6 Simulaciones del criptosistema caótico y del criptocircuito caótico.

En este capítulo se presentan una serie de simulaciones donde se analiza el desempeño del criptosistema caótico en cuanto a seguridad y en cuanto a la calidad de la información recuperada en el desencriptor. En la primera sección se analiza la dinámica del sistema con diferentes niveles de potencia de la señal de información. En la segunda sección se analiza la sincronización del circuito encriptor y desencriptor en condiciones ideales sin ruido, y después se procede a hacer lo mismo bajo en condiciones que presenten ruido y se estudia la forma en la que el sistema se ve afectado por el ruido. En la tercera sección se analiza la seguridad que ofrece el criptosistema, y por medio de las simulaciones se dan una serie de recomendaciones en referencia a las características de la señal de información a encriptar. Por último en la cuarta sección se muestran las simulaciones del circuito diseñado a partir del criptosistema y se muestra que su comportamiento concuerda con el esperado.

6.1 Relación señal de información a llave caótica (KMR)

El criptosistema caótico diseñado tiene como objetivo garantizar una comunicación segura; esto se logra si un intruso es incapaz de entender la señal que se transmite del encriptor al desencriptor. Para empezar por medio de simulaciones se analizó el nivel de potencia que debe de tener la señal de información que entra al encriptor.

Como ya se ha comentado, la señal de información entra al encriptor, específicamente al bloque de la función de encripción donde es mezclada no linealmente con la llave caótica x_1. La función de encripción se diseñó para que en promedio no afectara la trayectoria del sistema caótico, sin embargo, si la señal de información tiene mucha potencia, puede sacar

al sistema de una región caótica. Asumiendo que la señal de información es un proceso aleatorio, por medio de simulaciones se encontró que la potencia de la señal de información debe de tener menor potencia que la llave que la encripta x_1; dicho de otro modo, la relación entre la potencia de la señal de la llave y el mensaje debe ser mayor a cero, a esta relación se le llamará de ahora en adelante KMR.

Las Figura 6-1 a 6-4, muestran el plano de fases de las variables x_1 y x_2, para diversos valores del KMR, la fuente de información se simuló como un proceso aleatorio con un ancho de banda de 5kHz. Se puede observar que de preferencia la señal de información debe tener una potencia menor a 2.5dBW, que es aproximadamente la potencia de la señal caótica de la llave, ya que si se es mayor a este valor es probable que el sistema dinámico salga de su régimen caótico, como se ve el la Figura 6-4.

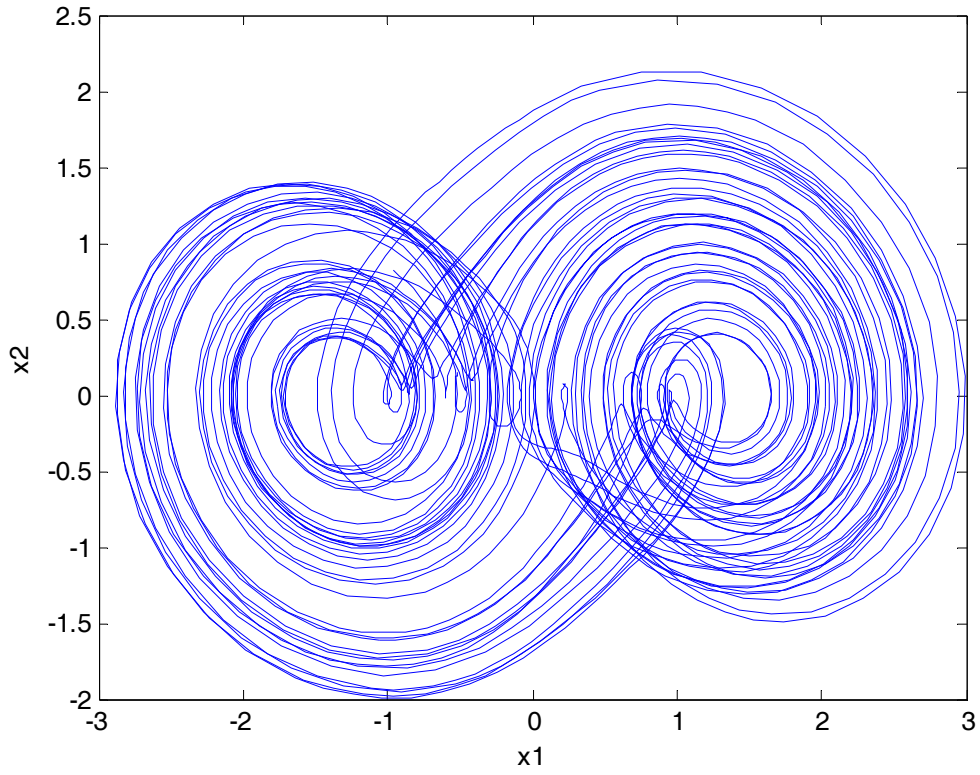

Figura 6-1 Diagrama de fases x1, x2 para KMR=22.5dB. (m(t) @ -20dBW).

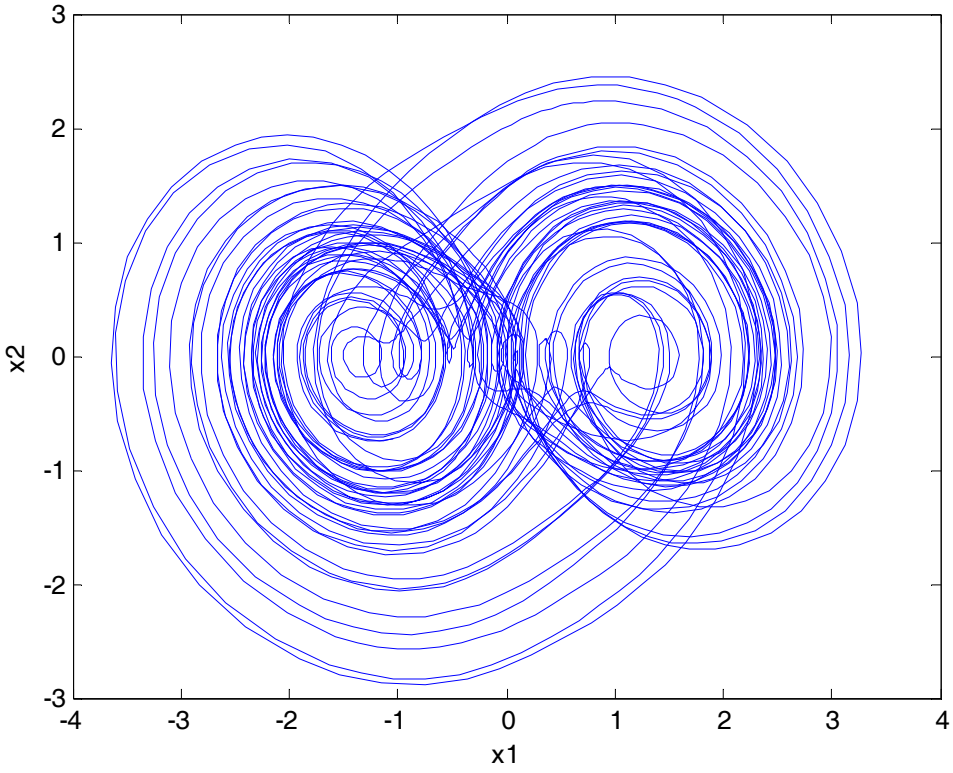

Figura 6-2 Diagrama de fases x1, x2 para KMR=12.5dB. (m(t) @ -10dBW).

