SISTEMAS ELECTRÓNICOS DIGITALES

PRÁCTICA 6

SISTEMA DE ENCRIPTACIÓN

1. Objetivos

- Estudio del funcionamiento de memorias RAM y CAM.
- Estudio de métodos de encriptación y compresión de datos.

2. Enunciado

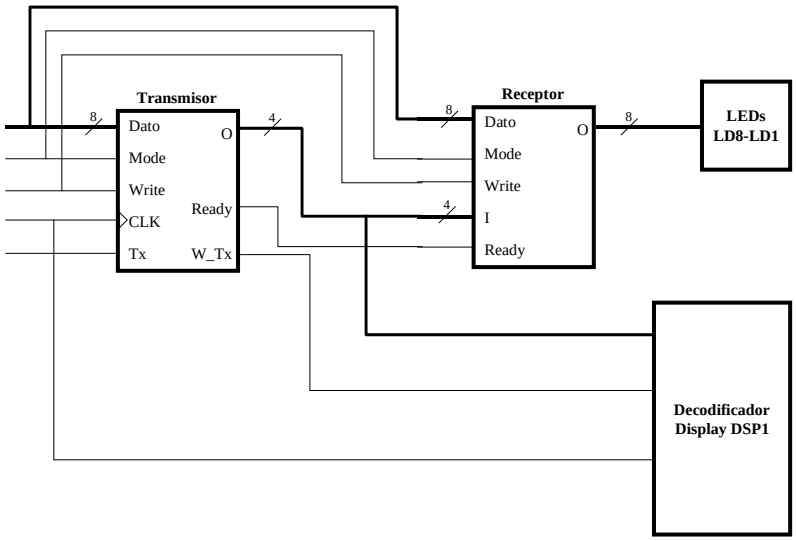
Diseñar un sistema sencillo de transmisión y recepción de datos con encriptación y compresión. Para encriptar y comprimir los datos el transmisor utilizará una memoria CAM (Content Addressable Memory) de 16 posiciones de 8 bits. El sistema deberá enviar información numérica y de operaciones sencillas, por lo que los símbolos a enviar serán los 10 números decimales, la coma de los decimales, el signo igual y los signos de las 4 operaciones básicas (sumar, restar, multiplicar y dividir). Estos símbolos se enviarán codificados en un código internacional como es el ASCII. Cuando se quiera enviar uno de estos símbolos, en la entrada del transmisor se introducirá el código ASCII correspondiente y transmitirá la dirección donde esté almacenado dicho código según la correspondiente tabla de encriptación.

TABLA ENCRIPTACIÓN

Dirección	Símbolo	Código ASCII
0	+	101011
1	-	101101
2	*	101010
3	/	101111
4	=	111101
5	,	101100
6	0	110000
7	1	110001
8	2	110010
9	3	110011
10	4	110100
11	5	110101
12	6	110110
13	7	110111
14	8	111000
15	9	111001

Por lo tanto se conseguirá una encriptación y una compresión ya que por el canal de comunicación se transmite un código de 4 bits correspondiente a la dirección de almacenamiento de la memoria CAM en vez del verdadero código ASCII de 6 bits del símbolo a enviar. El receptor tendrá que recibir el dato enviado por el canal de comunicación y realizar una desencriptación para obtener el verdadero código ASCII para el símbolo enviado. Para ello debe tener una memoria RAM con la misma tabla de encriptación que la cargada en la memoria CAM del transmisor.

El diagrama de bloques del diseño debe ser el siguiente:



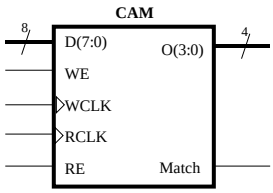
El bloque transmisor tiene 2 modos de funcionamiento: modo escritura para cargar la tabla de encriptación en la memoria CAM y modo de transmisión para transmitir el dato presente en la entrada. En el modo escritura la memoria CAM se irá direccionando de un modo ascendente y consecutivo utilizando un contador para proceder a su grabación. En modo transmisión en la salida del transmisor aparecerá el dato a transmitir que será un código de 4 bits correspondiente a la dirección donde está almacenado el código ASCII del símbolo que se quiere transmitir. Este dato será válido cuando la señal de "ready" esté a nivel alto. las señales de entrada y salida de este módulo serán las siguientes:

