5 Diseño del criptocircuito caótico

En este capítulo se reporta el diseño de un criptocircuito caótico en base al criptosistema caótico que se formuló en el capítulo 4. El diseño del circuito se basa en amplificadores operacionales y los circuitos que con ellos se pueden construir: sumadores, restadores, integradores, funciones lineales por partes, etc. En el diseño del circuito se procura usar valores comerciales de resistencias y capacitores con precisión de 5%, a modo de que sea fácilmente realizable.

5.1 Bloque de integración

En el capítulo 4, se diseñó el encriptor descrito por las ecuaciones (4.32)-(4.35) y su respectivo sistema desencriptor (4.36)-(4.39). Al observar las ecuaciones del encriptor y desencriptor se encuentran muchas similitudes: el sistema dinámico (4.32) es, en estructura, igual a (4.36), la función no lineal (4.33) es igual a (4.37), y la ecuación (4.35) es muy parecida a (4.38); como consecuencia el diseño se facilita.

Para empezar se diseñará el bloque principal del encriptor y desencriptor, el cual corresponde a las ecuaciones (4.32) y (4.36), respectivamente. Dicho bloque está descrito por la ecuación:

$$\dot{\mathbf{v}} = \begin{bmatrix} 0 & -\tau & 0 \\ 0 & 0 & -\tau \\ 0 & \tau & -0.6\tau \end{bmatrix} \mathbf{v} + \begin{bmatrix} 0 \\ 0 \\ \tau \end{bmatrix} \left(f\left(v_1\right) + p\left(t\right) \right), \tag{5.1}$$

donde $\mathbf{v}, v_1, p\left(t\right)$ equivale a $\mathbf{x}, x_1, e\left(t\right)$ o $\mathbf{y}, y_1, \tilde{e}\left(t\right)$, según se trate del bloque encriptor o desencriptor.

La ecuación (5.1) es equivalente al sistema de ecuaciones integrales:

$$\begin{cases} v_1 = -\tau \int v_2 dt \\ v_2 = -\tau \int v_3 dt \\ v_3 = -\tau \int \left(-v_2 + 0.6 v_3 - f\left(v_1\right) - p\left(t\right) \right) dt \end{cases} . \qquad (5.2)$$

Cada operación integral de (5.2) puede ser implementada con un arreglo de integrador inversor, como el mostrado en la Figura 5-1.

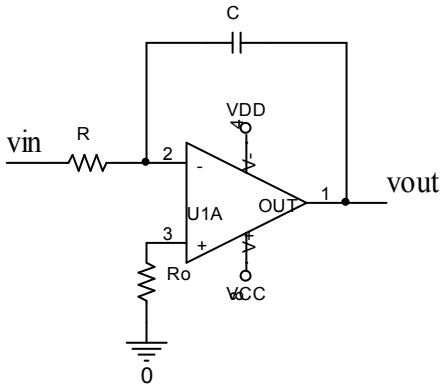

Figura 5-1 Circuito integrador Inversor.

La función de transferencia del integrador inversor es:

$$v_{out} = -\frac{1}{RC} \int v_{in} dt \, . \qquad (5.3)$$

Por lo tanto, el sistema de ecuaciones integrales (5.2) puede realizarse en un circuito como el mostrado en la Figura 5-2, donde $R_{v1,v2,v3} C_{v1,v2,v3} = \tau^{-1} = 2 \times 10^{-5}$. Si $R_{v1,v2,v3} = 10k\Omega$, entonces $C_{v1,v2,v3} = 2nF$. Para minimizar niveles de offset en los amplificadores operacionales la resistencia que ve la terminal negativa del amplificador operacional debe ser igual o parecida a la que ve su terminal positiva; por lo anterior se hace que $R_{v4,v5,v6} = 10k\Omega$.

