智能密码锁

数字系统设计

12210159 应逸雯
12210357 徐婧珺

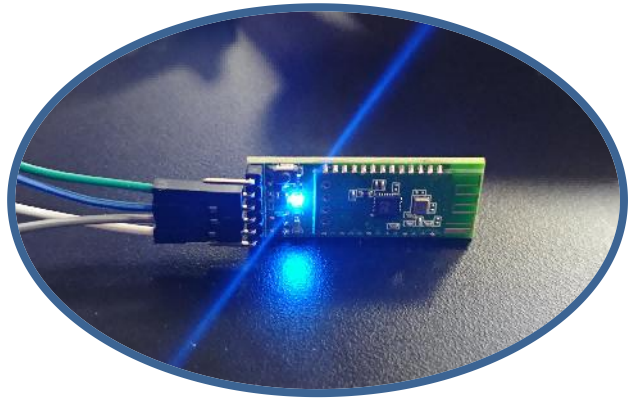
目录

CONTENT

01. 项目简介

项目背景

密码锁因其便捷性和安全性，在多个领域中得到了广泛应用。它们常见于家庭住宅、办公场所、私人设备等，用于增加设备安全性。智能密码锁尤其受到青睐，它们结合了传统密码锁和现代智能技术，如远程控制等，提供了更高水平的安全保障。



项目简介

本智能数字密码锁系统，在简单数字密码锁的基础上，结合多种安全功能，致力于为用户提供一个更安全又便捷的密码保护方案。该系统将确保在密码输入、错误尝试、以及系统锁定等关键环节提供及时的反馈和有效的安全保障。

项目功能

高效的密码输入： 系统能够通过数码管实时清晰地显示输入数字。

安全的密码储存： 系统存入密码时，使用加密算法，提高安全性。

智能的错误尝试： 系统会计算错误尝试次数，若错误超过四次，系统会自动锁定两分钟，防止暴力破解。

明确的对错反馈： 系统验证密码时，通过数码管，LED灯以及蜂鸣器的不同状态，告知用户密码的对错。

远程监控与警报： 系统将支持远程监控和警报功能，当错误尝试次数达到四次，系统将通过蓝牙模块将警报信息发送到用户手机应用。

02. 系统架构

硬件连接

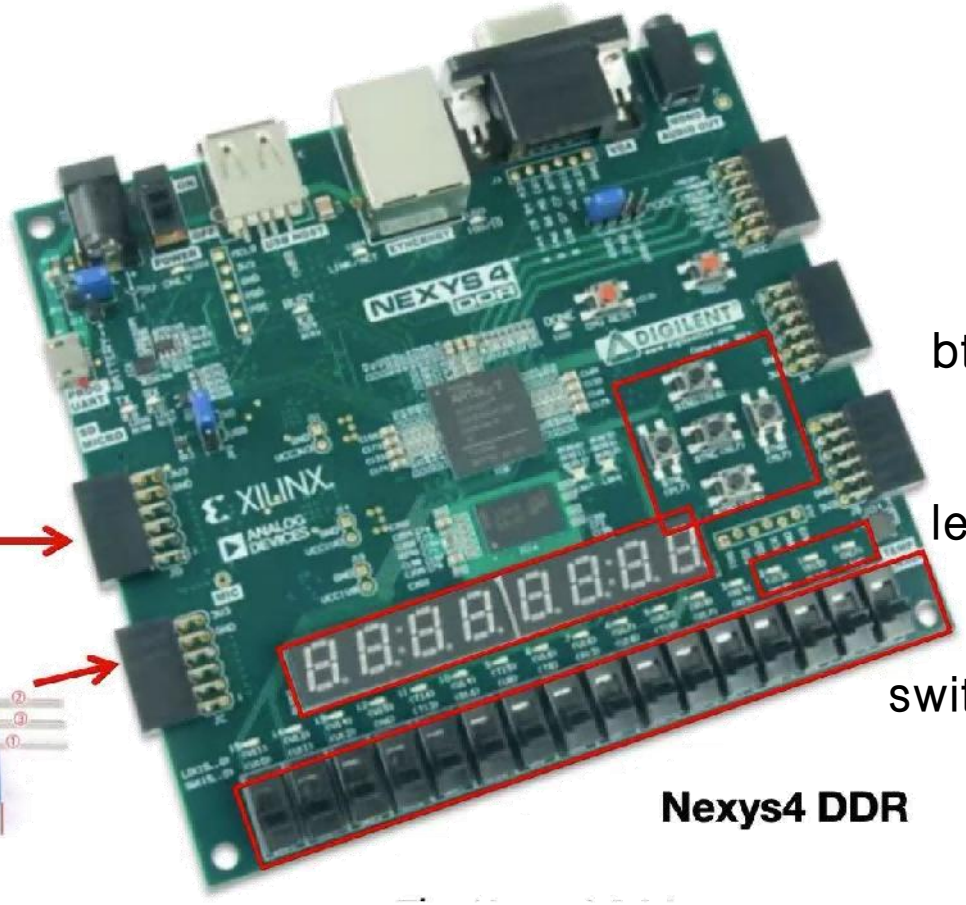
七段数码管：
- 左边四个：显示状态
- 右边四个：显示输入四位密码，以及锁定后的两分钟倒计时。