- Dato: Es un bus de 8 bits. Cuando el transmisor está en modo escritura la palabra de 8 bits presente en esta entrada se grabará en la correspondiente dirección de memoria de la CAM cuando se reciba un pulso de escritura (señal Write). Cuando el transmisor está en modo transmisión en esta entrada se pondrá el código ASCII del símbolo que se quiere transmitir.
- Mode: Esta entrada alterna entre los dos modos de funcionamiento del transmisor. Cada vez que se recibe un pulso en esta entrada el transmisor cambia de modo de funcionamiento.
- Write: Señal que se utiliza en modo escritura para validar el dato de entrada en la respectiva posición de memoria.
- CLK: señal de reloj principal que se utiliza como el reloj de lectura de la memoria CAM.
- Tx: Señal de desinhibición de transmisión. Cuando el transmisor está en modo transmisión y se recibe un pulso en esta entrada se procede a validar la salida del transmisor como dato válido para transmitir.
- O: Salida del transmisor. En modo escritura contiene la dirección de escritura de la memoria CAM. En modo transmisión contiene la información que se transmite por el canal de comunicación.
- Ready: Señal que valida la información a transmitir.
- W_Tx señal que indica el modo de funcionamiento en el que está el transmisor. Se puede utilizar para seleccionar los dígitos del display DSP1 que se deben activar en cada modo de funcionamiento.

Cuando el transmisor está en modo escritura se deben iluminar los 2 dígitos que están más a la izquierda del display DSP1 de la placa de periféricos y en estos dígitos se debe visualizar la dirección de escritura de la CAM. Cuando el transmisor está en modo transmisión se deben iluminar los 2 dígitos que están más a la derecha del display DSP1 de la placa de periféricos y en estos dígitos se debe visualizar el dato que se transmite por el canal de comunicación (valor decimal de los 4 bits transmitidos). Para realizar esto se debe diseñar un bloque decodificador utilizando el decodificador diseñado en la práctica anterior (práctica 5).

El transmisor se basa en una memoria CAM (Content Addressable Memory) que es un tipo de memoria que compara la entrada con el contenido grabado en la CAM y genera una salida que puede ser de varios tipos dependiendo del tipo de CAM. Para esta práctica se utilizará una CAM que compara la entrada con el

contenido grabado previamente en la memoria y devuelve como salida la dirección de la posición de memoria cuyo contenido coincide con la información presente en la entrada. Una CAM de este tipo se diseña a partir de una memoria RAM y utilizando contadores y un comparador. Para poder grabar y leer la CAM con los elementos presentes de la placa de periféricos se diseñará una CAM que tenga una señal para seleccionar el modo de funcionamiento (escritura o lectura) y la escritura se realizará utilizando un contador que va direccionando la memoria RAM de una forma ascendente. El bloque de la memoria CAM que se debe diseñar es el siguiente:



Las señales de entrada y salida deben ser las siguientes:

- D(7:0): Contenido a grabar en la correspondiente dirección de memoria cuando se está en modo escritura o dato de entrada que se tiene en cuenta para obtener la correspondiente salida cuando se está en modo lectura.
- WE: Señal de desinhibición de escritura. Cuando tiene un valor alto desinhibe la escritura de la memoria (modo escritura) y cuando tiene valor bajo se realiza la lectura de la memoria.
- WCLK: Reloj de escritura. Cuando se está en modo escritura, cada vez que se produce un flanco ascendente de esta señal se escribe en la posición de memoria direccionada por la salida de un contador de 4 bits el dato presente en D(7:0) y el contador de direccionamiento incrementa en uno su salida para direccionar la próxima posición de memoria a ser grabada.
- RCLK: Reloj de lectura. Cuando se está en modo lectura, cada vez que se produce un flanco ascendente de esta señal se incrementa en uno la salida de un contador de lectura que direcciona la siguiente posición de memoria para comparar su contenido con la entrada D(7:0) y establecer utilizando un comparador cuando el contenido y la entrada son iguales. Cuando se produce la igualdad se inhibe el contador de lectura y la dirección de la posición de memoria correspondiente se presenta en la salida de la CAM y se valida mediante una señal “match” que se pone a nivel alto.
- RE: Señal de desinhibición de la lectura. Se pone a nivel alto cuando la entrada de la lectura está lista. El flanco ascendente de esta señal carga el contenido de la entrada en una de las entradas del comparador. En la otra entrada del comparador se introduce el contenido de las posiciones de la memoria que se van leyendo secuencialmente a través del contador de lectura.
- O(3:0): Dirección de lectura de la memoria. Cuando el contenido de la posición de memoria direccionada coincide con el dato de entrada esta dirección se valida a la salida de la CAM mediante la señal “match”.
- Match: Emparejamiento. Señal de salida que se pone a nivel alto cuando en el modo de lectura se produce una igualdad entre el dato de entrada y el contenido de una posición de memoria. Esta señal a nivel alto valida el dato de salida de la memoria.

