

Análisis y Diseño Parcial 1

Sistema de encriptación

Maria Fernanda Tasco ALquichire

Departamento de Ingeniería Electrónica y
Telecomunicaciones
Universidad de Antioquia
Medellín
Febrero de 2022

Índice

1. Objetivos	2
1.1. generales	2
1.2. Especificos	2
2. Sección introductoria	2
2.1. Resumen	2
2.2. Introducción	2
3. Marco Teorico	2
3.1. Terminología / preguntas en la investigación	2
3.2. Investgación soluciuones propuestas	4
4. Marco Expremiental	5
5. Resultados	6
6. Conclusiones	6

1. Objetivos

1.1. generales

resumen - abstrac

1.2. Especificos

introducion

2. Sección introductoria

2.1. Resumen

resumen - abstrac

2.2. Introducción

introducion

3. Marco Teorico

Esta sección es para agregar toda la información correspondiente con código, citas, etc.

3.1. Terminología / preguntas en la investigación

¿Qué es, para qué sirve y cómo se usa la señal de reloj?

Una **Señal de Reloj** [1] es una señal usada para coordinar las acciones de 2 o más circuitos o sistemas. Oscila entre estado alto y bajo en forma de señal cuadrada.

En este caso se usará un primer reloj para sincronizar los datos que estarán en la primera parte de registro de desplazamiento, es decir autorizar la entrada en serie de cada bit. Un segundo reloj para sincronizar el registro de almacenamiento que autoriza el paso de los datos que van a estar en la salida (estos relojes están implementados dentro de CI 74HC595). Una breve representación la podemos ver en la figura 1 y 2.

¿74HC595?

El circuito integrado 74HC595 es un **registro de desplazamiento** [3] que cuenta con entrada en serie y salida en paralelo de 8 bits. Lo que quiere decir es que en este **tipo de registros** [4] con salida en paralelo se dispone de la salida de cada **flip-flop o biestable** [5] que nos servirá para memorizar la información a la que antes se hacía referencia por lo que una vez almacenados los datos cada

Figura 1: 74HC595 con los mismo bits en el **registro** [2] de desplazamiento y almacenamiento

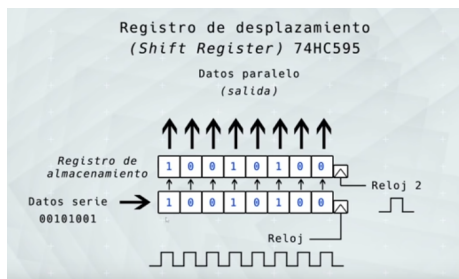
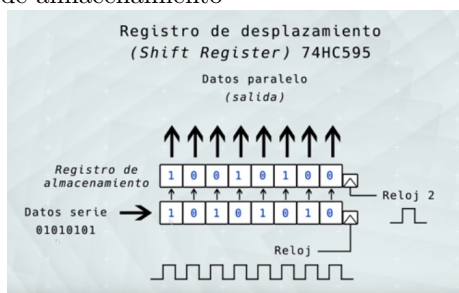


Figura 2: 74HC595 con un nuevo byte en el **registro** [2] de desplazamiento y el byte anterior en el de almacenamiento



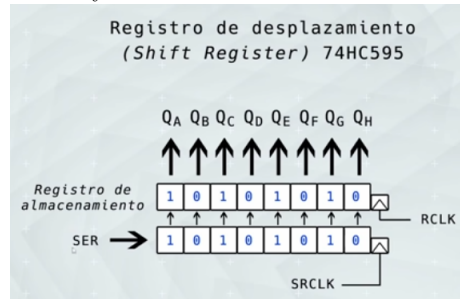
bits se representa en su respectiva salida.

La utilidad que puede darle este elemento a la solución del problema es que con el **desplazamiento** [6] de datos y dependiendo del sistema de descryptación, yo voy a tener en la salida que es paralela el bit que voy a comparar dado el caso, mientras que se van ingresando otros bits, y hacer esto de manera sincronica ya que con la ayuda de los relojs ayuda a que las salidas no se vea afectada con la entrada, así finalmente ganando eficiencia y agilidad.

