

加密解密装置设计文档

董恒

PB16111545

开发平台

1. EDA 平台：ISE Design Suite 14.7
2. 仿真平台：Isim 14.7
3. 开发板型号：Xilinx Nexys2
4. FPGA 型号：nexys2 Spartan3E XC3S500E FG320

外设

1. PS/2 接口键盘
2. LCD 1602 显示器
3. 扬声器
4. LED、数码管、拨动开关、按钮

整体概述及功能说明

主体功能是一个基于键盘输入、lcd 显示的加密解密装置，在该装置中增加了一些附加功能以使整个设计趋于完善。

下面简要叙述功能，详细的设计内容在下文

1. 开机音乐
 - a) 设计目的：缓解调试时的尴尬气氛
 - b) 乐曲：柯南《如果有你》
2. 加密解密
 - a) 类似恩尼格码的加密解密方式
 - b) 设置一个拨动开关，拨向一方表示加密，拨向另一方表示解密
 - c) 一个字符(0-9 A-Z)对应一个字符，但是同一字符在不同位置对应不同密文
 - d) 5 位密钥，由于密码本身不难破解，因而没有必要设置过长的密码
3. 输入
 - a) PS/2 接口的键盘输入字符
 - b) 拨动开关输入密钥、加密解密选择
 - c) 按钮复位
4. 输出
 - a) LCD 流动显示历史记录
 - i. 第一行表示输入的文字
 - ii. 第二行表示加密或者解密后的文字
 - iii. 从右边开始，随着字符的输入逐渐左移
 - b) 数码管显示当前输入输出，左边输入，右边输出

- c) Led 闪烁显示密文的摩斯电码
 - i. 常亮表示 dah
 - ii. 闪烁表示 di

具体实现

1. 开机音乐

a) 原理

- i. 简化处理，音乐涉及到的东西是频率和音长
- ii. 频率通过预置数来实现，分成 21 个音（除去休止符），低音、中音、高音各 7 个，从而设置 21 个预置数
- iii. 根据简谱再使用脚本写出相应的程序

b) 具体实现

- i. 简谱如下

1= $\text{b}\Delta \frac{4}{4}$ 名侦探柯南 キミがいれば 如果有你
♩=135
($\text{---}\frac{7}{4}\text{---}$)

0 0 0 17 | 6 3 - 16 | 7 4 3 2 | 12 12 3 17 |
6 2 17 067 | 1 6 3 1 | 2 6 5 432 | 3 - - - | 3 - 0 17 |
6 3 - 16 | 7 4 3 2 | 12 12 3 17 | 6 2 17 067 | 1 6 3 1 |
2 6 5 432 | 3 - - - | 3 - 0 33 | i 6 · #5 6i | 7 6 5 5 - |
6 1 2 1 23 | 3 - 01 23 | 4 32 2 - | 6 54 5 6 7 | 7 - - - |
7 - 0 17 | 6 3 - 16 | 7 4 3 2 | 12 12 33 45 | 6 i 7#5 6 |
6 - - - | 6 - 01 23 | 3 - 04 56 | 67 1 2 7 | 0 0 06 71 |
1 - 01 23 | 3 - 02 345 | 5 43 3 (17 | 间奏15 | 0 0 0) 33 |
i 6 · #5 6i | 7 6 5 5 - | 6 1 2 1 23 | 3 - 01 23 | 4 32 2 - |
6 54 5 6 7 | 7 - - - | 7 - 0 17 | 6 3 - 16 | 7 4 3 2 |
12 12 33 45 | 6 i 7#5 6 | 6 - - - | 6 - - - | 6 - - - |
5 · 4 43 23 | 3 - - - | 3 - 04 56 | 6 - - - | 0 0 0 0 |
0 0 0 0 5#5 | 63 42 37 16 ||

本乐曲收录自搜谱网，由书明谱库缓存(www.spuku.com)。

- ii. 人工生成 note=[...]列表，具体内容见附录
- iii. 演示视频以及音频（百度网盘） <https://pan.baidu.com/s/1hsMVXUO>





































2. 加密解密

- a) 恩尼格玛密码机小知识 http://blog.sina.com.cn/s/blog_4033131f010007wr.html

b) 说明：

- i. 本装置是对该编码方式的简化，仅仅设置了 5 位二进制的密钥用于生成初始状态以及相应的下一编码状态的转换
- ii. 由于输出显示的限制，仅仅将字符限制在数字和字母（不区分大小写）