蓝牙：超过错误上限，给手机发送警报信号

蓝牙模块

蜂鸣器：密码正确播放旋律，密码错误播放警报。

蜂鸣器



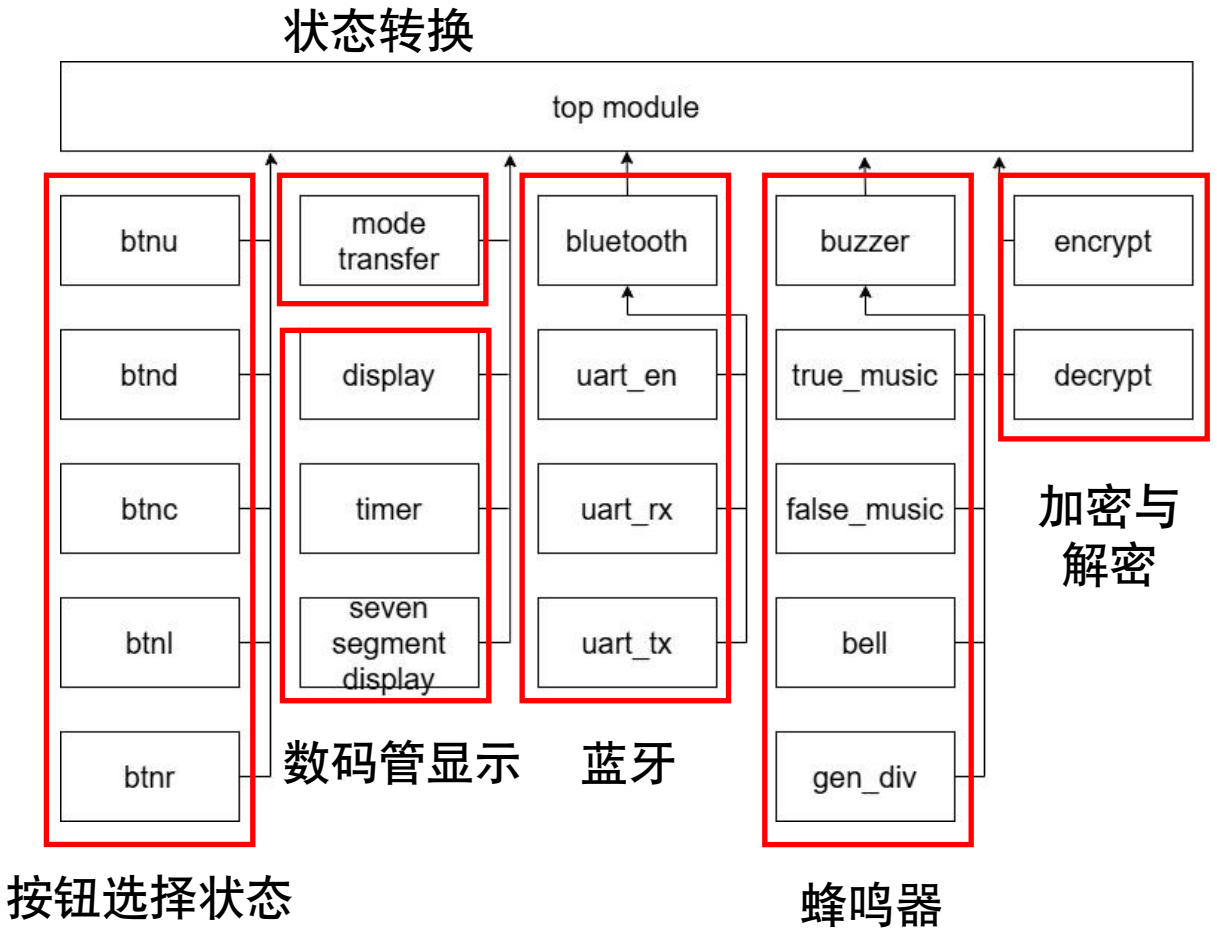
Nexys4 DDR

btn：切换状态

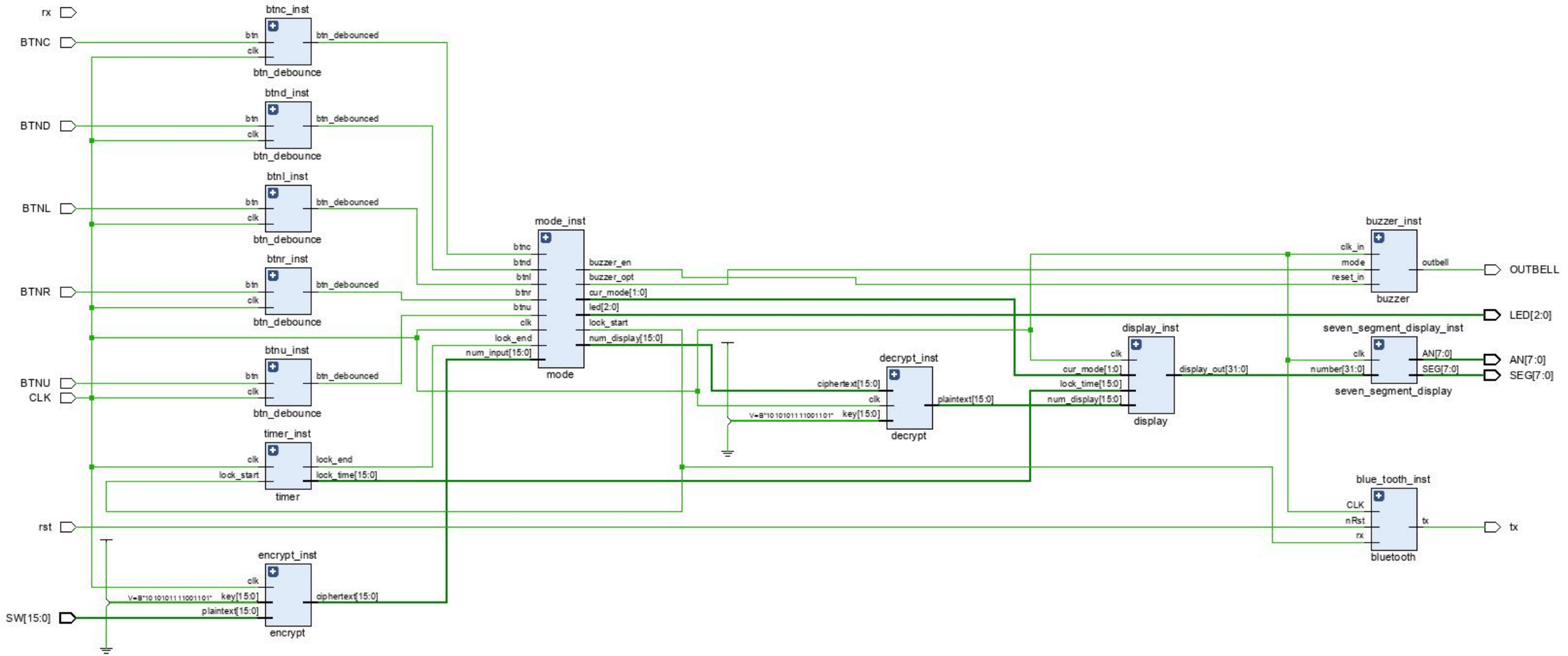
led：显示错误次数

switch：密码输入

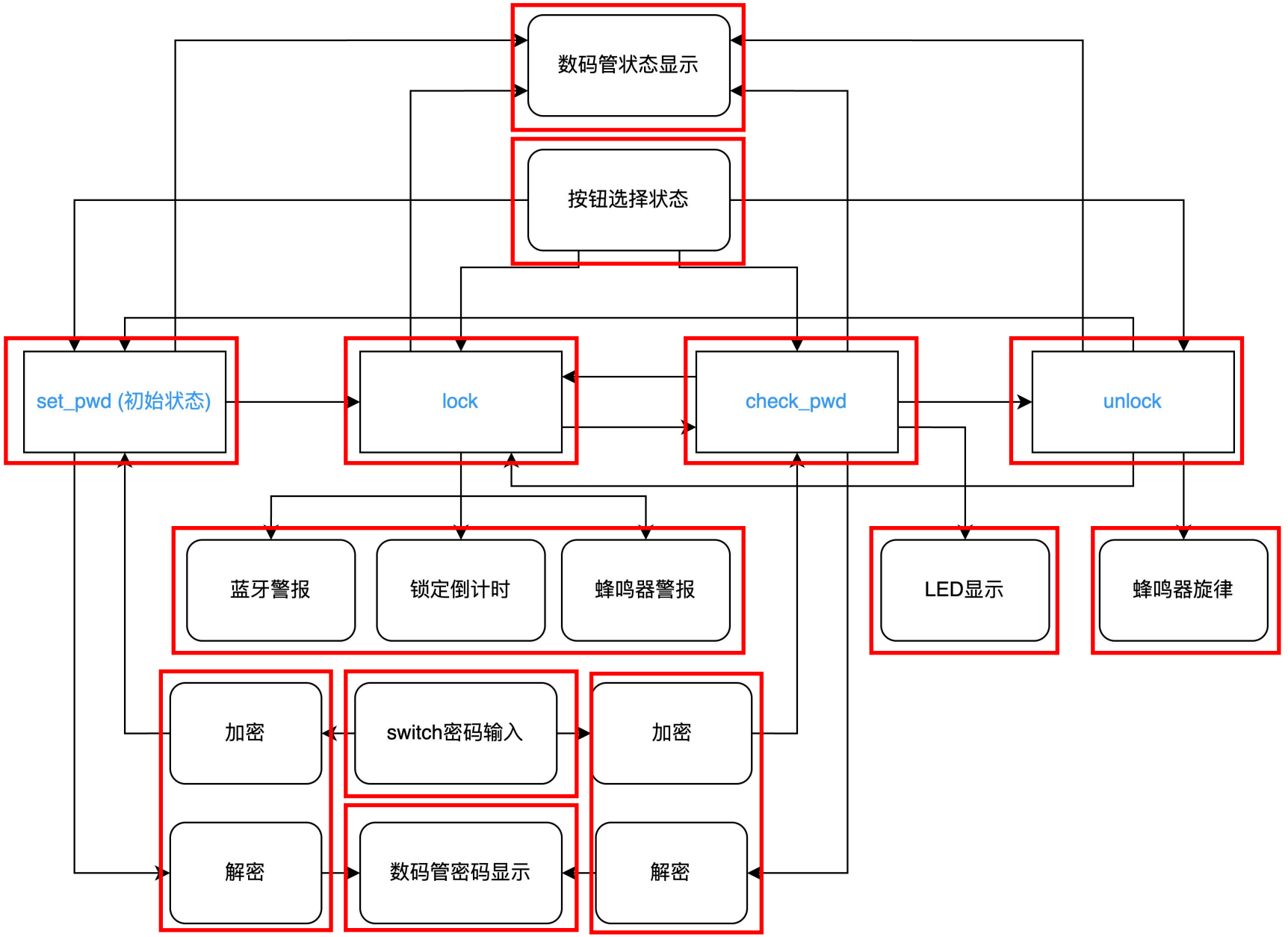
代码模块框图


状态转换
top module
btnu
btnd
btnc
btnl
btnr
mode transfer
display
timer
seven segment display
bluetooth
uart_en
uart_rx
uart_tx
buzzer
true_music
false_music
bell
gen_div
encrypt
decrypt
加密与解密
数码管显示
蓝牙
按钮选择状态
蜂鸣器