Otra utilidad [2] que tiene este CI en especial es el RCLK (Registro de reloj/Latch) Cuando este en BAJO (LOW), el contenido del registro de desplazamiento (los 8 bits) se copia en el registro de almacenamiento; que finalmente se muestra en la salida. Eso permite que mientras se realiza este proceso se puedan ir ingresando datos en serie usando el SRCLR (Shift Register Clear) que reinicia todo el registro de desplazamiento, haciendo que todos sus bits sean 0, cuando este esta en LOW y así dando paso a que el SRCLK (Shift Register Clock) que registra el cambio y desplaza los bits en el registro de desplazamiento, cuando este esta en HIGH. Una pequeña representación en la figura 3.

Se puede ver la implementación de este CI con pulsadores / switches y con arduino en la sección de marco experimental.

Figura 3: 74HC595 con el **registro** [2] de desplazamiento y almacenamiento con los pines más importantes y los de salida



¿Qué variable usar para un arreglo de números enteros de 1byte?

Inicialmente en el programa de Qt se hará uso de la variable `unsigned char` (es una variable que almacena 8bits sin signo, desde 0-255) que aunque no pueda imprimir caracteres que no son imprimibles, solo se usará para que al leer el archivo de texto encriptado guarde la información allí. En arduino se hará el uso del tipo de variable `byte` (es una variable que almacena 8bits sin signo, desde 0-255). Así las dos variables tienen el mismo tamaño lo cuál ayuda a que en el paso de información no haya algún problema.

¿Cómo se pueden conectar dos arduinos,y con qué fin?

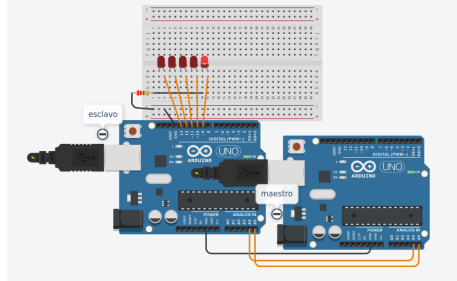
Se usan los conceptos de maestro y esclavo. El arduino esclavo en este caso será el que cumplirá la función de sistema de recepción y el arduino maestro es el que obtendrá los datos iniciales que serán procesados para obtener el mensaje real que se le pasará al arduino esclavo para que al final lo muestre por medio de una pantalla lcd.

El objetivo de esta parte es **cómo enviar bits** [7] desde uno y ser recibidos por el otro de forma exitosa. Para empezar sus tierras/GND deben ser la misma para tener el mismo potencial electrico y no hayan complicaciones luego. Se usa la libreria `Wire.h` ya que tiene funciones para la comunicación. Esto se puede en la figura 6.

3.2. Investigación soluciones propuestas

aun no he investigado nada

Figura 4: Conexión entre **arduinos** [7] usando la libreria Wire.h

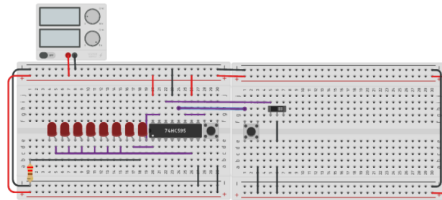


4. Marco Expremiental

74HC595 Ejemplo de uso con pulsadores / switches

Para esta primera implementación de ejemplo se probará el 74HC595 con un **pulsador** [8] que registra los desplazamientos, otro que registra la salida y el interruptor deslizante como entrada (HIGH-LOW). Se puede ver en la figura 4.