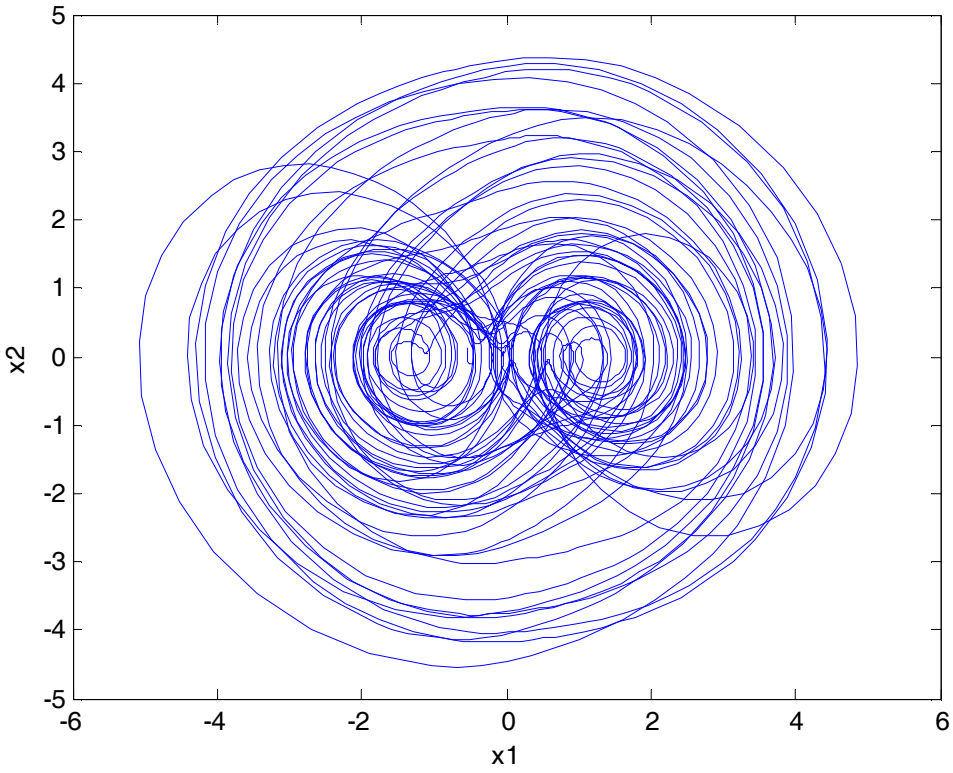

Figura 6-3 Diagrama de fases x1, x2 para KMR=2.5dB. (m(t) @ 0dBW).

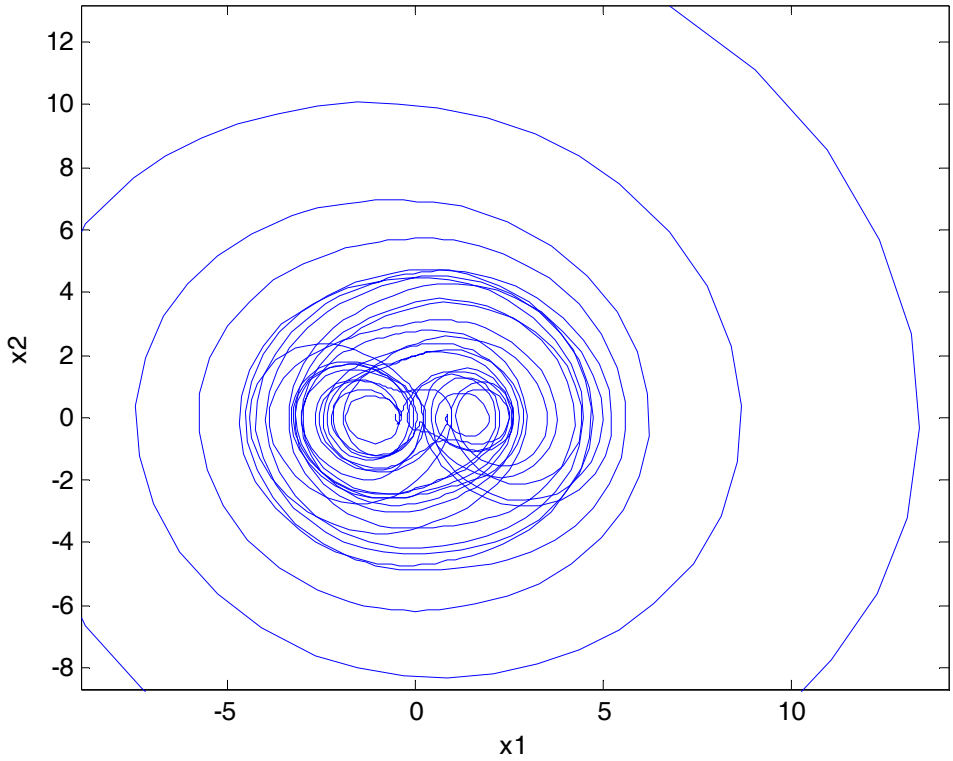

Figura 6-4 Diagrama de fases x1, x2 para KMR=0.5dB. (m(t) @ 3dBW).

En suma, se recomienda utilizar un nivel de potencia menor a -10dBW en la señal de información, lo que además garantizará mayor seguridad ya que al ser mayor la llave caótica que la señal de información, el proceso de encripción ocultará más la señal.

6.2 Sincronización y recuperación de la información

El criptosistema además de dar un buen nivel de seguridad, debe de lograr que la señal desencriptada sea lo más parecida posible a la señal de información, esto se logra cuando el encriptor y el desencriptor se sincronizan de forma correcta.

6.2.1 Canal sin ruido

Si el criptosistema funciona en un sistema sin ruido, es posible recobrar perfectamente la señal de información en el desencriptor; esto se debe a que el desencriptor es un

observador no lineal del encriptor, y por lo tanto puede seguir su dinámica. Para demostrar esto se simuló el criptosistema caótico con relación llave caótica a información (KMR) con la que se trabajó es de -10dB, donde la señal de información fue representada por un proceso aleatorio de potencia igual a -7.5dBW y ancho de banda de 5kHz.

La Figura 6-5 muestra la evolución en el tiempo de los errores de sincronización (e_1, e_2, e_3) entre las variables de encriptor y el desencriptor, ahí se aprecia cómo de cómo en aproximadamente $5/\tau = 10^{-4}\,s$, el sistema desencriptor se sincroniza con el encriptor.

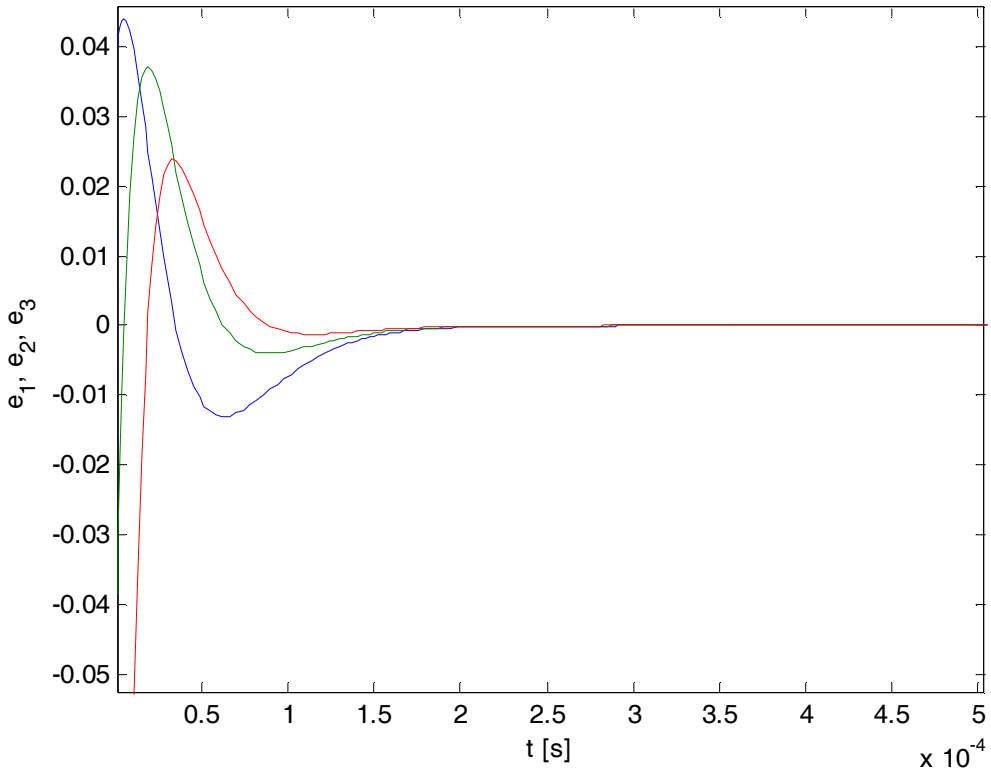

Figura 6-5 Error de sincronización e_1 (azul), e_2 (rojo), e_3 (verde), KMR=10dB y canal sin ruido.

La Figura 6-6 muestra a la señal de información que entra al encriptor (verde) y la señal de información que se recupera en el desencriptor (azul), por lo tanto se ve que en ausencia de ruido el criptosistema se comporta de la forma esperada y la señal de información se puede recuperar sin ruido.