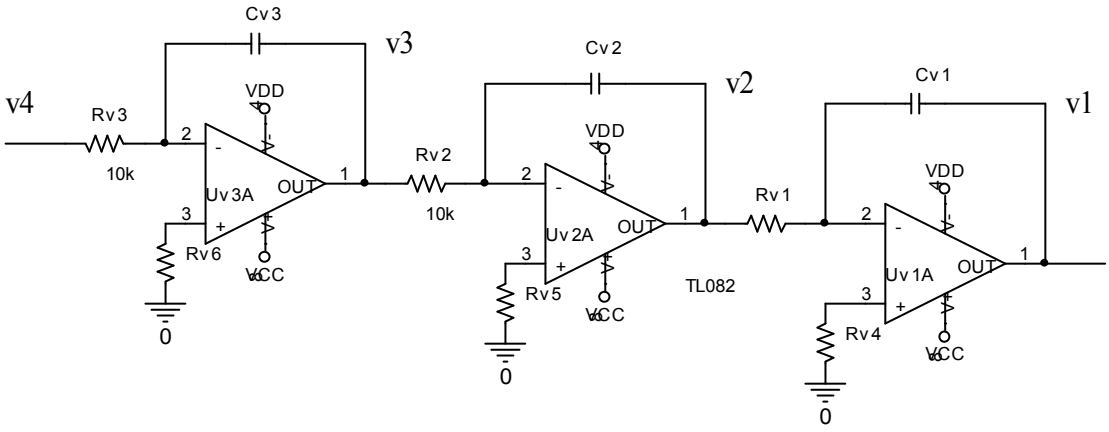

Figura 5-2 Circuito del bloque integrador.

La señal de entrada al integrador número tres es:

$$v_4 = -v_2 + 0.6v_3 - f\left(v_1\right) - p\left(t\right), \tag{5.4}$$

y puede obtenerse de un amplificador operacional sumador/restador conectado como se muestra en la Figura 5-3.

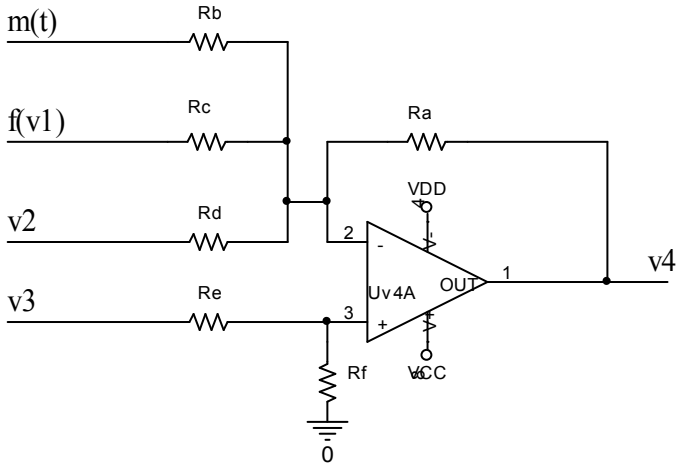

Figura 5-3 Circuito sumador/restador para retroalimentación del bloque de integración.

La función se transferencia para este arreglo está dada por:

$$v_4 = -\frac{R_a}{R_b}p\left(t\right) - \frac{R_a}{R_c}g\left(v_1\right) - \frac{R_a}{R_d}v_2 + \frac{R_f}{R_b \parallel R_c \parallel R_d}\left(\frac{R_a + R_b \parallel R_c \parallel R_d}{R_e + R_f}\right)v_3 . \tag{5.5}$$

Igualando (5.4) con (5.5) se obtiene:

$$\frac{R_a}{R_b} = \frac{R_a}{R_c} = \frac{R_a}{R_d} = 1, \tag{5.6}$$

$$\frac{R_f}{R_b \parallel R_c \parallel R_d}\left(\frac{R_a + R_b \parallel R_c \parallel R_d}{R_e + R_f}\right) = 0.6. \tag{5.7}$$

De la ecuación (5.6) se concluye que:

$$R_a = R_b = R_c = R_d. \tag{5.8}$$

Para minimizar niveles de offset indeseados en el amplificador operacional, se debe procurar:

$$\frac{R_e R_f}{R_e + R_f} = \frac{R_a}{4}. \tag{5.9}$$

A partir de (5.7) y de (5.8) se tiene que:

$$\left(\frac{R_f}{R_e + R_f}\right)\left(\frac{R_a + \frac{R_a}{3}}{\frac{R_a}{3}}\right) = \frac{3}{5}, \tag{5.10}$$

$$\frac{R_f}{R_e + R_f} = \frac{3}{20}. \tag{5.11}$$

De dividir (5.9) entre (5.11) se llega a:

$$R_e = \frac{5}{3} R_a. \tag{5.12}$$

Por último, sustituyendo (5.12) en (5.11) se obtiene:

$$R_f = \frac{5}{17} R_a. \tag{5.13}$$

Las ecuaciones (5.8), (5.12), (5.13) están expresadas en función de la resistencia R_a, Si se escoge $R_a = 12k\Omega$, entonces se tiene que las demás resistencias son: $R_b = 12k\Omega$, $R_c = 12k\Omega$, $R_d = 12k\Omega$, $R_a = 20k\Omega$, $R_a \approx 3.529k\Omega \rightarrow 3.6k\Omega$.