Schematic

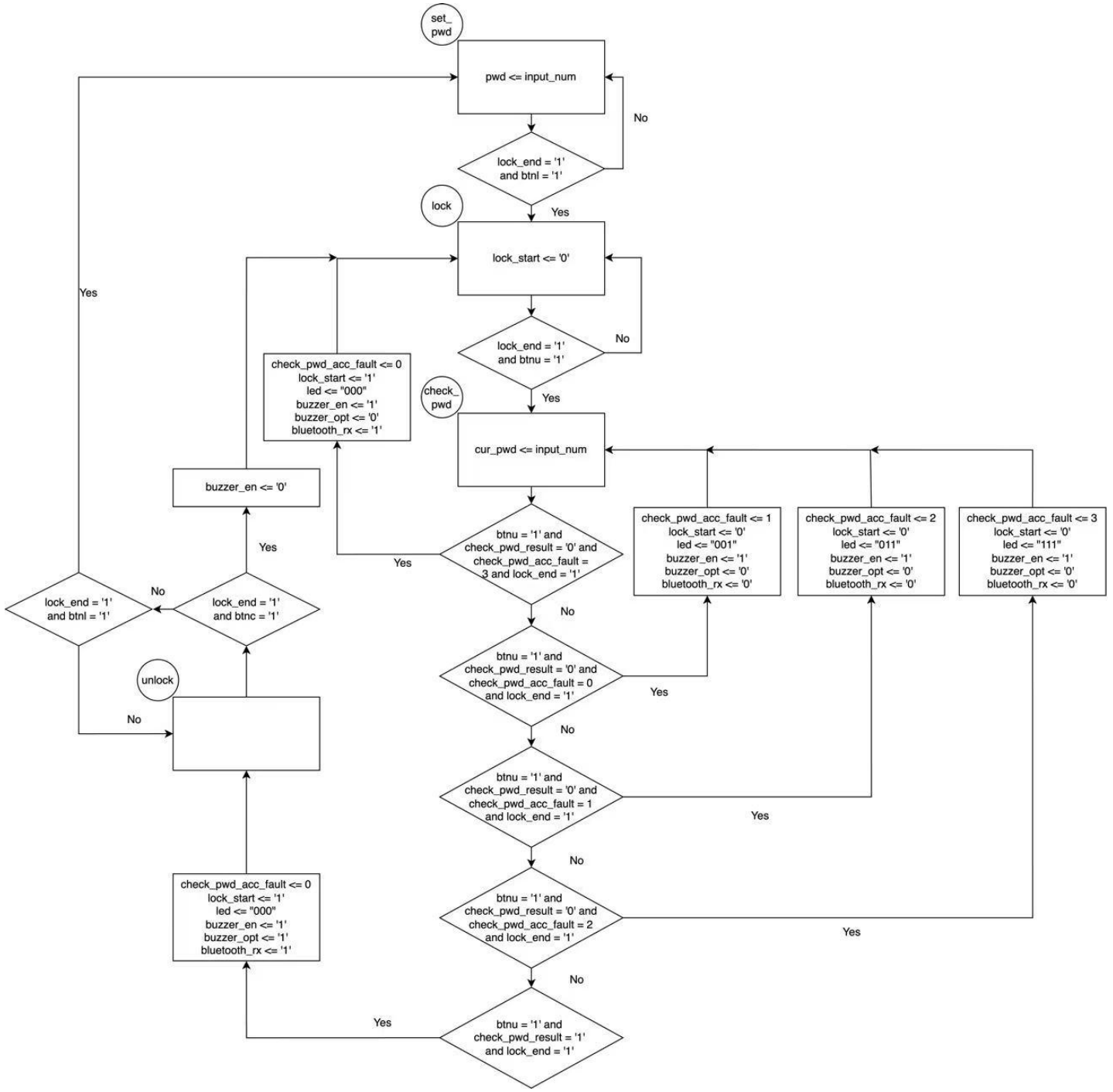

rx
BTNC
BTND
BTNL
BTNR
BTNU
CLK
rst
SW[15:0]
btnc_inst
btn
clk
btn_debounced
btn_debounce
btnd_inst
btnl_inst
btnr_inst
btnu_inst
timer_inst
lock_start
lock_end
lock_time[15:0]
timer
encrypt_inst
key[15:0]
plaintext[15:0]
ciphertext[15:0]
encrypt
mode_inst
btnc
btnd
btnl
btnr
btnu
num_input[15:0]
buzzer_en
buzzer_opt
cur_mode[1:0]
led[2:0]
num_display[15:0]
mode
decrypt_inst
decrypt
display_inst
cur_mode[1:0]
lock_time[15:0]
display_out[31:0]
display
buzzer_inst
clk_in
mode
reset_in
outbell
buzzer
OUTBELL
LED[2:0]
seven_segment_display_inst
number[31:0]
AN[7:0]
SEG[7:0]
seven_segment_display
blue_tooth_inst
CLK
nRst
rx
tx
bluetooth

VHDL框图

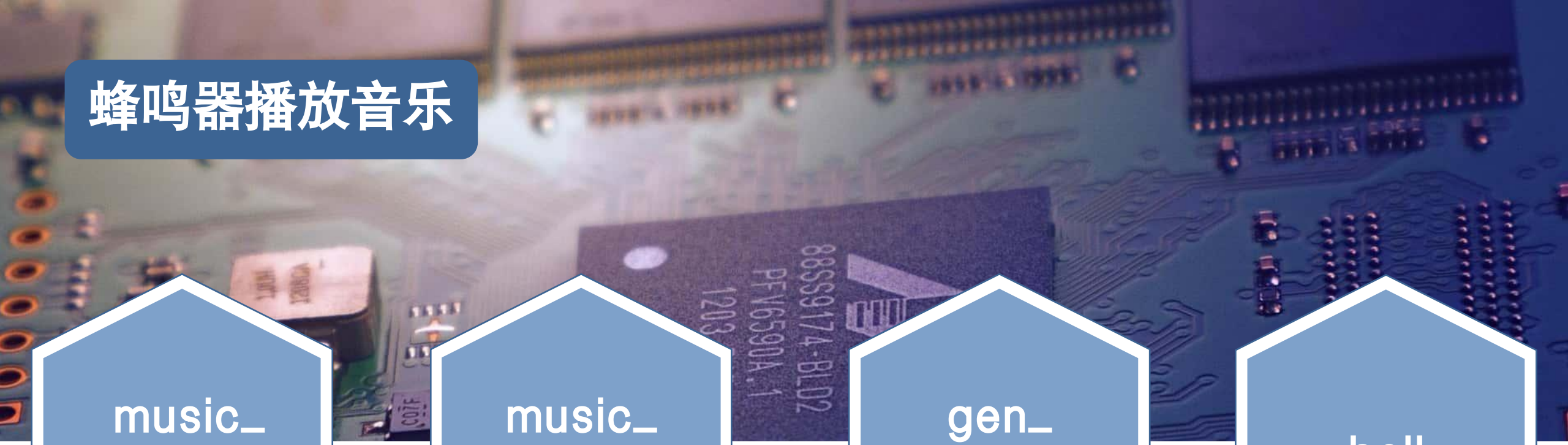

数码管状态显示
按钮选择状态
set_pwd (初始状态)
lock
check_pwd
unlock
蓝牙警报
锁定倒计时
蜂鸣器警报
LED显示
蜂鸣器旋律
加密
switch密码输入
加密
解密
数码管密码显示
解密

03. 实现原理

状态转换


set_
pwd
pwd <= input_num
No
lock_end = '1'
and btnl = '1'
lock
Yes
lock_start <= '0'
No
lock_end = '1'
and btnu = '1'
check_
pwd
Yes
cur_pwd <= input_num
check_pwd_acc_fault <= 0
lock_start <= '1'
led <= "000"
buzzer_en <= '1'
buzzer_opt <= '0'
bluetooth_rx <= '1'
buzzer_en <= '0'
Yes
Yes
btnu = '1' and
check_pwd_result = '0' and
check_pwd_acc_fault =
3 and lock_end = '1'
check_pwd_acc_fault <= 1
lock_start <= '0'
led <= "001"
buzzer_en <= '1'
buzzer_opt <= '0'
bluetooth_rx <= '0'
check_pwd_acc_fault <= 2
lock_start <= '0'
led <= "011"
buzzer_en <= '1'
buzzer_opt <= '0'
bluetooth_rx <= '0'
check_pwd_acc_fault <= 3
lock_start <= '0'
led <= "111"
buzzer_en <= '1'
buzzer_opt <= '0'
bluetooth_rx <= '0'
No
lock_end = '1'
and btnl = '1'
lock_end = '1'
and btnc = '1'
btnu = '1' and
check_pwd_result = '0' and
check_pwd_acc_fault = 0
and lock_end = '1'
Yes
unlock
No
No
btnu = '1' and
check_pwd_result = '0' and
check_pwd_acc_fault = 1
and lock_end = '1'
Yes
No
check_pwd_acc_fault <= 0
lock_start <= '1'
led <= "000"
buzzer_en <= '1'
buzzer_opt <= '1'
bluetooth_rx <= '1'
btnu = '1' and
check_pwd_result = '0' and
check_pwd_acc_fault = 2
and lock_end = '1'
Yes
No
Yes
btnu = '1' and
check_pwd_result = '1'
and lock_end = '1'