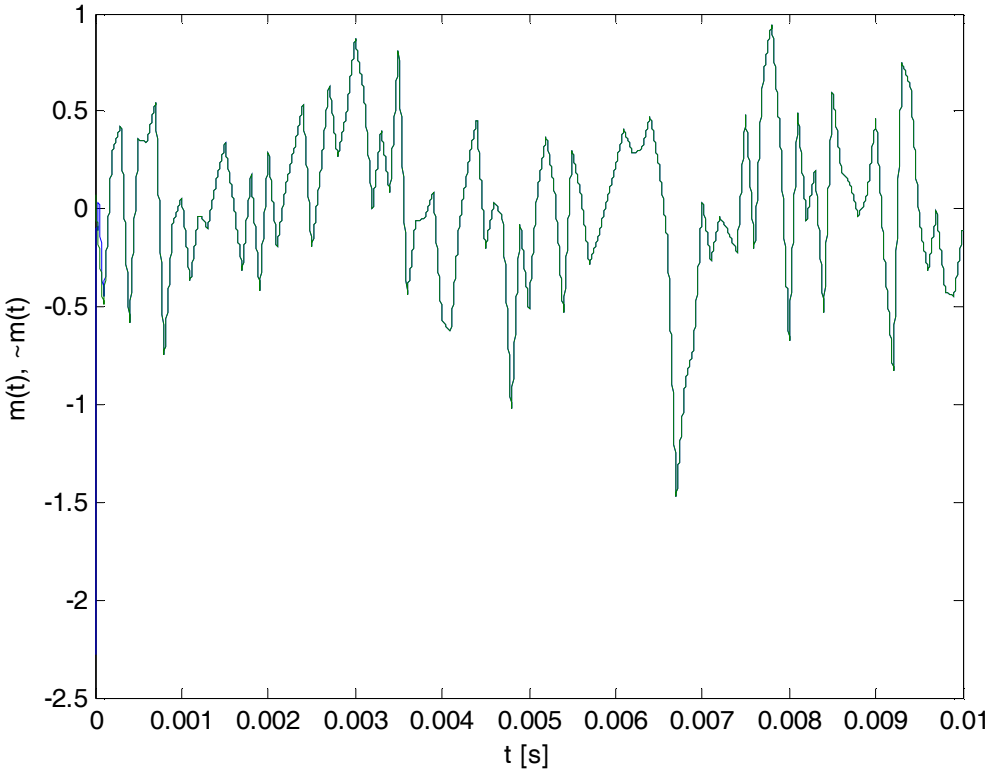

Figura 6-6 Señal de información original (verde) y estimada (azul), KMR=10dB y canal sin ruido.

6.2.2 Canal con ruido

Si el canal tiene ruido no será posible lograr una sincronización perfecta entre los estados del sistema, por lo tanto la señal de información estimada en el desencriptor presentará niveles de ruido, proporcionales al nivel de ruido del canal. La señal que se envía por el canal es una combinación entre estados del sistema y la señal encriptada, por lo tanto el análisis de cómo afecta el ruido en la transmisión se hará agregando ruido a la señal transmitida (y no a la señal de información o a la señal encriptada). A continuación se presentan simulaciones para situaciones con KMR=10dB y una relación entre la señal enviada a ruido de canal SNR= 60dB, 40dB, 20dB.

Si KMR=10dB y SNR=60dB, el error de sincronización no se estabiliza en cero si no que se mantiene variando muy cercanamente éste. Las oscilaciones de los errores de

sincronización del sistema que se mantienen alrededor de cero son una consecuencia de las ligeras variaciones en las oscilaciones de la señal trasmitida. La Figura 6-7 muestra la evolución en el tiempo de los errores entre los estados del sistema desencriptor y encriptor.

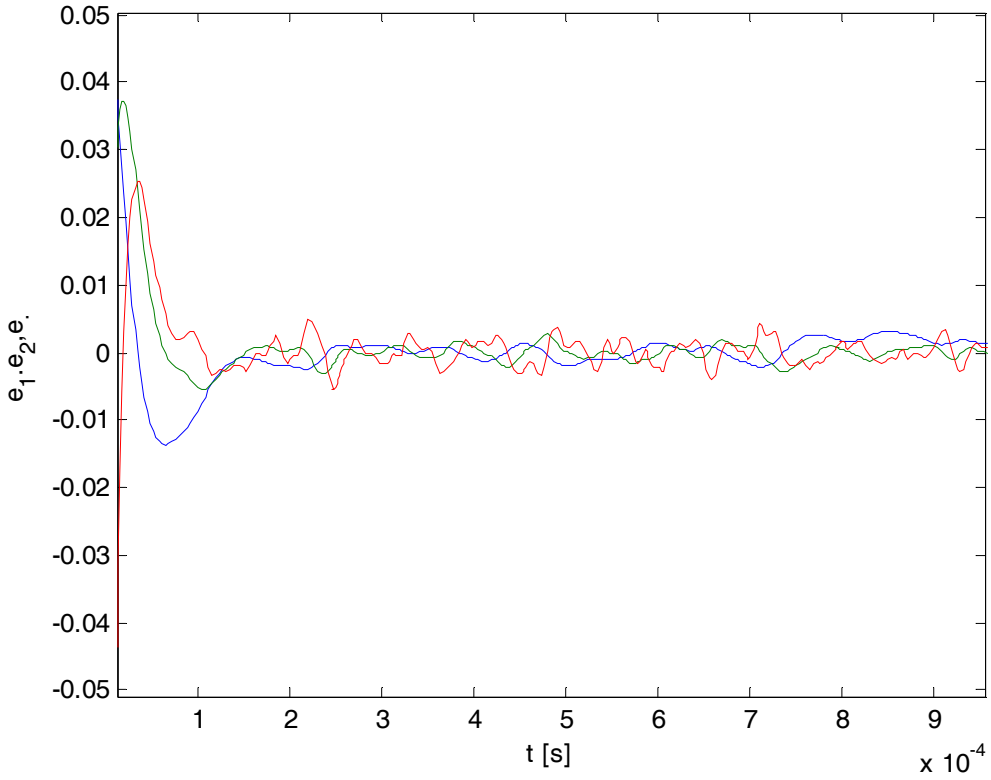

Figura 6-7 Error de sincronización e_1 (azul), e_2 (rojo), e_3 (verde), KMR=10dB y SNR=60dB.

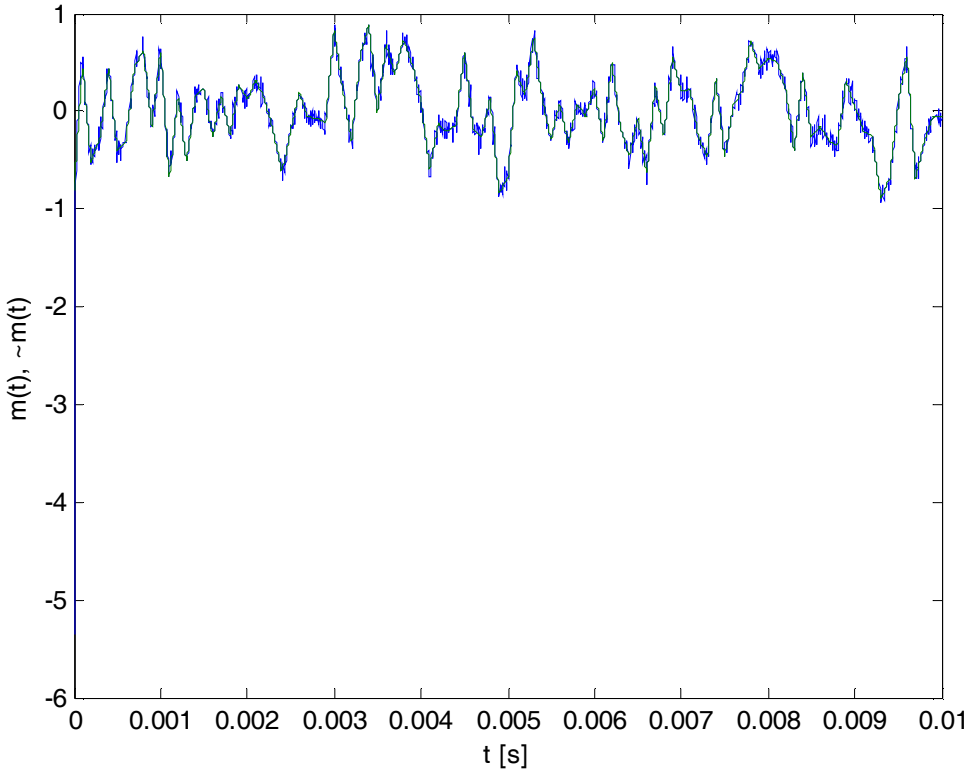

Figura 6-8 Señal de información original (verde) y estimada (azul), KMR=10dB y SNR=60dB.