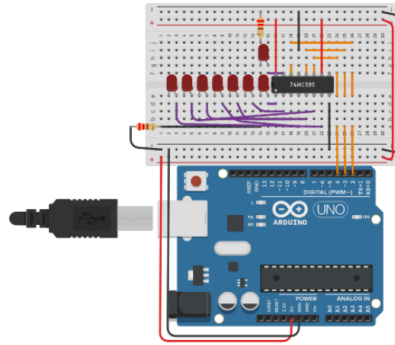
Figura 5: Uso 74HC595 con pulsadores en **tinkercad** [9]



Por último se implementó el CI con arduino, en este caso colocando los 3 pines principales (SER: a donde enviar los datos serie, SRCLK: reloj del registro de desplazamiento, RCLK: reloj del registro de almacenamiento) en los pines digitales de arduino, también se hizo uso de la función `shiftOut()`; de **arduino** [10] la cual es la función estrella en el registro de desplazamiento ya que recibe 4 parametros (SER,SRCLK,LSBFIRST/MSBFIRST,i) el tercera parametro es para definir el orden de la entrada si desde el primer bit o el segundo, en este caso para que al ingresar y desplazar los bits y al final me quede el byte que se ingreso por medio de la variable i se usará el LSBFIRST. Se puede ver en la figura 5.

con esto se concluye que el uso del primer reloj en este CI nos ayuda a sincronizar los datos que van entrando en Serie al 74HC595 y gracias al segundo reloj que tiene implementado este CI nos ayuda a hacer el registro de almacenamiento con un único pulso, permitiendo almacenar los datos que van a la salida mientras que se van ingresando otros datos en el registro de desplazamiento; esto asegura que la salida no se vea afectada mientras que se hace la carga.

Figura 6: Uso 74HC595 con arduino en **tinkercad** [11]



5. Resultados

Una clave para el desarrollo del algoritmo fue el orden de los pasos, ya que un orden adecuado, omitir algunos pasos o no generar las condiciones necesarias para el buen desarrollo de la solución, podría generar alguna ambigüedad o error.

6. Conclusiones

Una clave para el desarrollo del algoritmo fue el orden de los pasos, ya que un orden adecuado, omitir algunos pasos o no generar las condiciones necesarias para el buen desarrollo de la solución, podría generar alguna ambigüedad o error.

(1),(), (), (), () y ()

Referencias

- [1] ALEGSA. Definición de señal de reloj. [Online]. Available: [https://www.alegsa.com.ar/Dic/señal de reloj.php](https://www.alegsa.com.ar/Dic/señal%20de%20reloj.php)
- [2] B. Ar. Arduino desde cero en español - capítulo 70 - 74hc595 registro de desplazamiento (shift register). [Online]. Available: <https://www.youtube.com/watch?v=LFqIA3ZvZE8>
- [3] U. Electronics. 74hc595 registro de desplazamiento sn74hc595n. [Online]. Available: <https://uelectronics.com/producto/74hc595-registro-de-desplazamiento-sn74hc595n/>
- [4] personales unican. Regg4. [Online]. Available: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad>

- [5] E. contributors. Biestable. [Online]. Available: <https://www.ecured.cu/index.php?title=Biestable&oldid=2509697>
- [6] D. Arduino. Cómo funciona el registro de turnos 74hc595 y su interfaz con arduino. [Online]. Available: <https://descubrearduino.com/74hc595/>
- [7] M. F. T. Alquichire. Conexión entre arduinos parcial1 info2 2022-2. [Online]. Available: <https://www.tinkercad.com/things/fTjcYnZNOFS>
- [8] ElectroTodos. ¿qué es un shift register? ¿cómo funciona? [Online]. Available: <https://www.youtube.com/watch?v=sXEfsXg-O9w>
- [9] M. F. T. Alquichire. Ejemplo 74hc595 con pulsadores. [Online]. Available: <https://www.tinkercad.com/things/jlg16Gdkl6L>
- [10] T. A. Reference. shiftout(). [Online]. Available: <https://www.arduino.cc/reference/en/language/functions/advanced-io/shiftout/>
- [11] M. F. T. Alquichire. Ejem_{74hc595_a}arduino.[Online].Available : [https : //www.tinkercad.com/things/kNF6ghNkPcH](https://www.tinkercad.com/things/kNF6ghNkPcH)