蜂鸣器播放音乐



music_correct

编写密码正确时的乐谱，使得音符能够按照节奏，当需要播放时，每秒输出音符给bell模块播放。

music_wrong

编写密码错误时的乐谱，使得音符能够按照节奏，当需要播放时，每秒输出音符给bell模块播放。

gen_div

对100M的时钟进行分频，输出分频之后的时钟信号，作为bell的时钟信号。

bell

根据输入的音符，以特定频率输出信号，以播放特定音高的声音。

辅助模组

seven segment display

- 将需要展示的数码管字符转换为SEG和AN，并轮流显示
- 除0-9外，另需定义C，E，L，H，P，以及全暗，用于特定显示需求

01

display

- 七段数码管显示逻辑在不同模式下有多种组合
- 左侧四位显示状态：锁定(LC)、解锁(OK)、设置密码(SEPD)、校验密码(CHPD)
- 右侧四位在倒计时时显示时间，在输入密码时显示密码

02

timer

- 计时器，用于密码错误后锁定一定时间，预防暴力破解密码
- 接收开始信号开始计时，倒计时2分钟
- 分频运算，从100MHz时钟获取1s，剩余时间以分和秒输出，计时归零，结束信号置1

03

加密解密算法-基于Feistel

01 密钥生成

$$K_i = \text{left\_rotate}(K, 4i)[15:8] \oplus i, \quad i = 1, 2, 3, 4$$

由主密钥，生成每一轮加密时的子密钥

02 循环加密

$$L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus \text{rotate\_left}((R_{i-1} \oplus K_i) + 5, 1)$$

$$C = R_4 \parallel L_4$$

左右交换，右半部分为异或操作结果
循环迭代多次

明文为 P，密钥为 K，密文为 C

加密解密算法-基于Feistel

03 循环解密

$$R_{i-1} = L_i, \quad L_{i-1} = R_i \oplus \text{rotate\_left}((L_i \oplus K_i) + 5, 1)$$
$$P = L_0 \parallel R_0$$

逆向左右交换，左半部分为异或操作结果
循环迭代多次

04 实现技巧

子密钥生成函数、循环移位操作，采用并行计算，
体现了FPGA的硬件加速能力

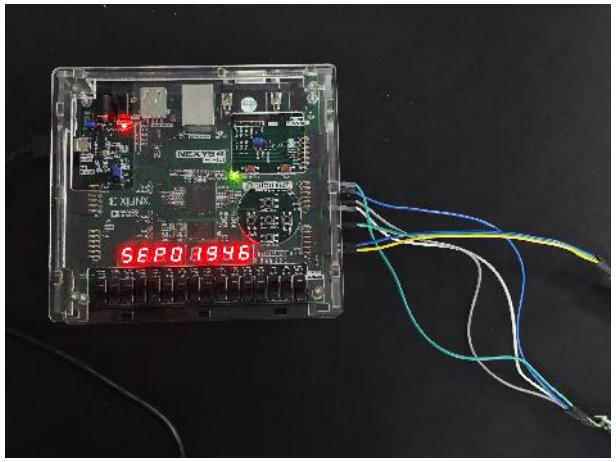
明文为 P，密钥为 K，密文为 C

蓝牙串口通信

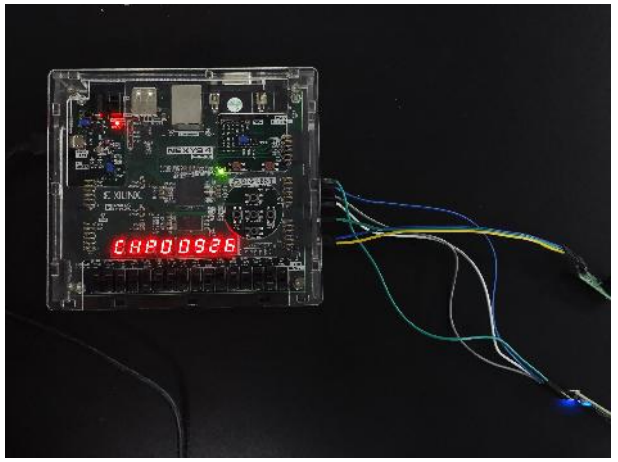
- uart_en：根据系统时钟频率（sysclk，100MHz）和波特率（BPS，9600），得到接收和发送的采样周期，tx为一倍频，rx为八倍频，在每个采样周期结束时输出一个使能信号
- uart_rx：使用状态机接收UART数据，检测数据段为起始位/数据位/奇偶校验位/停止位，并根据数据格式接收数据，转发数据并输出接收完成信号
- uart_tx：使用状态机发送UART数据，当接收到发送请求后，在数据包中加入串口数据格式（起始位，奇偶校验位，停止位），串行发送数据，全部发送完成后输出完成确认
- bluetooth：接收到报警信号后，写入发送数据，使能发送端