La señal de información original y la recobrada se muestran en la Figura 6-8, ahí se puede ver que la señal de información estimada está afectada por pequeños niveles de ruido y se calculó que la relación de señal de información recuperada a ruido (MNR) en el desencriptor era de 28dB.

Si KMR=10dB y SNR=40dB, el error de sincronización no se estabiliza en cero, pero se mantiene aproximadamente cercano a este valor. La Figura 6-9 muestra la evolución en el tiempo de los errores entre los estados del sistema desencriptor y encriptor.

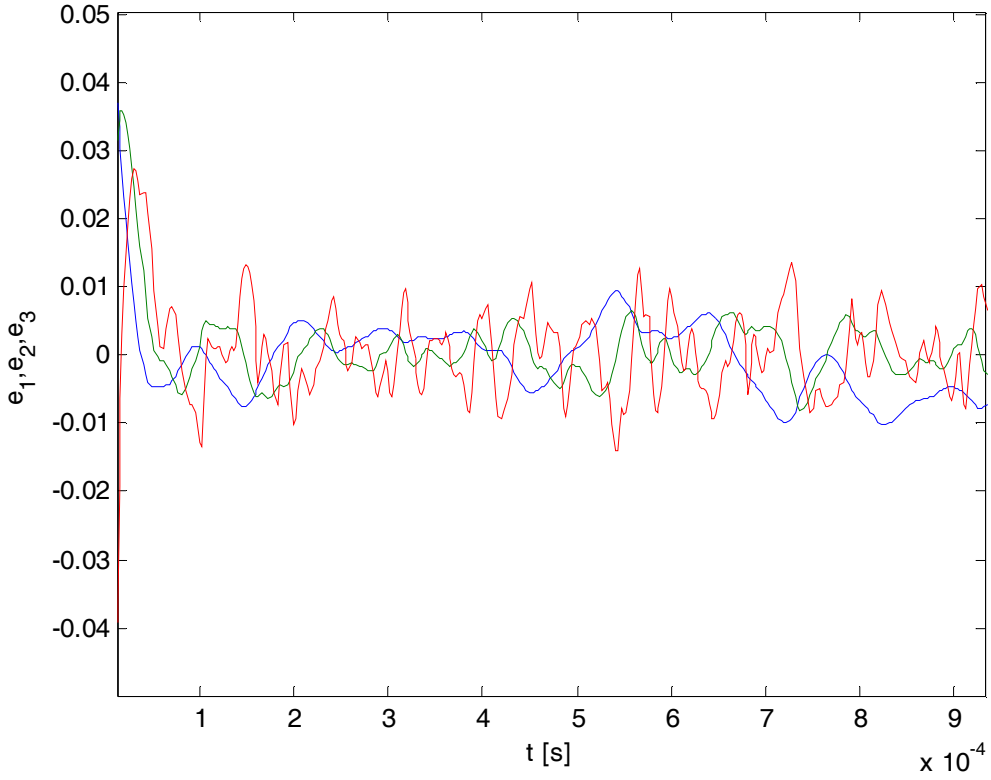

Figura 6-9 Error de sincronización e_1 (azul), e_2 (rojo), e_3 (verde), KMR=10dB y SNR=40dB.

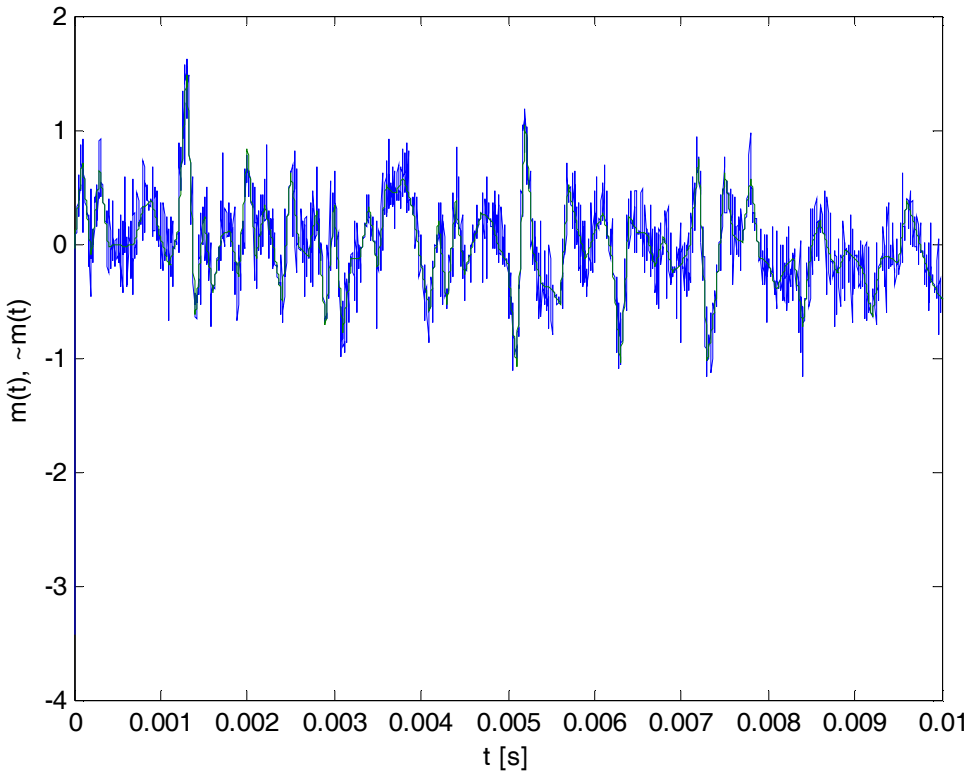

Figura 6-10 Señal de información original (verde) y estimada (azul), KMR=10dB y SNR=40dB.

Por otro lado, la señal de información original y la recobrada se muestran en la Figura 6-10, se puede observar que la señal de información estimada está afectada por ruido y se calculó que la relación de señal de información recuperada a ruido (MNR) en el desencriptor era de 8.7dB.

Por último, si KMR=10dB y SNR=20dB, el error de sincronización no se estabiliza en cero ni queda cercano a dicho valor. La Figura 6-11 muestra la evolución en el tiempo de los errores entre los estados del sistema desencriptor y encriptor.

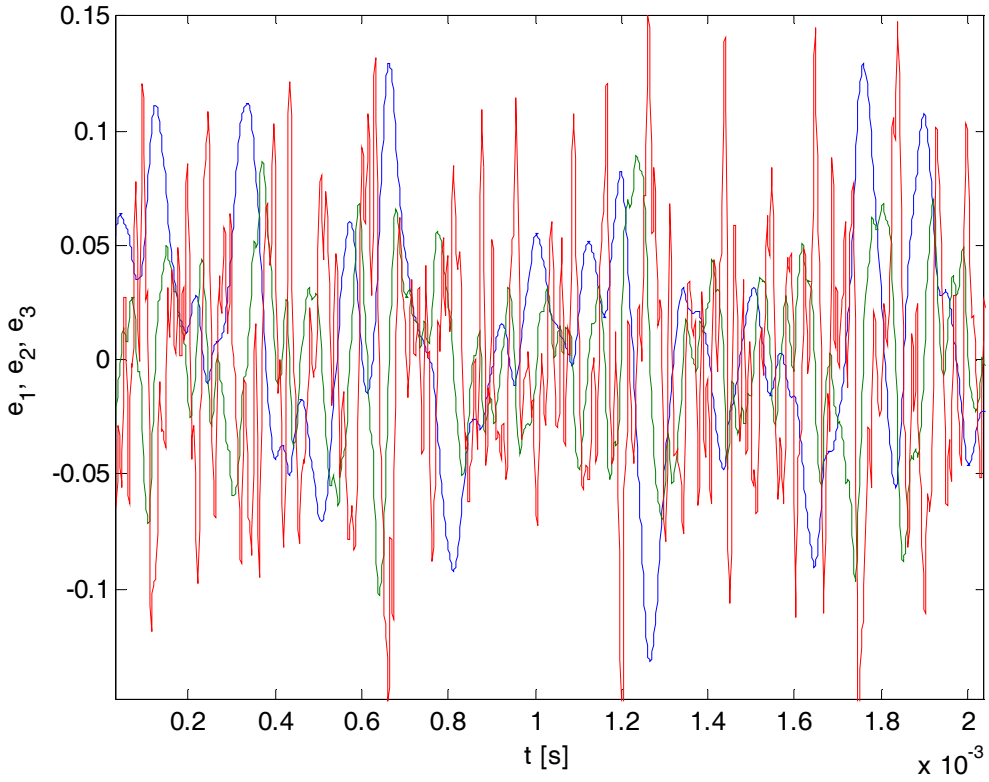

Figura 6-11 Error de sincronización e_1 (azul), e_2 (rojo), e_3 (verde), KMR=10dB y SNR=20dB.