5.2 Bloque de sincronización

La ecuación (4.35) expresa la señal que es mandada del encriptor al desencriptor y consta de la señal encriptada y de una señal de sincronía. Por su parte, la ecuación (4.38) muestra la señal que se genera en el desencriptor como estimación de la señal encriptada y sirve para estabilizar la sincronía en el criptosistema y para recuperar el mensaje. La estructura de ambas ecuaciones es:

$$q(t) = -p(t) - f(v_1) - v_1 + 2v_2 - 2.4v_3, \tag{5.14}$$

donde $q(t), p(t), v_1, v_2, v_3$ equivalen a $z(t), e(t), x_1, x_2, x_3$, en el caso del encriptor, y a $\tilde{e}(t), z(t), y_1, y_2, y_3$, en el caso del desencriptor.

La ecuación (5.14) puede ser realizada por el circuito de la Figura 5-4.

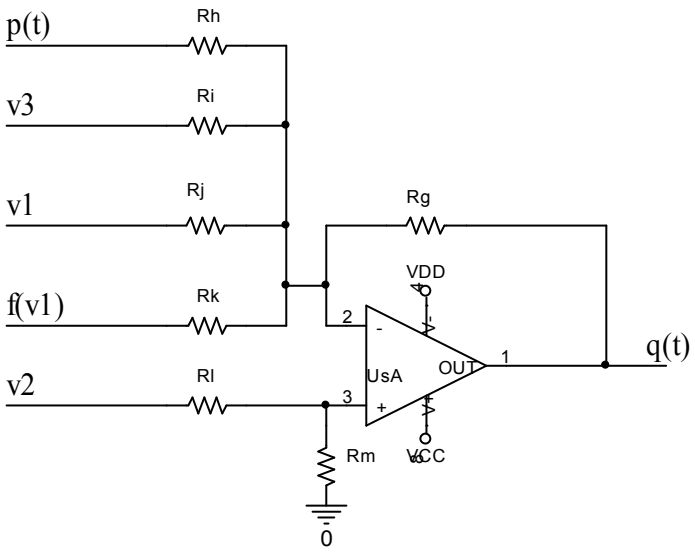

Figura 5-4 Circuito del bloque de sincronización.

La función de transferencia del circuito de la Figura 5-4 es:

$$\begin{aligned} q(t) = &-\frac{R_g}{R_h}p(t) - \frac{R_g}{R_i}v_3 - \frac{R_g}{R_j}v_1 - \frac{R_g}{R_k}f(v_1) \\ &+ \frac{R_m}{R_h \parallel R_i \parallel R_j \parallel R_k}\left(\frac{R_g + R_h \parallel R_i \parallel R_j \parallel R_k}{R_l + R_m}\right)v_2. \end{aligned} \tag{5.15}$$

Si se iguala la ecuación (5.15) con (5.14) se tiene que:

$$\frac{R_g}{R_h}=\frac{R_g}{R_j}=\frac{R_g}{R_k}=1, \tag{5.16}$$

$$\frac{R_g}{R_i}=2.4, \tag{5.17}$$

$$\frac{R_m}{R_h \,||\, R_i \,||\, R_j \,||\, R_k}\left(\frac{R_g + R_h \,||\, R_i \,||\, R_j \,||\, R_k}{R_l + R_m}\right)=2. \tag{5.18}$$