- iii. 加密与解密是对称的，因而将 7 号拨动开关调整到另一个方向，就表示相反方向的编码
- 3. 输入
 - a) PS/2 键盘输入字符
 - i. 现常用的键盘一般是 USB 接口，而板子上用于键盘和鼠标的接口是 PS/2 类型，因而需要另购转接口或者自带该接口的键盘
 - b) 拨动开关输入密钥、编码状态、关闭音乐
 - c) 按钮复位
- 4. 输出
 - a) LCD 显示历史记录
 - i. 使用标准的 LCD1602，其工作方式类似数码管扫描
 - ii. 杜邦线直接插入，可能会出现接触不良的情况
 - iii. 需要一个电位器与 V 0 相接再接地
 - iv. VSS、VDD 的电压需要增大
 - b) 数码管显示实时记录
 - i. 显示数字和字母
 - ii. 对应的关系如下

数码管显示英文字母							
显示	含义	显示	含义	显示	含义	显示	含义
	0		9		I		R
	1		A		J		S
	2		B		K		T
	3		C		L		U
	4		D		M		V
	5		E		N		W
	6		F		O		X
	7		G		P		Y
	8		H		Q		Z

- iii.
- c) led 显示摩斯电码
 - iv. 摩斯电码的设计属于未完成设计（原本设计是实现无线电密文通讯，未完成）
 - v. 对应关系如下

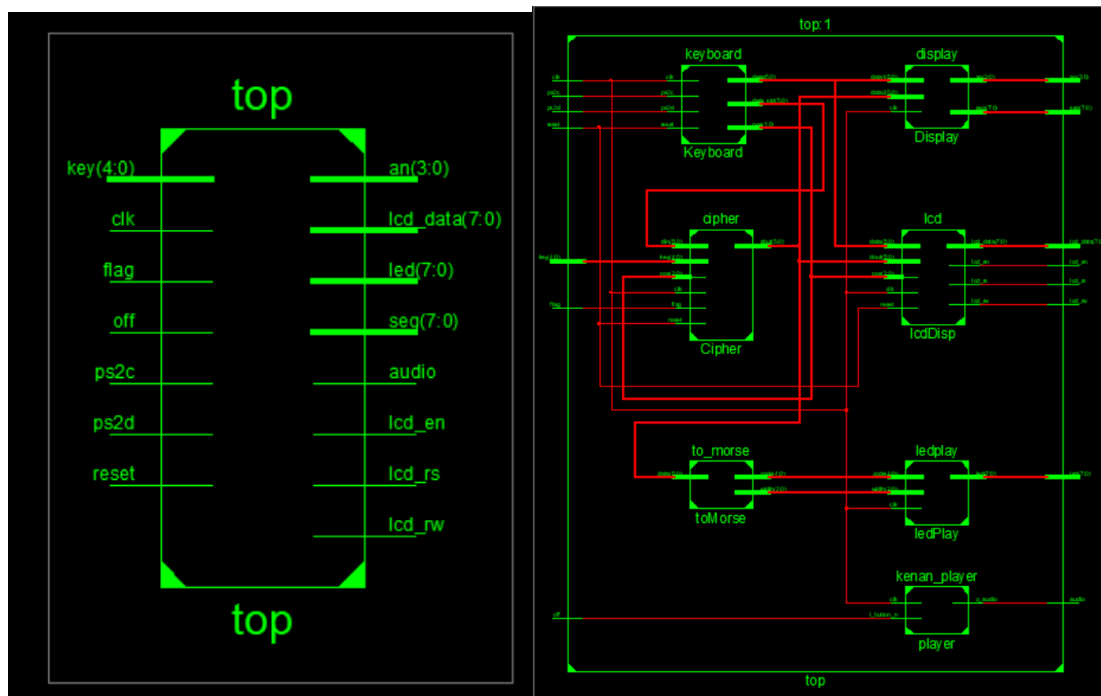
一、26个字母的摩斯密码表

字符	电码符号	字符	电码符号	字符	电码符号	字符	电码符号
A	. -	B	- . . .	C	- . - .	D	- . .
E	.	F	. . - .	G	- - .	H
I	. .	J	. - - -	K	- . -	L	. - . .
M	- -	N	- .	O	- - -	P	. - - .
Q	- - . -	R	. - .	S	. . .	T	-
U	. . -	V	. . . -	W	. - -	X	- . . -
Y	- . - -	Z	- - . .				