El bloque receptor se basa en una RAM donde debe cargarse la tabla de encriptación. Este bloque tiene dos modos de funcionamiento: modo escritura para cargar la tabla de encriptación en la memoria RAM y modo de recepción donde se recibe el dato enviado por el transmisor Cuando la señal “ready” se pone a nivel alto el dato presente en la entrada “I” se desencripta y a la salida ofrece el código ASCII del símbolo que envió el transmisor. Las señales de salida y entrada de este bloque deben ser las siguientes:

- Dato: Es un bus de 8 bits. Cuando el receptor está en modo escritura la palabra de 8 bits presente en esta entrada se grabará en la correspondiente dirección de memoria de la RAM cuando se reciba un pulso de escritura (señal Write). Cuando el receptor está en modo recepción esta entrada no se utiliza.
- Mode: Esta entrada alterna entre los dos modos de funcionamiento del receptor. Cada vez que se recibe un pulso en esta entrada el receptor cambia de modo de funcionamiento.
- Write: Señal que se utiliza en modo escritura para validar el dato de entrada en la respectiva posición de memoria.

- I: Entrada del receptor. El dato presente en esta entrada se considera que es la información enviada por el transmisor cuando la señal "ready" se pone a nivel alto. Este dato debe ser desencriptado para obtener el verdadero código ASCII del símbolo enviado por el transmisor.
- Ready: Señal que valida el dato a recibir.
- O: Salida del receptor. Es el código ASCII del símbolo enviado por el transmisor.

La salida del receptor se debe visualizar en los leds presentes en la placa de periféricos (LD8-LD1).

En el diseño se deben especificar que pines de la FPGA tienen que corresponder a las señales de entrada y salida del diseño para utilizar los siguientes elementos de la placa de periféricos:

- Señal de reloj:

  CLK: se utilizará como señal de reloj el oscilador de 50 MHz que contiene la placa de desarrollo y que está conectado a la entrada GLK2 de la Spartan 2E (pin 182).
- Señales de entrada

  D(7:0): 8 bits de datos. Cuando el receptor y el transmisor están en modo escritura se utilizarán estos bits para introducir el dato a almacenar en cada posición de memoria según la correspondiente tabla de encriptación. Cuando el transmisor está en modo transmisión se utilizarán para introducir el código ASCII del símbolo que se quiere enviar. Se introducirán utilizando los interruptores 8, 7, 6, 5, 4, 3, 2 y 1 (SW8, SW7, SW6, SW5, SW4, SW3, SW2, SW1) de la placa de periféricos. SW8 se corresponderá al bit de mayor peso (D7) y SW1 al de menor peso (D0).

  Mode: Señal que selecciona el modo de funcionamiento del receptor y el transmisor. Se generará utilizando el botón 5 (BTN5) de la placa de periféricos.

  Write: Señal que valida los datos a escribir en las respectivas memorias del transmisor y receptor. Se generará utilizando el botón 4 (BTN4) de la placa de periféricos.

  Tx: Señal que inicia la transmisión de un símbolo. Se generará utilizando el botón 1 (BTN1) de la placa de periféricos.
- Señales de salida:

  a, b, c, d, e, f, g, AN1, AN2, AN3, AN4: señales de control del display de la placa de periféricos. Se deben generar a partir de la salida del transmisor y del modo de funcionamiento del transmisor y asignarles los pines correspondientes de los conectores de expansión de la placa de periféricos.

  O(7:0): 8 bits de salida del receptor. Contienen la información enviada por el transmisor. Deben iluminar los 8 LEDS de la placa de periféricos. LD8 se corresponderá al bit de mayor peso (O7) y LD1 al de menor peso (O0).