04. 成果展示

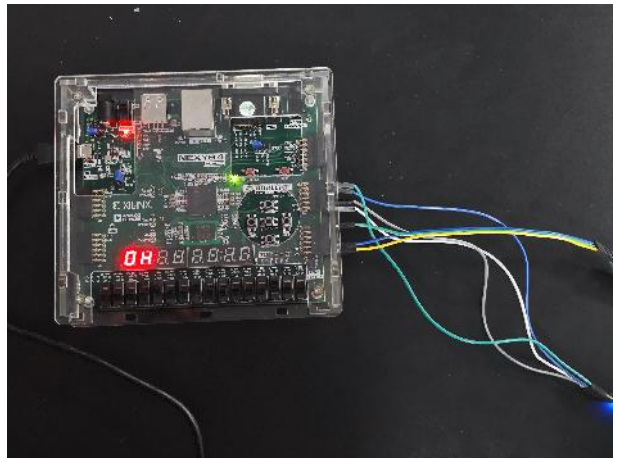
各状态效果



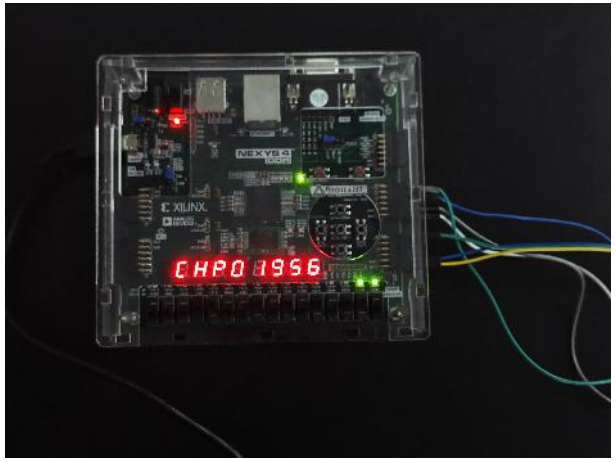
设置密码（SEPD）



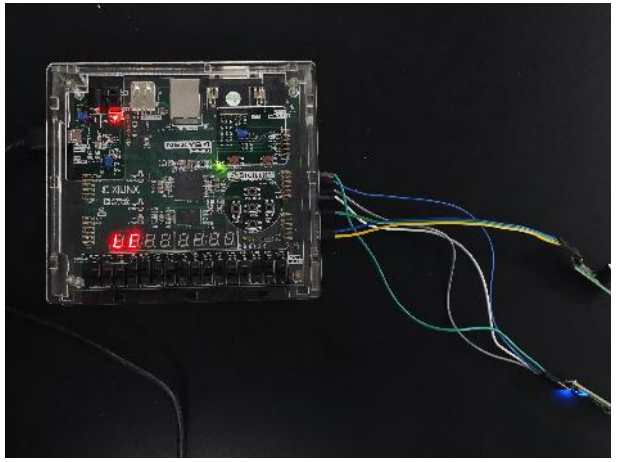
校验密码（CHPD）



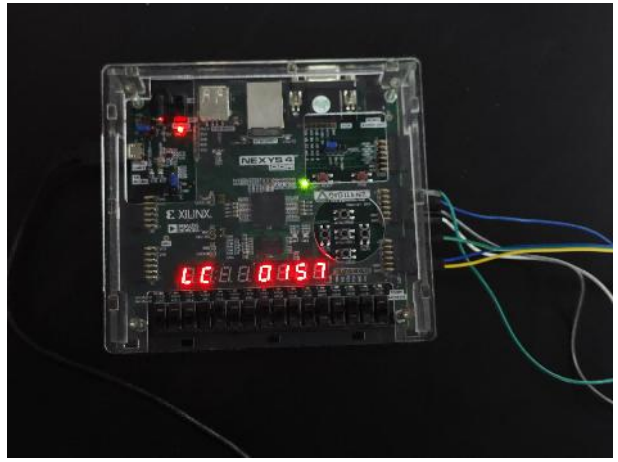
解锁状态（OK）



校验密码错误中（CHPD）