La señal de información original y la recobrada se muestran en la Figura 6-12, se aprecia que la señal de información estimada está afectada por ruido muy fuertemente, el radio de señal de información a ruido se calculo ser de MNR=-5.1dB lo que significa que el ruido es mayor a la señal de información.

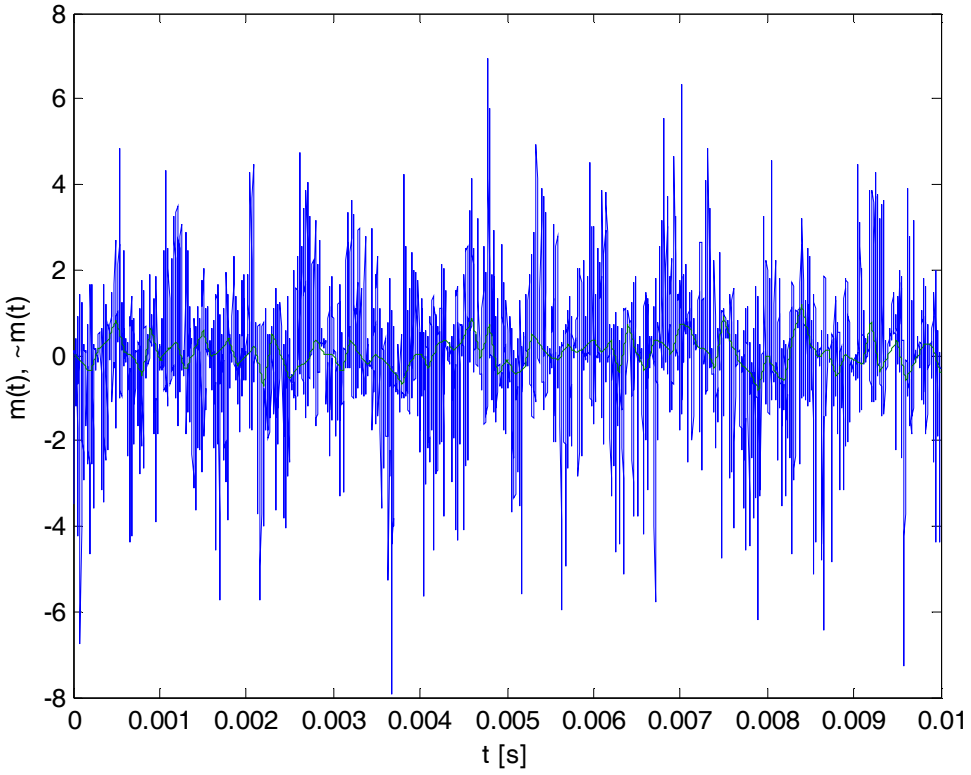

Figura 6-12 Señal de información original (verde) y estimada (azul), KMR=10dB y SNR=40dB.

Se pudo ver en las simulaciones anteriores que el ruido blanco aditivo del canal afecta la sincronización entre el desencriptor y el encriptor. Dada una relación llave a señal de información en el encriptor (KMR), la relación señal transmitida a ruido del canal (SNR) se ve reflejada directamente en la relación señal de información a ruido en el desencriptor (MNR); la relación entre estos dos radios se muestra en la Figura 6-13.

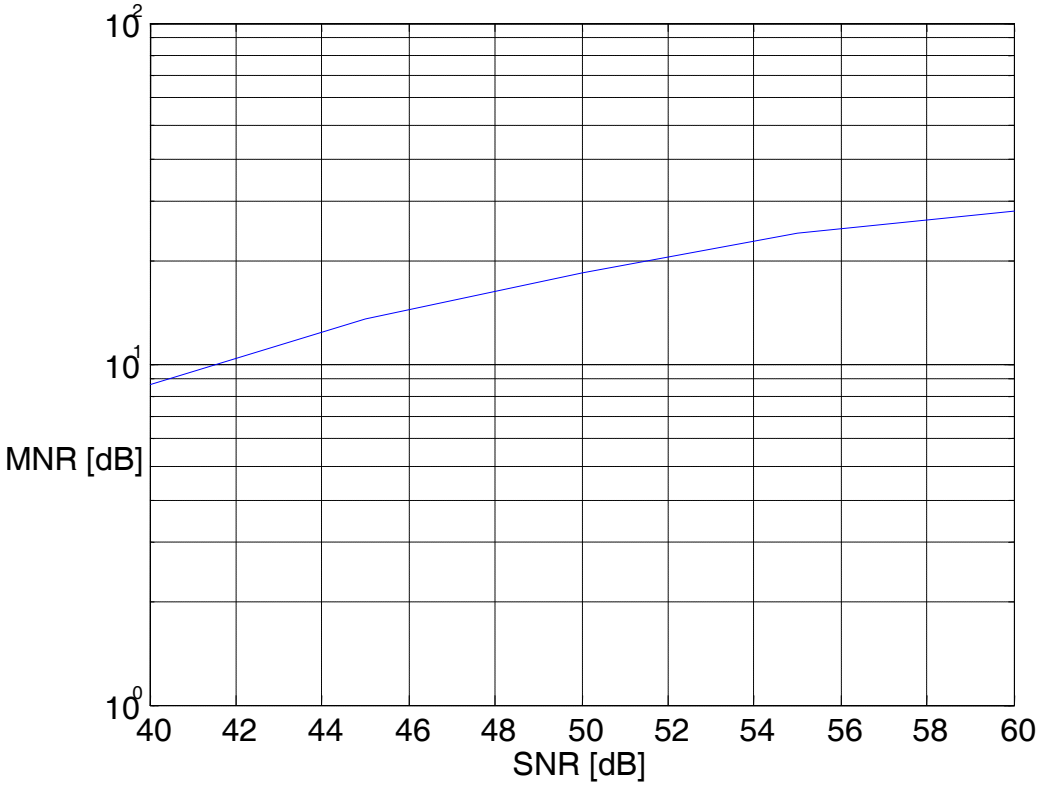

Figura 6-13 Relación entre SNR en el canal y MNR en el desencriptor, KMR=10dB.

En la Figura 6-13 se observa cómo el ruido del canal afecta más a la señal de información de lo que le afecta a la señal que se transmitió, esto se debe que al dañar a la señal transmitida el ruido daña a la vez a la señal encriptada y a la señal de sincronización. Por lo anterior la señal de información que se recupera en el desencriptor es más afectada ya que la señal encriptada va dañada por ruido y la llave también, lo que hará que la señal de información sea más sensible al ruido.

En conclusión, se recomienda que la relación señal a ruido del canal sea de más de 40dB o 45dB, para que la señal de información desencriptada no sea tan ruidosa. Si no se puede lograr lo anterior, es posible filtrar a la señal estimada en el desencriptor para mejorar la relación entre la señal de información y el ruido en el desencriptor, y así ganarle algunos dBs al ruido.

6.3 Seguridad del sistema

A modo de verificar la seguridad del sistema se analiza la relación entre la señal de información y la señal encriptada, y la relación entre la señal de información y la señal transmitida.

La Figura 6-14 muestra el espacio de fases entre la señal de información y la señal encriptada, difícilmente se puede ver una relación entre una variable y la otra, más que existe una región con pendiente unitaria negativa y otra con pendiente de negativa con valor de un décimo, las cuales se deben a las pendientes de la función g en la función de encripción. Esas dos rectas limitan el espacio sobre el cual se relacionan no linealmente la señal de información con la señal encriptada.