Si se hace que $R_g = 36k\Omega$, entonces a partir de (5.16) y (5.17) se puede concluir que $R_h = 36k\Omega$, $R_j = 36k\Omega$ y $R_k = 36k\Omega$, y $R_i = 15k\Omega$. Por su parte la ecuación (5.18) se vuelve:

$$\left(\frac{R_m}{R_l + R_m}\right)\left(\frac{36k\Omega+\frac{20}{3}k\Omega}{\frac{20}{3}k\Omega}\right)=2, \tag{5.19}$$

$$\frac{R_m}{R_l + R_m}=\frac{5}{16}. \tag{5.20}$$

Para minimizar niveles de offset de voltaje se debe cumplir:

$$\frac{R_l R_m}{R_l + R_m}=R_g \,||\, R_h \,||\, R_i \,||\, R_j \,||\, R_k=\frac{45}{8}k\Omega. \tag{5.21}$$

Dividiendo la ecuación (5.21) por la ecuación (5.20) se obtiene que $R_l = 18k\Omega$, y por consiguiente de la ecuación (5.20) se concluye que $R_m = 8.\overline{18}k\Omega \rightarrow 8.2k\Omega$.

5.3 Bloque de función no lineal

La función no lineal que se muestra en la ecuación (5.22), aparece tanto en el encriptor ($v_1 = x_1$) como en el desencriptor ($v_1 = y_1$):

$$f(v_1)=\frac{\delta}{2\alpha}\left(|v_1+\alpha|-|v_1-\alpha|\right)-\mu v_1, \tag{5.22}$$

donde $\delta = 1.35$, $\mu = 1$, $\alpha = 0.3375$.

Dicha función es una función lineal por partes que se puede expresar de forma análoga como:

$$f(v_1) = \begin{cases} -\mu v_1 - \delta & v_1 < -\alpha \\ \left(\frac{\delta}{\alpha} - \mu\right) v_1 & |v_1| \le \alpha \\ -\mu v_1 + \delta & v_1 > \alpha \end{cases} . \qquad (5.23)$$

El circuito que se propone para implementar tal función es el que se muestra en la Figura 5-5.

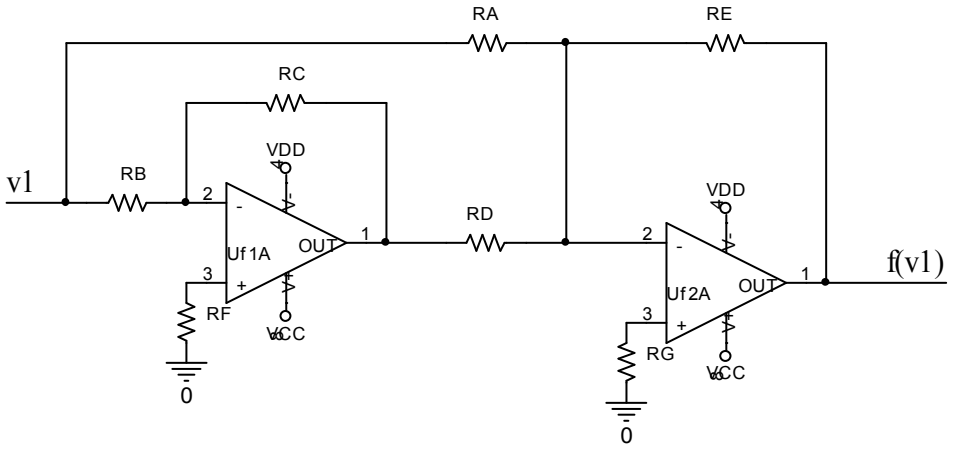

Figura 5-5 Circuito de la función no lineal f(v1).

Por lo general, los efectos de saturación de un amplificador operacional no se toman en cuenta en la función de transferencia. Sin embargo, en esta ocasión se usan para formar la función lineal por partes. La función de transferencia del circuito de la Figura 5-5 es:

$$f(v_1) = \begin{cases} -\frac{R_E}{R_A} v_1 - \frac{R_E}{R_D} V_{SAT} & v_1 < -\frac{R_B}{R_C} V_{SAT} \\ -\frac{R_E}{R_A} v_1 + \frac{R_E}{R_D}\frac{R_C}{R_B} v_1 & |v_1| \le \frac{R_B}{R_C} V_{SAT} \\ -\frac{R_E}{R_A} v_1 + \frac{R_E}{R_D} V_{SAT} & v_1 > \frac{R_B}{R_C} V_{SAT} \end{cases} . \qquad (5.24)$$

Si se iguala la ecuación (5.23) con (5.24) se obtiene que:

$$\frac{R_E}{R_A} = \mu, \tag{5.25}$$

$$\frac{R_E}{R_D} = \frac{\delta}{V_{SAT}}, \tag{5.26}$$

$$\frac{R_B}{R_C} = \frac{\alpha}{V_{SAT}}, \tag{5.27}$$

donde $\delta = 1.35$, $\mu = 1$, $\alpha = 0.3375$ y el voltaje de saturación típico es de $V_{SAT} = 13.5V$ cuando los amplificadores operacionales se alimentan con $\pm 15V$.