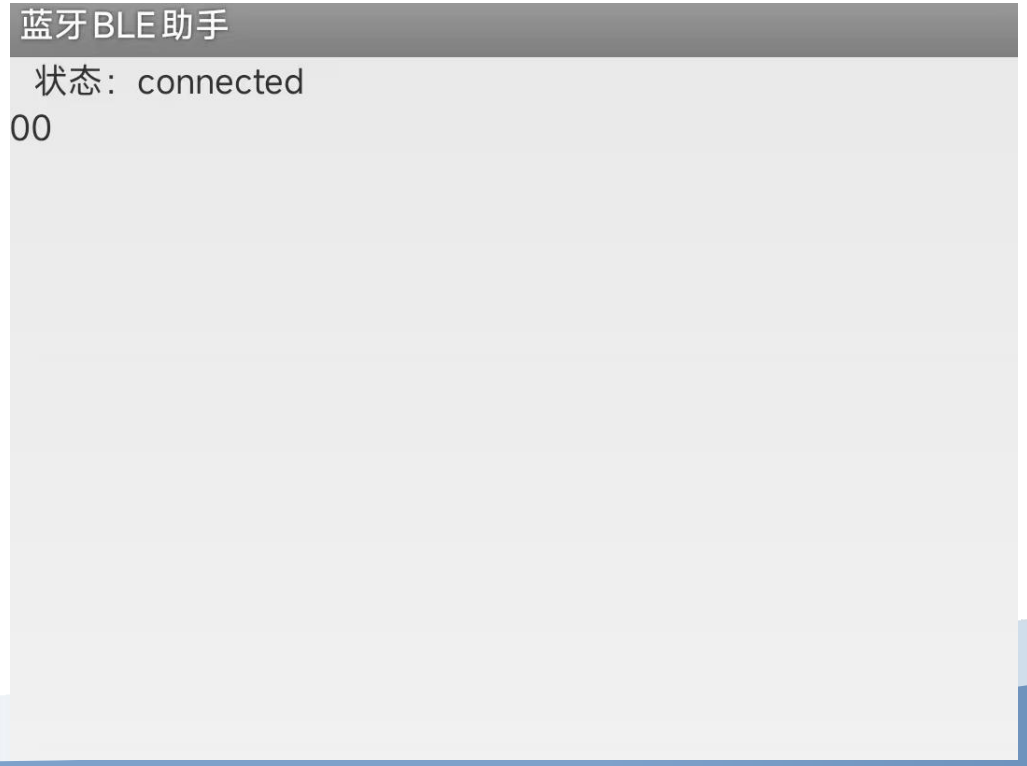
锁定状态（LC）



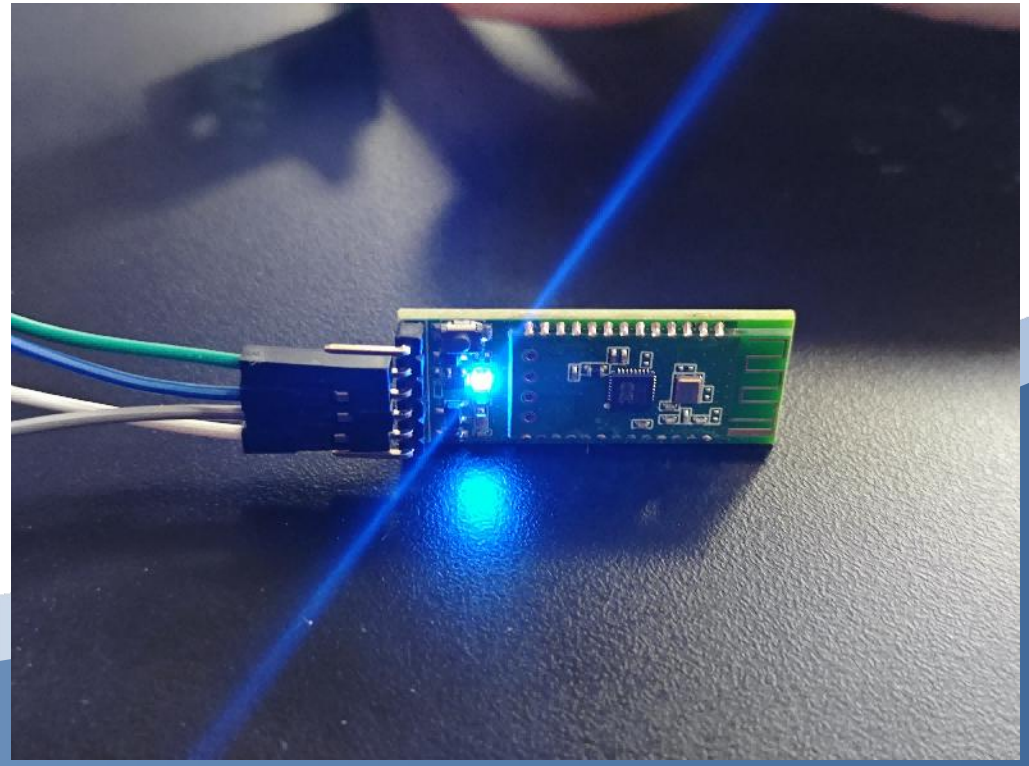
锁定状态，倒计时中（LC）

蓝牙效果

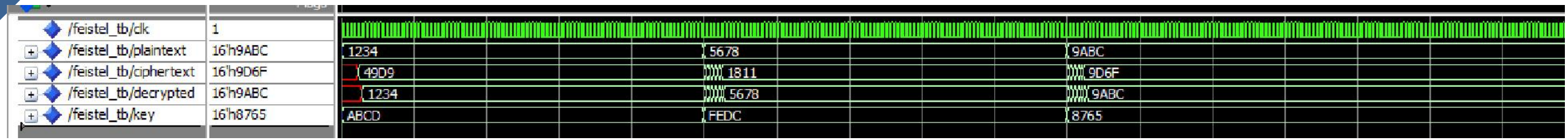
手机端结果



蓝牙模块



加密解密



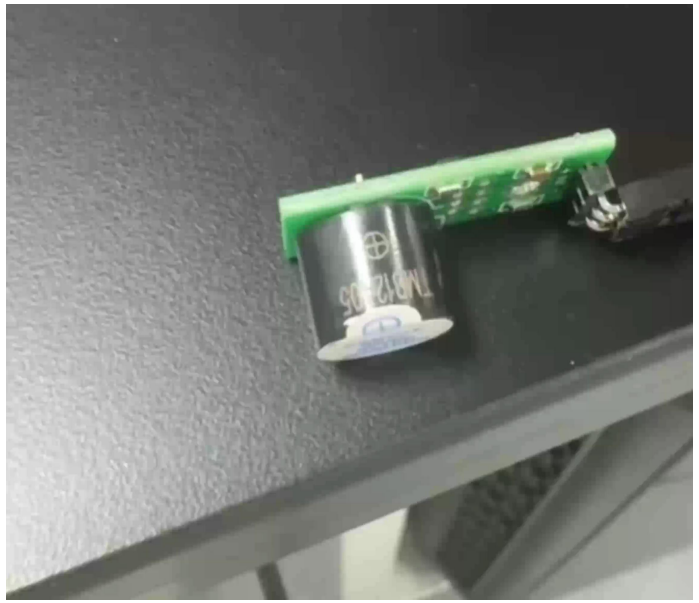
测试了三组不同的密码及密钥
（1234+ABCD，5678+FEDC，9ABC+8765）