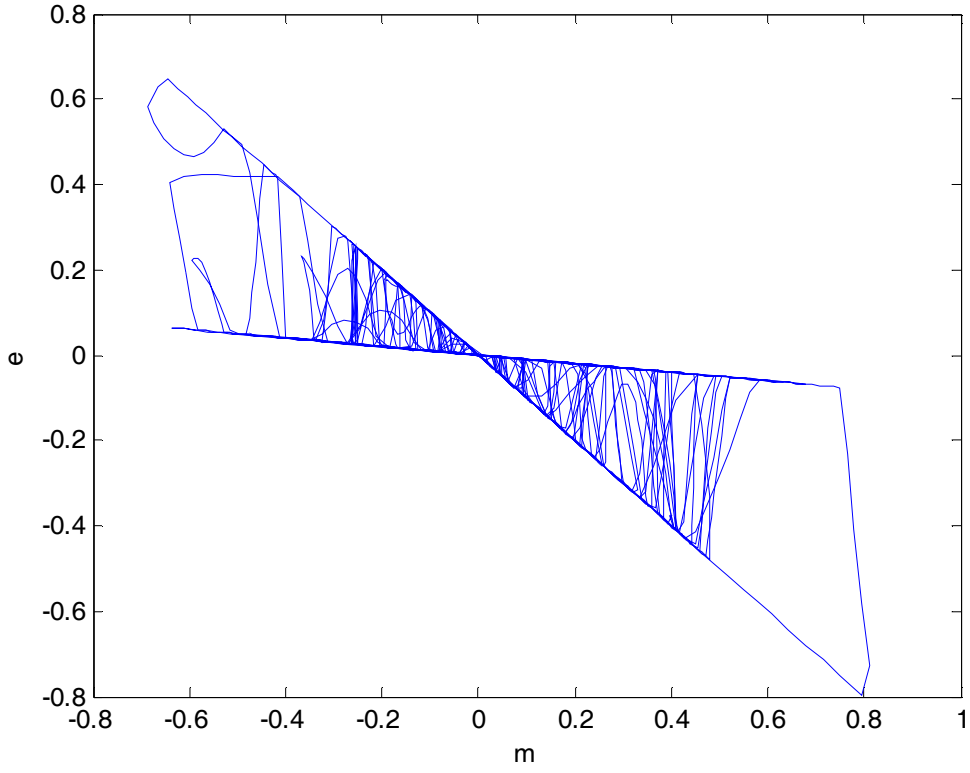

Figura 6-14 Espacio de fases entre la señal de información y la señal encriptada.

En frecuencia, la relación que hay entre la señal de información y la señal encriptada se puede ver en la Figura 6-15, donde se puede ver que la función de encripción logra un

efecto de esparcimiento en la frecuencia cuando convierte la señal de información a la señal encriptada. Este efecto hará que sea más difícil de detectar la información, ya que no sólo estará en su banda base, si no que también regada en bandas alternas.

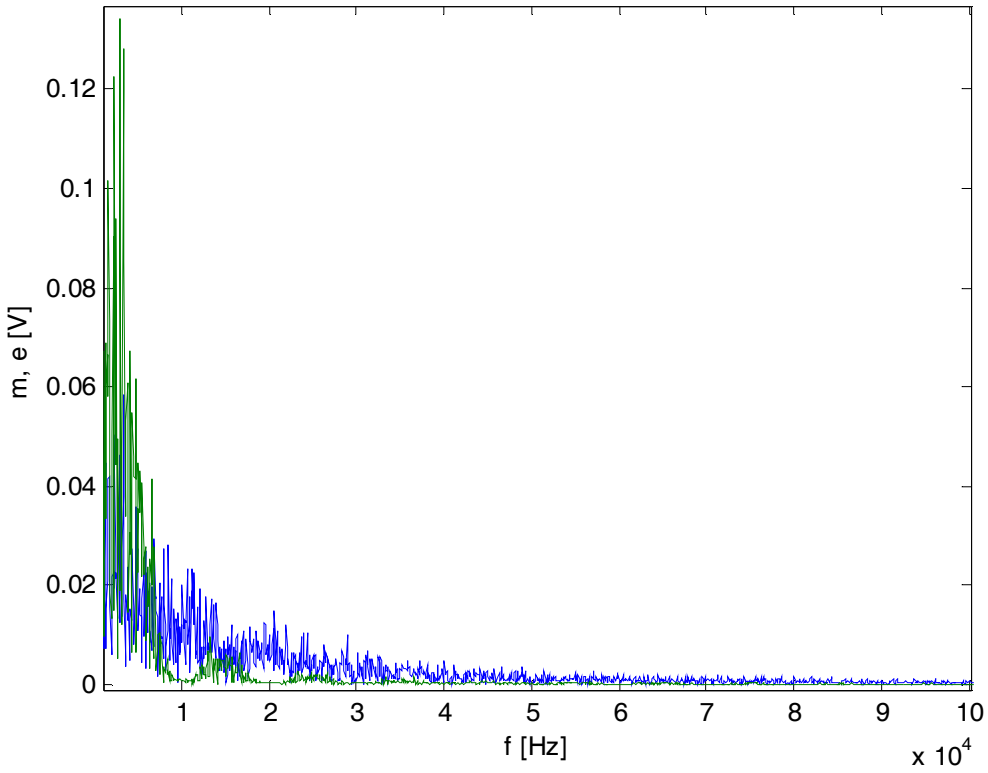

Figura 6-15 Espectro de frecuencias de la señal de información (verde), y señal encriptada (azul).

Por otro lado, la Figura 6-16 muestra el espacio de fase entre la señal de información y la señal transmitida. Para romper el sistema una persona tendría que hallar la relación que tiene cada valor en el eje de la señal transmitida con un valor en el eje de la señal de información; lo anterior parece ser muy complejo dada la relación caótica que tienen estos valores, de hecho es difícil ver una dinámica entre estas dos variables, y por lo tanto el sistema se confirma como seguro.

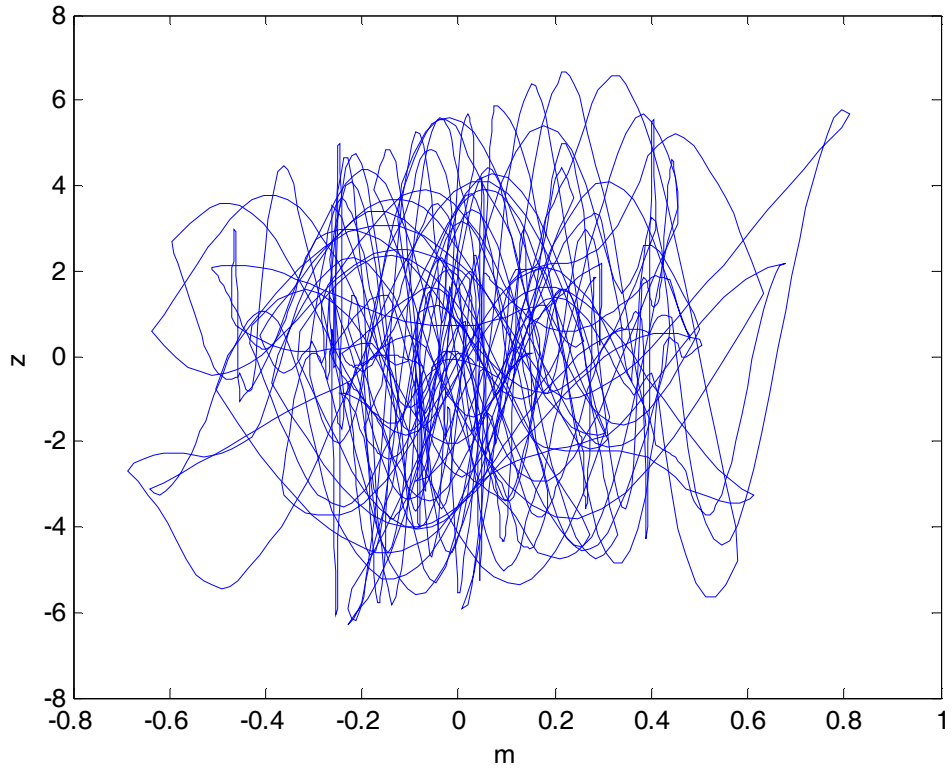

Figura 6-16 Espacio de fases entre la señal de información y la señal transmitida.

Si se analiza en frecuencia la señal transmitida con la señal encriptada se encuentra que no son parecidos. Además la señal transmitida tiene su mayor potencia en frecuencias alrededor de 8kHz, debido a que la señal de sincronía aporta mucha energía a esas frecuencias, por lo tanto, la señal de información además de estar encriptada con caos va enmascarada con caos lo que hace más seguro el sistema.