A partir de (5.25), (5.26) y (5.27), se llega a que $10R_A = 10R_E = R_D$ y que $R_C = 40R_B$. Si se escoge $R_D = 100k\Omega$, entonces $R_A = R_E = 10k\Omega$; por otro lado si se hace $R_B = 3k\Omega$, se tiene que $R_C = 120k\Omega$. Por último, para minimizar los niveles de offset en los amplificadores operacionales, se hace $R_F = 3k\Omega \approx R_B \,||\, R_C$ y $R_G = 4.7k\Omega \approx R_A \,||\, R_D \,||\, R_E$.

5.4 Bloque de la función de encripción

La función de encripción es una función que debe cumplir con la siguiente ecuación:

$$E\left(m(t), x_1\right) = g\left(m(t) + x_1\right) - g\left(x_1\right). \tag{5.28}$$

El núcleo del la función de encripción radica en la función g, la cual esta expresada por la ecuación:

$$g(v) = \begin{cases} -\rho v + \eta(1-\rho) & v < -\eta \\ -v & |v| < \eta \\ -\rho v - \eta(1-\rho) & v > \eta \end{cases} \tag{5.29}$$

donde $\rho = 1/10$ y $\eta = 0.7$. El circuito que se propone para implementar dicha función es el que muestra la Figura 5-6.

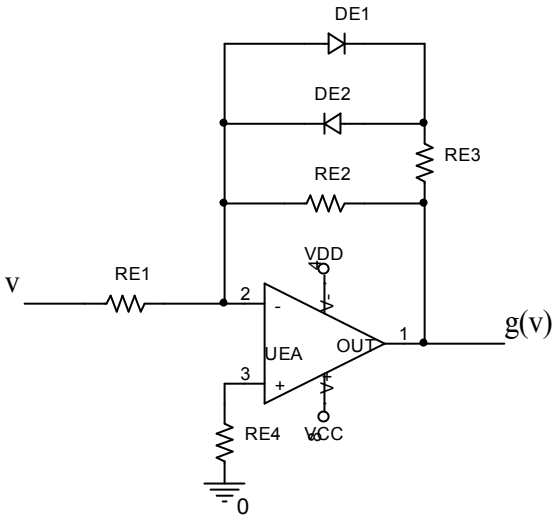

Figura 5-6 Circuito de la función g(v).

Usando el modelo de fuente de 0.7V del diodo, se tiene que ninguno de los dos diodos conduce cuando el voltaje a la salida del amplificador operacional es de magnitud menor a 0.7V, y por lo tanto la resistencia de retroalimentación es R_{E2}. En cambio si la magnitud del voltaje de salida excede los 0.7V, entonces uno de los dos diodos conduce y se comporta como fuente de voltaje de 0.7V y la retroalimentación se comporta como una resistencia de $\text{R}_{\text{E2}}||\text{R}_{\text{E2}}$ con un nivel de c.d. La función de transferencia del circuito de la Figura 5-6 es:

$$g(v)=\begin{cases} -\dfrac{1}{R_{E1}}\dfrac{R_{E2}R_{E3}}{R_{E2}+R_{E3}}v+\dfrac{0.7R_{E2}}{R_{E2}+R_{E3}} & v<-0.7 \\ -\dfrac{R_{E2}}{R_{E1}}v & |v|<0.7 \\ -\dfrac{1}{R_{E1}}\dfrac{R_{E2}R_{E3}}{R_{E2}+R_{E3}}v-\dfrac{0.7R_{E2}}{R_{E2}+R_{E3}} & v>0.7 \end{cases} \tag{5.30}$$