plaintext为加密前的值
ciphertext为加密后的值
decrypted为解密后的值
key为密钥

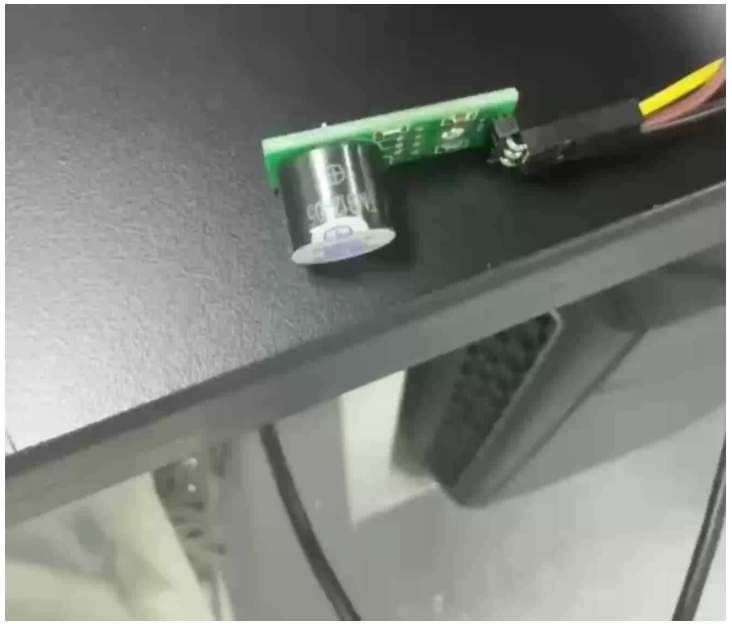
plaintext=decrypted

音乐效果

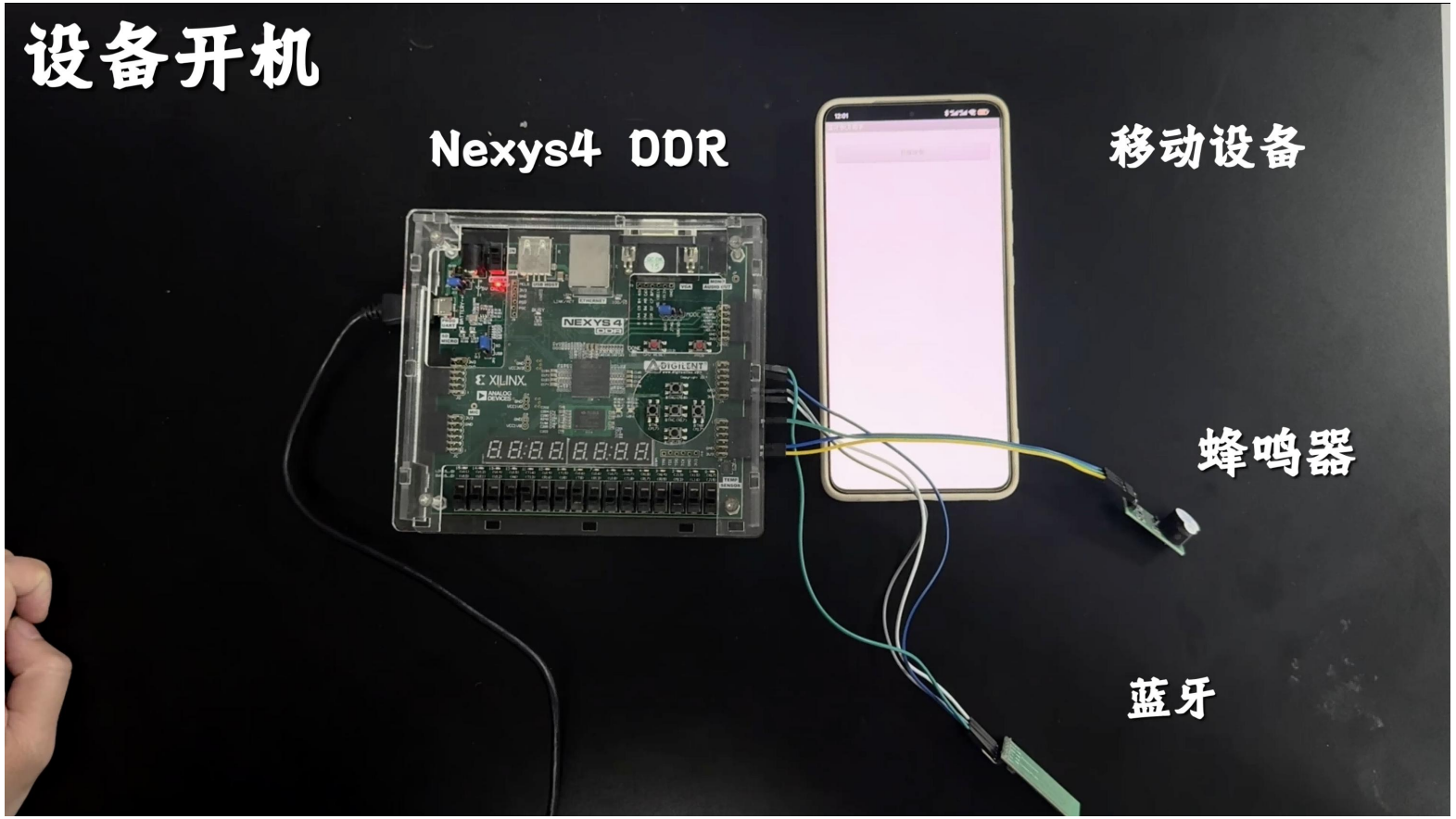
旋律声



警报声



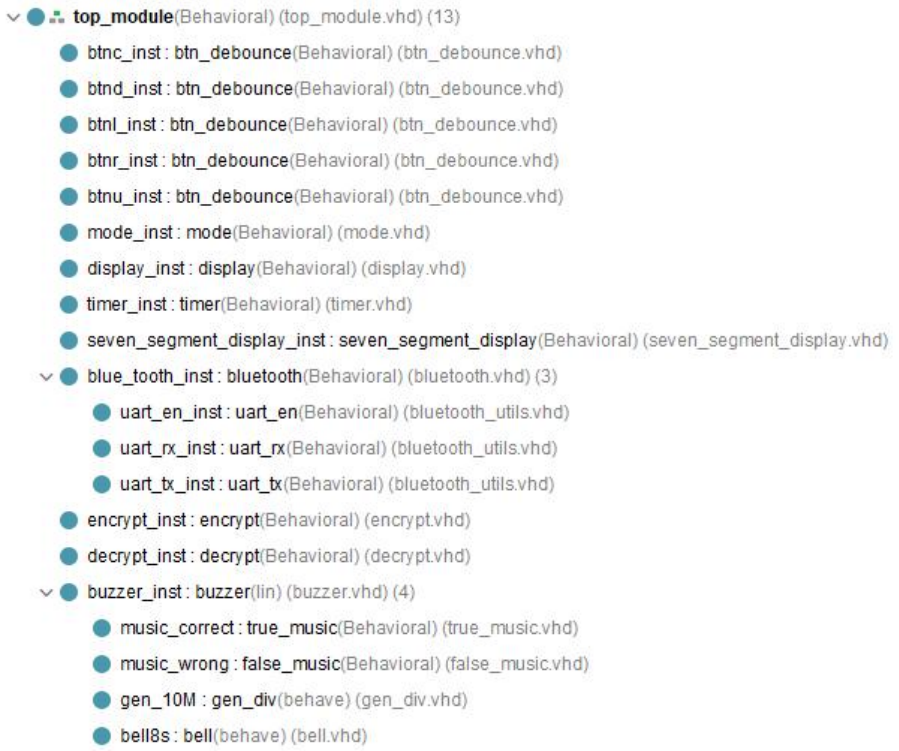
演示视频



05. 项目总结

项目总结

实现了智能密码锁的搭建，具有**设置密码，加密存储，密码校验，防暴力破解，蓝牙远程警报，声音警报**等多重功能



工作量

应逸雯：各模块集成，基本功能辅助模块，蓝牙串口通信，加解密算法，汇报文件制作

徐婧珺：各模块集成，状态转换逻辑，蜂鸣器模块，汇报文件制作

感谢聆听！