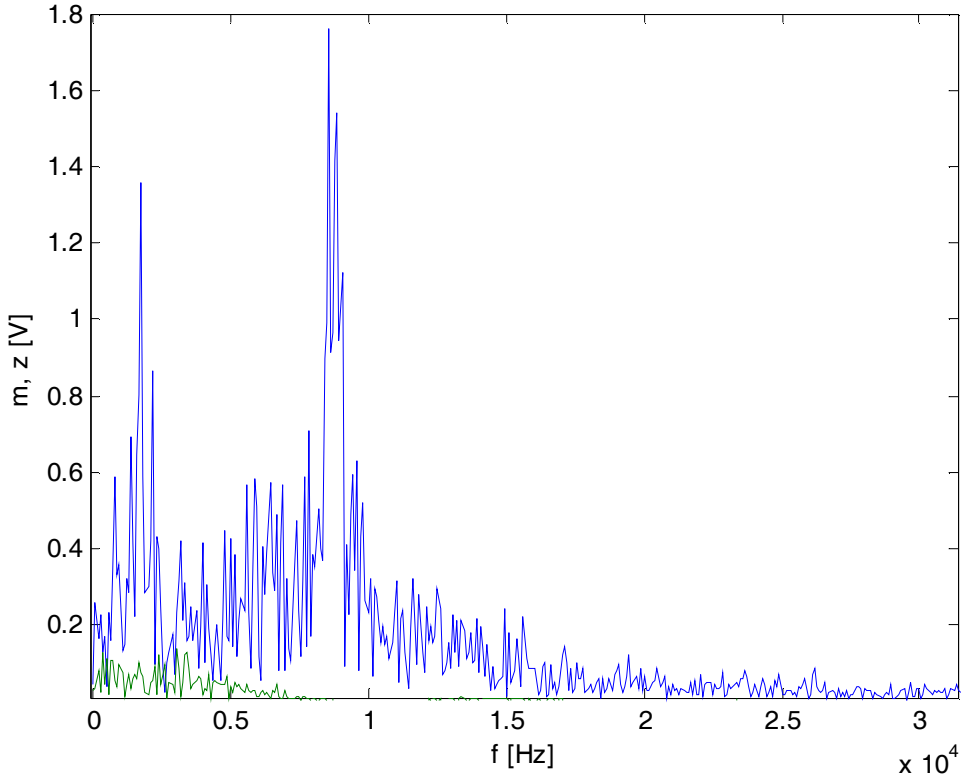

Figura 6-17 Espectro de frecuencias de la señal de información (verde), y señal transmitida (azul).

6.4 Simulación del criptocircuito caótico en PSPICE

En las secciones anteriores se han establecido las condiciones para el buen funcionamiento del sistema, además de que se han analizado las características de fidelidad y seguridad del sistema. En este apartado se presenta una simulación hecha en PSPICE, para demostrar que el funcionamiento del circuito es el esperado.

Para que el circuito funcione correctamente, cada una de sus partes lo debe hacer. En el circuito se usan 3 tipos de funciones no lineales (lineales por partes): f, g y g^{-1}. Haciendo un barrido de voltaje a la entrada del circuito de cada función se comprobó que el funcionamiento de dichos circuitos es el deseado, como se puede ver en la Figura 6-18 para la función f, en la Figura 6-19 para g, y en Figura 6-20 g^{-1}.

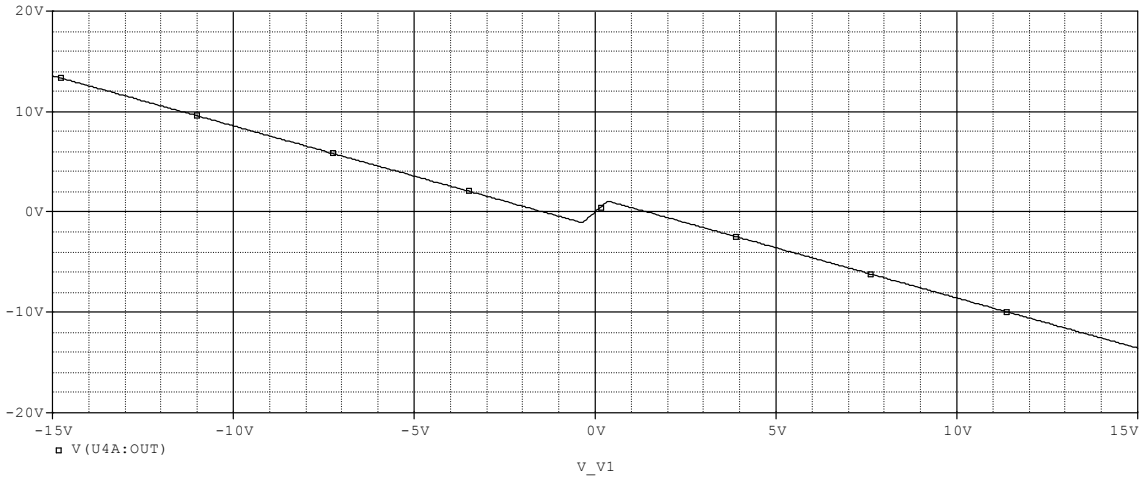

Figura 6-18 Función de transferencia para circuito de la función f.

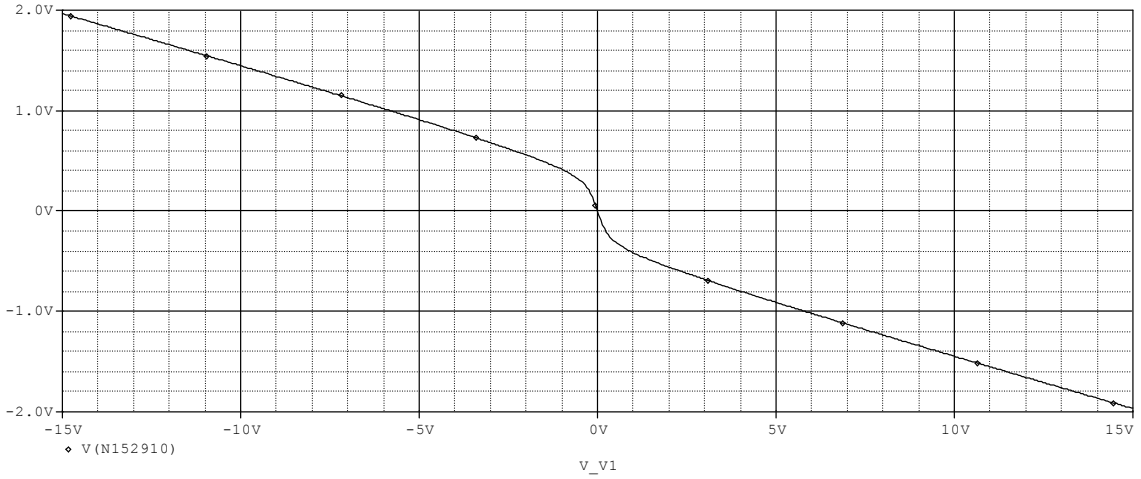

Figura 6-19 Función de transferencia para circuito de la función g.

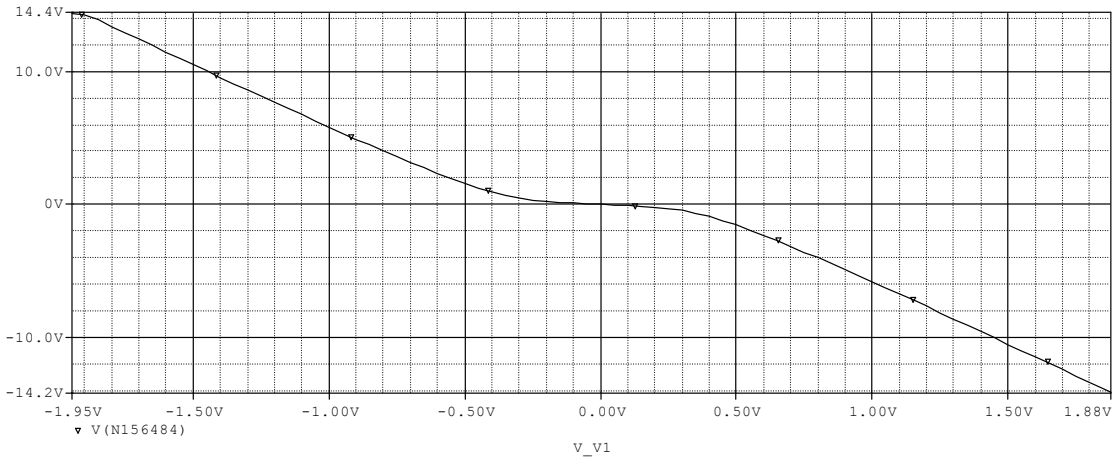

Figura 6-20 Función de transferencia para circuito de la función g^{-1}.