Igualando (5.30) con (5.29) se tiene que:

$$\frac{\text{R}_{\text{E2}}}{\text{R}_{\text{E1}}}=1, \tag{5.31}$$

$$\rho=\frac{1}{R_{E1}}\frac{R_{E2}R_{E3}}{R_{E2}+R_{E3}}, \tag{5.32}$$

$$1-\rho=\frac{R_{E2}}{R_{E2}+R_{E3}}. \tag{5.33}$$

De las ecuaciones (5.32), (5.33) se llega a la expresión:

$$R_{E3}=\frac{R_{E1}}{\rho^{-1}-1} \tag{5.34}$$

Dado que $\rho=1/10$ y $\eta=0.7$; si se escoge $\mathrm{R_{E1}}=\mathrm{R_{E2}}=27k\Omega$, entonces $\mathrm{R_{E3}}=3k\Omega$, y para minimizar niveles de offset en el amplificador operacional se hace que $\mathrm{R_{E4}}=13k\Omega$, lo que aproximadamente es el valor de $\mathrm{R_{E1}}\,||\,\mathrm{R_{E2}}$. Si se necesitara realizar la función $g(x+y)$, basta con aumentar una entrada con una resistencia de valor $\mathrm{R_{E1}}$ a la terminal negativa del amplificador operacional, así el circuito realizará la función g además de servir de sumador.

Una vez que se tiene diseñada el circuito para la función g, el circuito de la función de la función de encripción $E(m(t),x_1)=g(m(t)+x_1)-g(x_1)$, puede llevarse a cabo dos bloques de la función g y un restador: un bloque calcula $g(m(t)+x_1)$, el otro $g(x_1)$, y el restador genera la señal encriptada $e(t)$, tal como se muestra en la Figura 5-7.

