x_1\le\alpha\\ -\mu x_1+\delta & x_1>\alpha\end{cases}, \tag{4.33}$$

$$\begin{cases} e(t) = g\left(m(t)+x_1\right) - g\left(x_1\right) \\ g\left(m(t)+x_1\right) = -\rho\left(m(t)+x_1\right) + \dfrac{\rho-1}{2}\left(\left|m(t)+x_1+\eta\right| - \left|m(t)+x_1-\eta\right|\right), \\ g\left(x_1\right) = -\rho x_1 + \dfrac{\rho-1}{2}\left(\left|x_1+\eta\right| - \left|x_1-\eta\right|\right) \end{cases} \quad (4.34)$$

$$z(t) = -e(t) - f\left(x_1\right) - k_1 x_1 - k_2 x_2 - k_3 x_3, \quad (4.35)$$

donde $\tau = 5\times10^4, \gamma = 1,\ \beta = 0.6,\ \delta = 1.35,\ \mu = 1,\ \alpha = 0.3375,\ k_1 = 1,\ k_2 = -2,\ k_3 = 2.4,$ $\rho = 1/10$ y $\eta = 0.7$.

Por su parte, la dinámica del sistema desencriptor está descrita por las ecuaciones:

$$\frac{1}{\tau}\begin{bmatrix} \dot{y}_1 \\ \dot{y}_2 \\ \dot{y}_3 \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 0 & \gamma & -\beta \end{bmatrix}\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}\left(f\left(y_1\right) + \tilde{e}(t)\right), \quad (4.36)$$

$$f\left(y_1\right) = \begin{cases} -\mu y_1 - \delta & y_1 < -\alpha \\ \left(\dfrac{\delta}{\alpha} - \mu\right) y_1 & -\alpha \le y_1 \le \alpha, \\ -\mu y_1 + \delta & y_1 > \alpha \end{cases} \quad (4.37)$$

$$\tilde{e}(t) = -z(t) - f\left(y_1\right) - k_1 y_1 - k_2 y_2 - k_3 y_3, \quad (4.38)$$

$$\begin{cases} \tilde{m}(t) = g^{-1}\left(\tilde{e}(t) + g\left(y_1\right)\right) - y_1 \\ g^{-1}\left(\tilde{e}(t) + g\left(y_1\right)\right) = -\rho^{-1}\left(\tilde{e}(t) + g\left(y_1\right)\right) \\ \qquad\qquad + \dfrac{\rho^{-1}-1}{2}\left(\left|\tilde{e}(t) + g\left(y_1\right) + \eta\right| - \left|\tilde{e}(t) + g\left(y_1\right) - \eta\right|\right), \\ g\left(y_1\right) = -\rho\left(y_1\right) + \dfrac{\rho-1}{2}\left(\left|y_1+\eta\right| - \left|y_1-\eta\right|\right) \end{cases} \quad (4.39)$$

donde $\tau = 5\times10^4,\ \gamma = 1,\ \beta = 0.6,\ \delta = 1.35,\ \mu = 1,\ \alpha = 0.3375,\ k_1 = 1,\ k_2 = -2,$ $k_3 = 2.4$ $\rho = 1/10$ y $\eta = 0.7$.