二、数字的摩斯密码表

字符	电码符号	字符	电码符号	字符	电码符号	字符	电码符号
0	- - - - -	1	. - - - -	2	. . - - -	3	. . . - -
4 -	5	6	-	7	- - . . .
8	- - - . .	9	- - - - .				

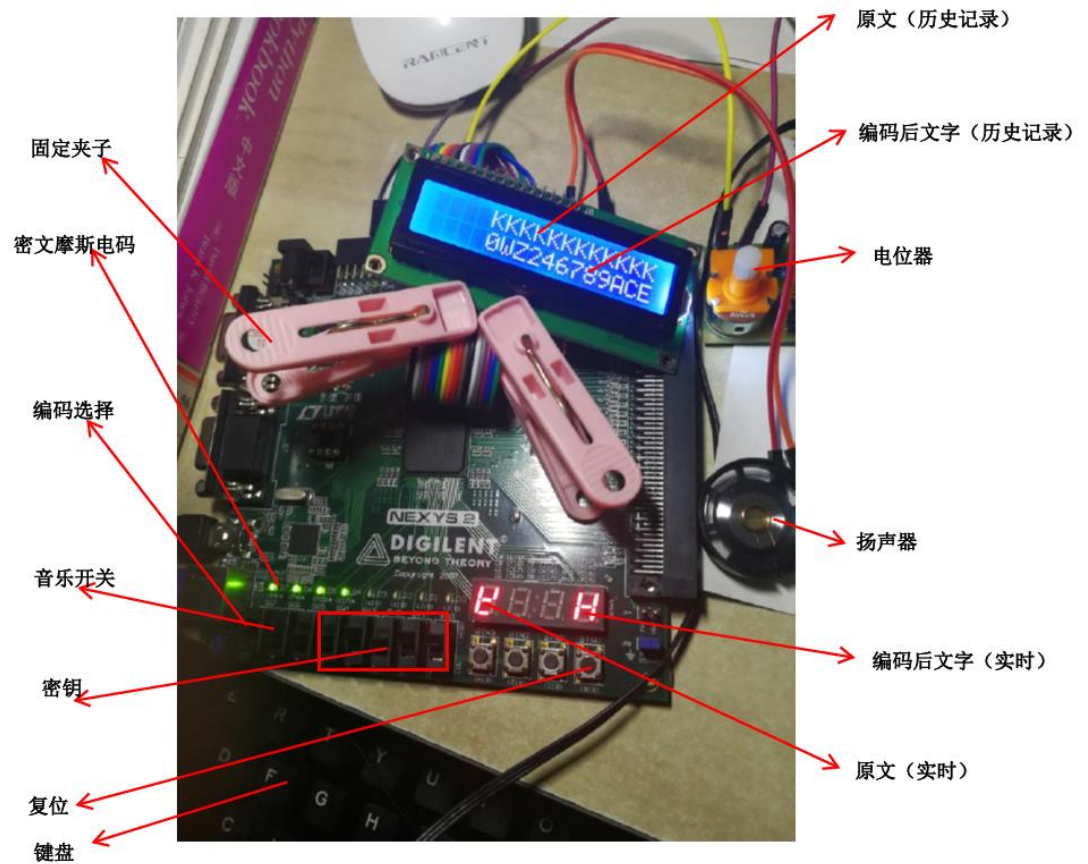
模块关系



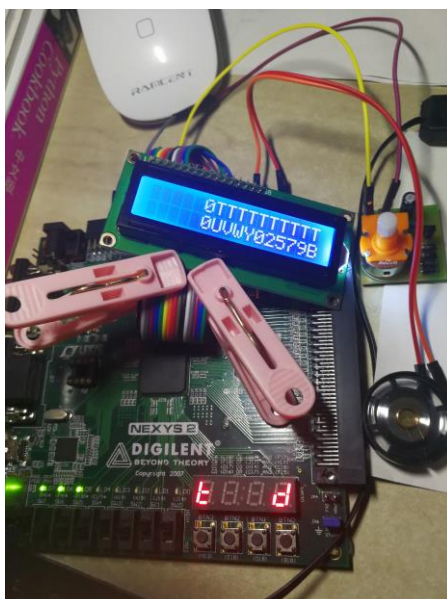
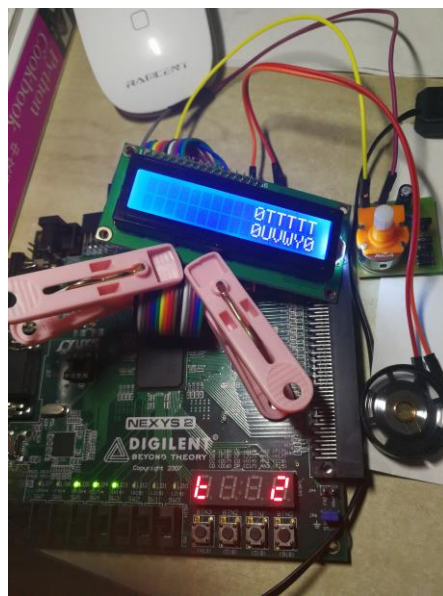
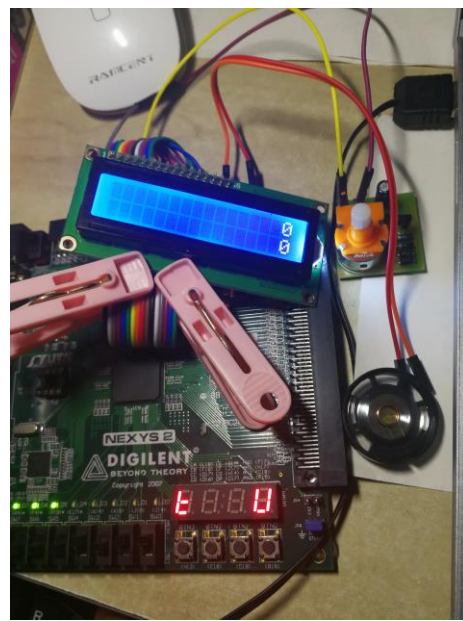
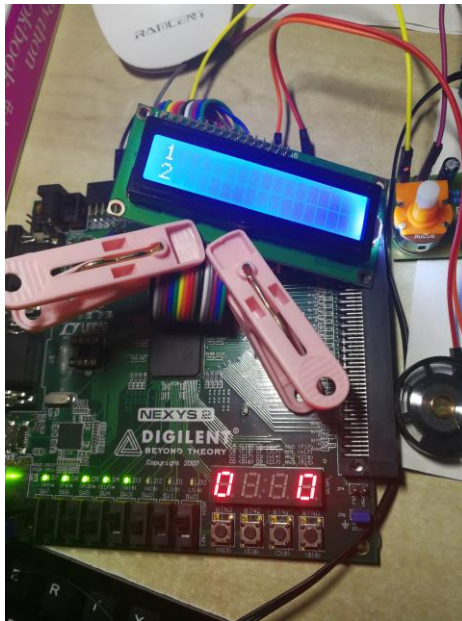
使用说明

1. 显示的视频均在该网盘：<https://pan.baidu.com/s/1hsMVXUO>
2. 下面详写步骤
 - a) 连接键盘、l c d、扬声器
 - b) 烧写完成后，会自动播放开机音乐
 - c) 调试完 LCD 可以显示后，拨下 6 号开关，关闭音乐
 - d) 用拨动开关 4 - 0 号设置密钥，按下按钮 0 复位
 - e) 然后可以进行键盘输入的加密或解密，由于数码管显示作为实时数据，LCD 作为历史数据

- f) 解密：将拨动开关调整到另一个方向，然后复位，输出编码
3. 说明
- a) 如果用其他的密钥，将得到错误的结果
- b) 加密与解密是相对的
4. 截图说明
- a) 粉红色夹子是固定杜邦线的
- b) 电位器调节 LCD 对比度



c)



尚未解决的问题及发展

1. LCD 的第一行显示会出现乱码,但是多次输入同一个字符却不会出现.而且出现这种情况可能与加入音乐有关,目前无法解决.
2. 最开始的设计是使用无线电发射和接收模块,进行加密通讯,但是选购的模块没有说明书,而且测试之后发现有并没有真的收发,而是一直显示噪声,如果要实现这一个可以考虑使用更加专业的模块.