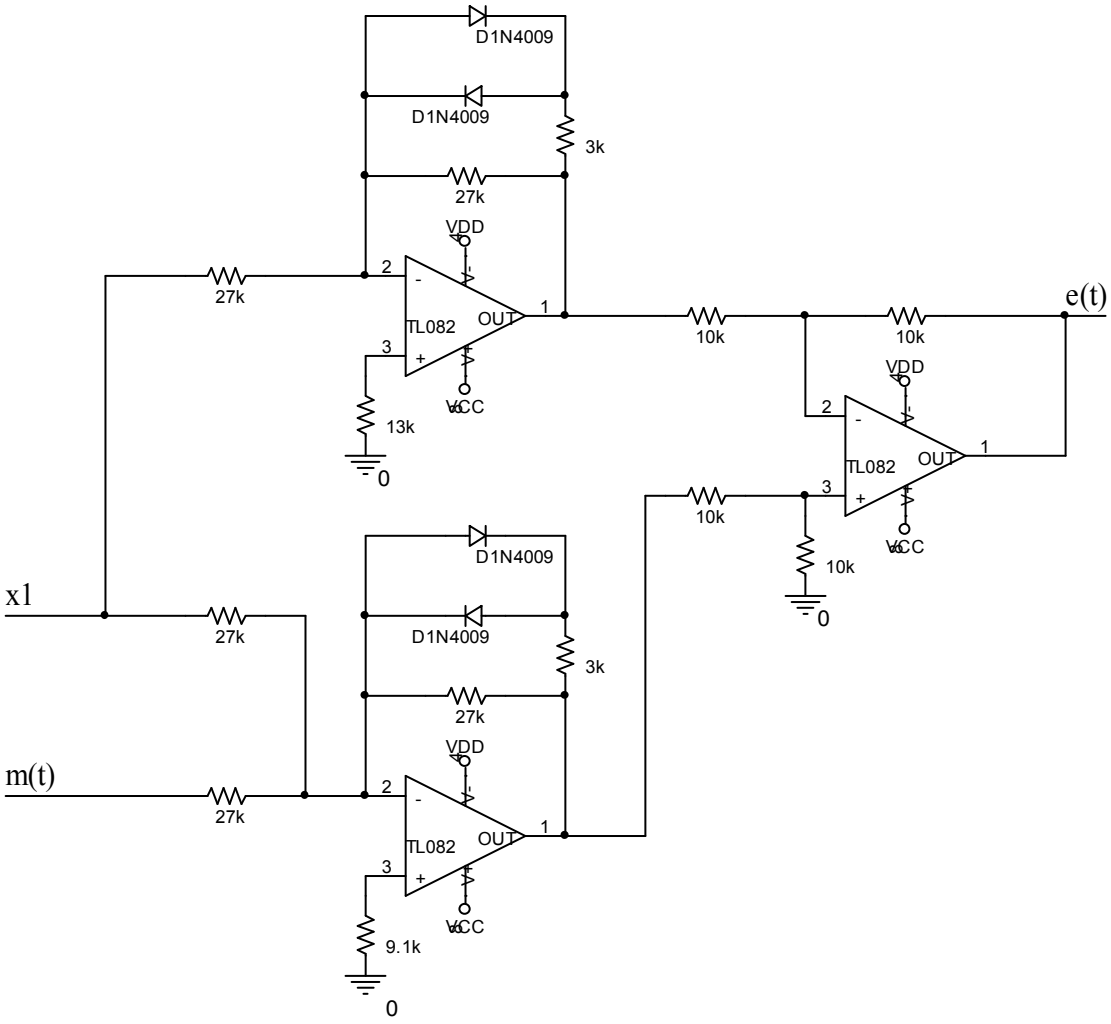

Figura 5-7 Circuito de la función de encripción E.

5.5 Bloque de la función de desencripción

La función de desencripción es una función que debe cumplir con la ecuación:

$$D\left(\tilde{e}\left(t\right), y_1\right) = g^{-1}\left(\tilde{e}\left(t\right) + g\left(y_1\right)\right) - y_1 . \tag{5.35}$$

En la ecuación (5.35), la función g es la misma que se desarrolló en la sección pasada y su inversa es:

$$g^{-1}\left(v\right) = \begin{cases} -\rho^{-1}v + \eta\left(1-\rho^{-1}\right) & v < -\eta \\ -v & \left|v\right| < \eta \\ -\rho^{-1}v - \eta\left(1-\rho^{-1}\right) & v > \eta \end{cases}, \tag{5.36}$$

donde $\rho = 1/10$ y $\eta = 0.7$. El circuito que se propone para la función g^{-1} se muestra en la Figura 5-8.

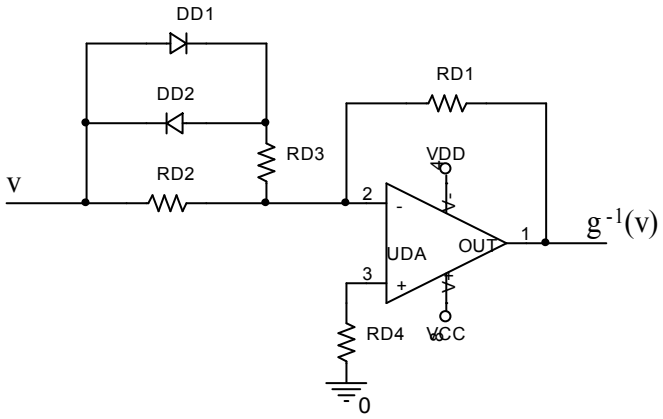

Figura 5-8 Circuito de la función $g^{-1}(v)$.

Usando el modelo de fuente de $0.7V$ del diodo, se tiene que ninguno de los dos diodos conduce cuando el voltaje de entrada es de magnitud menor a $0.7V$, y por lo la resistencia de entrada es R_{D2}. En cambio si la magnitud del voltaje de entrada excede los $0.7V$, entonces uno de los dos diodos conduce y se comporta como fuente de voltaje de $0.7V$, y la resistencia de entrada se comporta como una resistencia de $R_{D2}||R_{D3}$ con un nivel de c.d. La función de transferencia del circuito de la Figura 5-6 es:

$$g(v) = \begin{cases} -R_{D1}\dfrac{R_{D2}+R_{D3}}{R_{D2}R_{D3}}v - \dfrac{0.7R_{D1}}{R_{D3}} & v < -0.7 \\ -\dfrac{R_{D1}}{R_{D2}}v & |v| < 0.7 \\ -R_{D1}\dfrac{R_{D2}+R_{D3}}{R_{D2}R_{D3}}v + \dfrac{0.7R_{D1}}{R_{D3}} & v > 0.7 \end{cases}. \qquad (5.37)$$