3. Tareas del alumno previas a la asistencia al laboratorio

El alumno deberá de realizar las siguientes tareas antes de asistir al laboratorio:

- Lectura de la documentación sobre el software ISE 6.3
- Lectura de la documentación de la placa de desarrollo Digilent D2-SB
- Lectura de la documentación de la placa de periféricos DIO4
- Lectura de la práctica
- Estudio de la relación entre pines de la FPGA y pines de los conectores de expansión de la placa de desarrollo.
- Estudio de la relación entre los elementos de la placa de periféricos y los pines de los conectores de expansión de dicha placa.
- Estudio de la relación entre pines de los conectores de expansión de la placa de desarrollo y la placa de periféricos.
- Diseñar una memoria CAM de 16 posiciones de 8 bits a partir de una RAM de 16 posiciones y 8 bits y utilizando contadores para el direccionamiento en el modo escritura y lectura, un comparador para establecer que posición de memoria coincide con la entrada y los elementos lógicos que sean necesarios para conseguir un funcionamiento de la CAM como el propuesto en el enunciado.

- Diseñar un bloque transmisor basado en la memoria CAM anterior que cumpla las especificaciones del enunciado.
- Diseñar un bloque receptor basado en una memoria RAM que cumpla las especificaciones del enunciado.
- Diseñar el acoplamiento entre el bloque transmisor y el receptor.
- Añadir los circuitos y conexiones necesarias para utilizar los elementos de la placa de periféricos para introducir las entradas del sistema y visualizar las salidas según se indica en las especificaciones del enunciado.
- Asignar los pines adecuados de la FPGA a las señales de entrada y salida del diseño para utilizar los elementos correspondientes de la placa de periféricos según las especificaciones del enunciado.

4. Tareas a realizar en el laboratorio

El alumno deberá introducir en el software ISE 6.3 el esquemático del sistema de transmisión y recepción de datos encriptados y simular su correcto funcionamiento introduciendo la secuencia de señales adecuada. Una vez simulado el funcionamiento del sistema, se realizará físicamente programando la FPGA Spartan 2E de la placa de desarrollo. Se realizará la asignación de pines a las señales de entrada y salida adecuada para cumplir con las especificaciones de la práctica y para utilizar los elementos de la placa de periféricos propuestos. En su realización física utilizando una FPGA, se utilizará el botón 5 (BTN5) de la placa de periféricos para cambiar de modo de funcionamiento (escritura y transmisión/recepción). Cuando el sistema está en modo escritura se utilizará el botón 4 (BTN4) para validar el dato de entrada en la posición de memoria que se está visualizando en los 2 dígitos situados más a la izquierda del display DSP1. Cuando el sistema está en modo transmisión/recepción se utilizará el botón 1 (BTN1) para indicar cuando el dato a transmitir está listo en la entrada del transmisor y así iniciar la transmisión. El dato que se envía por el canal de comunicación se visualizará en los 2 dígitos que están más a la derecha del display DSP1. La salida del receptor se visualizará en los leds LD8-LD1. El contenido de las posiciones de la memoria en el modo escritura y el dato a enviar en el modo transmisión/recepción se introducirán utilizando los interruptores SW8-SW1.

Los pasos a seguir por el alumno en el laboratorio serán los siguientes:

- Crear un proyecto con un esquemático de la memoria CAM utilizando una memoria RAM16x8S y generar el símbolo correspondiente.
- Añadir el esquemático del bloque transmisor utilizando la CAM creada anteriormente y generar el símbolo correspondiente.
- Añadir el esquemático del bloque receptor utilizando una RAM16x8S y generar el símbolo correspondiente.
- Añadir el esquemático del sistema global conectando el transmisor con el receptor.
- Introducir las formas de onda adecuadas para las señales de entrada (Test Bench Waveform) para cada uno de los bloques anteriores.
- Simular el comportamiento cada uno de los bloques anteriores y del sistema global.
- Diseñar un bloque decodificador para poder representar los datos que se especifican en el enunciado en el display de la placa de periféricos. Utilizar el decodificador de 4 bits a 2 dígitos diseñado en la práctica 5.
- Adaptar el esquemático realizado anteriormente incluyendo el bloque decodificador diseñado para utilizar los elementos de la placa de periféricos indicados en el enunciado.
- Establecer los pines de la FPGA a utilizar por las entradas y salidas del diseño.
- Programar la FPGA.
- Comprobar el correcto funcionamiento del sistema utilizando los elementos de la placa de periféricos descritos en el enunciado. Para ello, primero se debe poner el sistema en modo escritura y realizar un ciclo completo de escritura introduciendo la correspondiente tabla de encriptación. A continuación se pasará al modo transmisión/recepción y se comprobará el correcto funcionamiento del sistema introduciendo con los interruptores los códigos ASCII de diferentes símbolos y comprobando que el dato enviado por el canal de comunicación es un código distinto al ASCII y que en la salida del receptor vuelve representarse el código ASCII correspondiente al símbolo enviado.