En las Figura 6-19 y Figura 6-20, se puede observar que la función de transferencia no es lineal por partes, esto se debe a que cuando se diseñó el circuito, por simplicidad se uso el modelo de fuente del diodo, aunque en realidad su comportamiento no lineal se ve reflejado en las figuras anteriores. Sin embargo, las funciones de transferencia siguen siendo inversas, ya que ambas usan los mismos diodos, que deben de ser muy similares en comportamiento para que exista una buena desencripción.

Se simuló sobre el circuito armado en PSPICE la transmisión de una suma de señales senoidales obteniendo los resultados esperados. En la Figura 6-21 se puede observar a la señal de información en rojo, la señal encriptada en azul, la señal transmitida en naranja y la señal desencriptada en verde. Claramente la señal desencriptada concuerda con la señal transmitida.

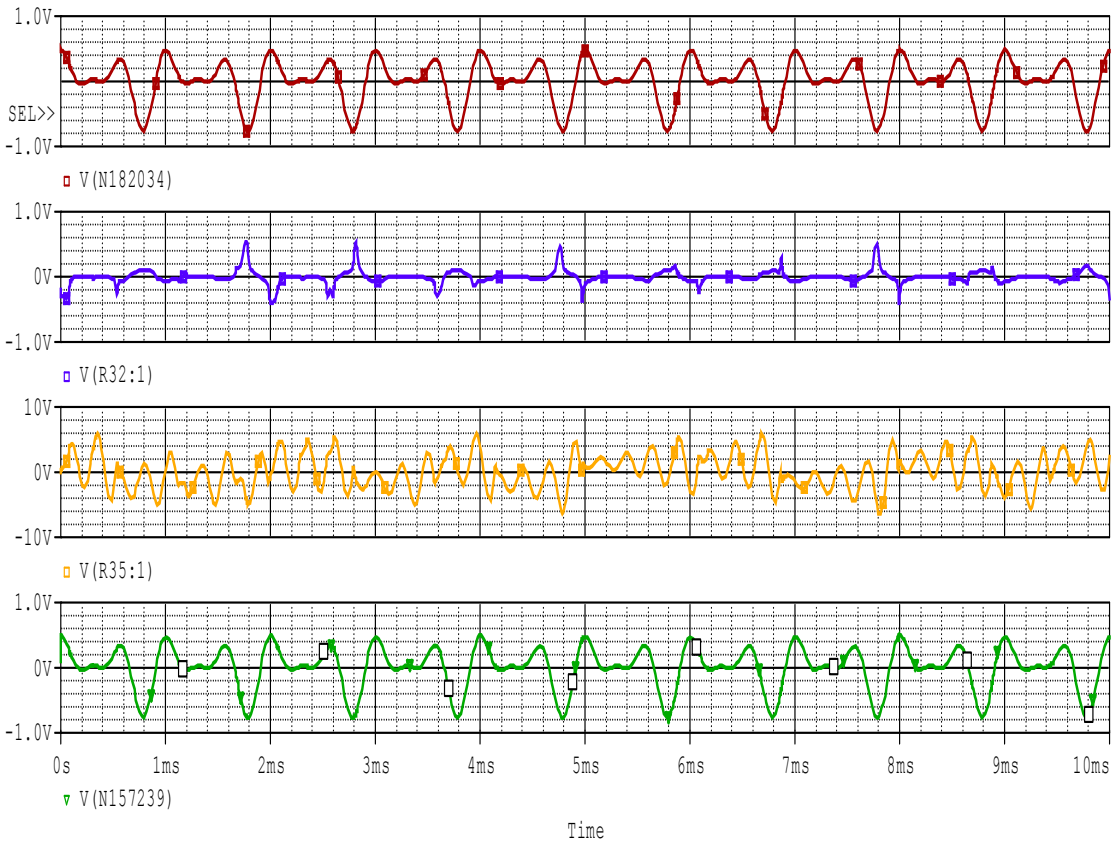

Figura 6-21 Señales: de información (rojo), encriptada (azul), transmitida (naranja) y desencriptada (verde).

La Figura 2-1 muestra el espectro en frecuencia para la transmisión simulada, se puede ver que la recuperación de la señal es correcta y que la señal transmitida no se parece en frecuencia a la señal de información. El espectro de la señal encriptada en esta ocasión no esconde la señal tan bien debido a que la señal es periódica y hace que la llave oscile con ella, en caso de ser aleatoria la función funciona de mejor forma, como se vio en las secciones anteriores.

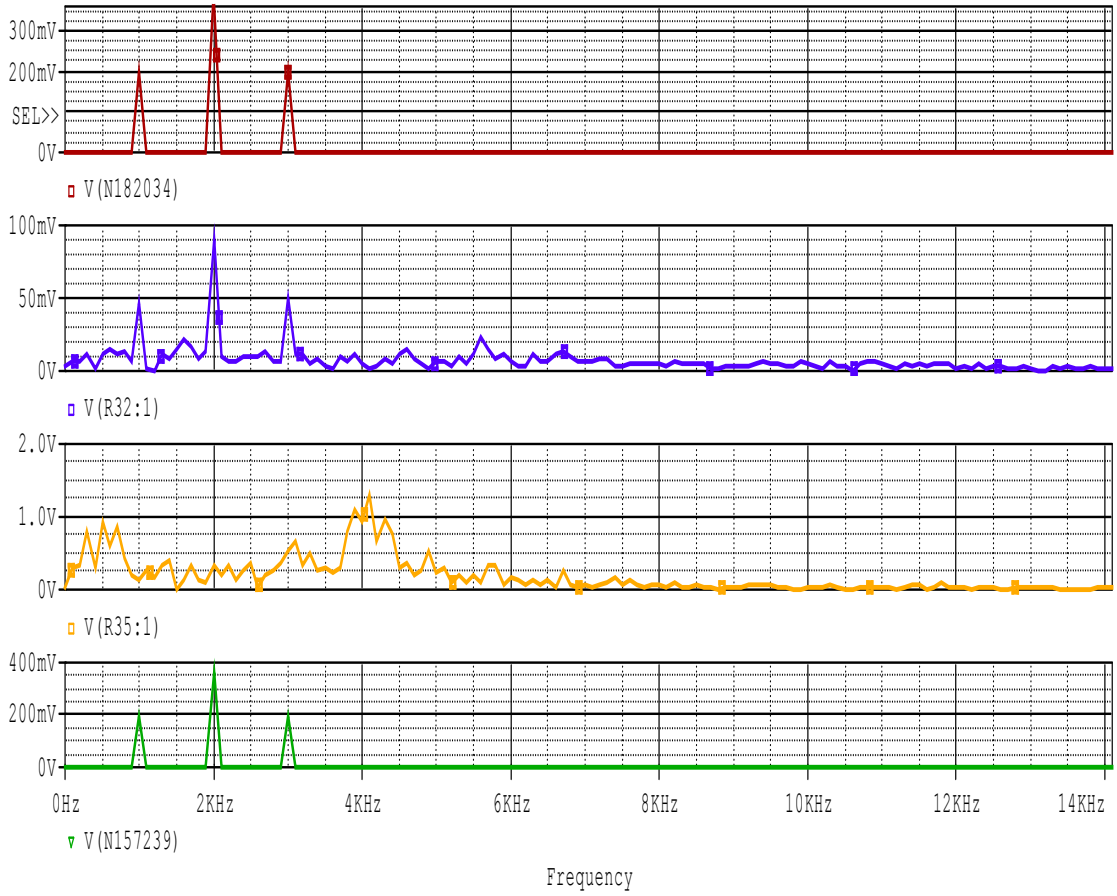

Figura 6-22 Espectro de señales: de información (rojo), encriptada (azul), transmitida (naranja) y desencriptada (verde).

En suma, el circuito funciona de acuerdo a las ecuaciones de las cuales se diseñó, y resulta difícil encontrar una relación entre la señal de información y la señal trasmitida, por lo tanto el criptosistema provee un buen nivel de seguridad.