Si se iguala (5.37) a (5.36) se llega a

$$\frac{R_{D1}}{R_{D2}} = 1, \qquad (5.38)$$

$$\rho = \frac{1}{R_{D1}}\frac{R_{D2}R_{D3}}{R_{D2}+R_{D3}}, \qquad (5.39)$$

$$1-\rho^{-1}=\frac{R_{D1}}{R_{D3}}. \tag{5.40}$$

Se tiene que $\rho=1/10$ y $\eta=0.7$; si se escoge $\mathrm{R}_{\mathrm{D1}}=\mathrm{R}_{\mathrm{D2}}=27k\Omega$, entonces $\mathrm{R}_{\mathrm{D3}}=3k\Omega$, y se escoge $\mathrm{R}_{D4}=13k\Omega$, para minimizar niveles de offset. Con la los circuitos que se han diseñado se puede implementar la función $D\left(\tilde{e}\left(t\right),y_1\right)=g^{-1}\left(\tilde{e}\left(t\right)+g\left(y_1\right)\right)-y_1$. Como la fórmula lo expresa primero se pasa la variable y_1 por un circuito con función g, ese resultado se suma a la estimación de la señal encriptada $\tilde{e}\left(t\right)$. El resultado de dicha suma se hace pasar por un circuito con función g^{-1} a cuya salida se le resta y_1; el resultado de la resta es la estimación de la señal de información $\tilde{m}\left(t\right)$, como se muestra en la Figura 5-9.

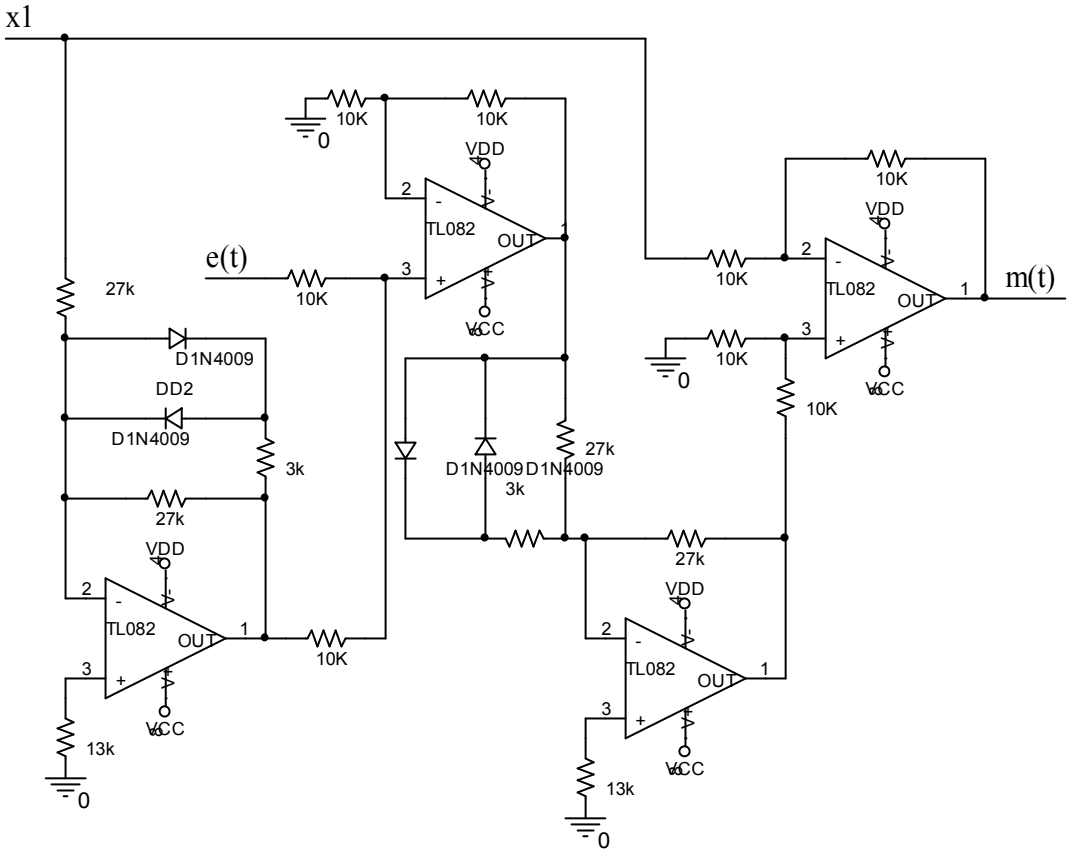

Figura 5-9 Circuito de la función de desencripción D.